Securing Digital India Against AI & Cyber Threats

Leveraging AI Security & Zero Trust

BY

VISHAL GAUTAM

SANJIT GANGULI

CONTRIBUTORS

JAY CHAUDHRY, CEO & Founder, Zscaler

LT GENERAL RAJESH PANT

Securing Digital India Against AI & Cyber Threats

Leveraging AI Security & Zero Trust

Published February 2026
First Edition
ISBN Number: 979-8-90333-906-8

Securing Digital India Against AI & Cyber Threats

Leveraging AI Security & Zero Trust

BY
VISHAL GAUTAM
SANJIT GANGULI

CONTRIBUTORS
JAY CHAUDHRY, CEO & Founder, Zscaler
LT. GENERAL (DR.) RAJESH PANT

About the Contributors

Jay Chaudhry is the Founder, Chairman, and CEO of Zscaler, the pioneering cloud security company that redefined network security with its Zero Trust Exchange platform. A serial entrepreneur, he has founded and led several successful cybersecurity and networking companies, before establishing Zscaler in 2007. Chaudhry is widely recognized for foreseeing the shift to cloud and mobile, and for championing the Zero Trust security model to protect distributed workforces and applications. His leadership has positioned Zscaler as a global leader in cloud-native security, significantly influencing the cybersecurity landscape for enterprises and governments worldwide

Lt. General (Dr.) Rajesh Pant served as India's National Cyber Security Coordinator (NCSC) in the Prime Minister's Office between 2019 and 2023. In this pivotal role, he was instrumental in shaping the nation's cybersecurity strategy and bolstering the protection of its critical information infrastructure. His mandate included fostering international collaboration, driving capacity building, and ensuring a robust response mechanism against cyber threats impacting India. General Pant played a crucial role in enhancing India's cyber resilience and positioning the country as a significant player in global cybersecurity efforts.

About the Authors

Vishal Gautam is Director of Zscaler AI & Cyber Threat Research Center – India. He has been part of Zscaler's journey since its early startup days in India, and played a pivotal role in building its flagship security products from the ground up. With experience spanning across India and the United States, he has contributed significantly to scaling Zscaler's engineering capabilities and establishing India as a core hub for innovation and product development.

Sanjit Ganguli is a CTO–in–Residence at Zscaler, specializing in Zero Trust strategy, network transformation and digital employee experience advisory. Prior to his role at Zscaler, he was a Gartner analyst leading research in network modernization, AIOps, and Zero Trust. Sanjit has previously written three books on the topics of Zero Trust and security transformation.

Foreword

By Jay Chaudhry

India is undergoing a foundational digital transformation, building systems at population scale, not just enterprise scale. This book, *Securing Digital India Against AI & Cyber Threats*, captures the essence of this change: a move from bounded systems to a borderless digital state. The old 'castle–and–moat' security model is failing, evidenced by sophisticated cyber attacks and the surge in ransomware and nation–state actors. Traditional security is inadequate for the modern threat landscape, which is further complicated by the rapid rise of Artificial Intelligence, exploiting identity, supply chains, and implicit trust. Cyber risk is no longer a niche IT problem; it is a critical component of national safety and economic stability.

For India to become *Viksit Bharat* by 2047, the ideas put forth in this book are vital. It elevates cybersecurity from a technical task to a strategic leadership imperative. The stakes are national security, economic growth, and citizen trust. Security must be built into the very architecture of national systems, not bolted on as an afterthought. Leaders across government and critical sectors must set clear priorities, allocate resources, and drive the cultural shift to align security with India's long–term economic and strategic goals.

The implementation of a Zero Trust architecture will fundamentally redefine how Indian leaders achieve security and resilience. Zero Trust is a design philosophy perfectly aligned with a cloud–first, mobile–first nation leveraging population–scale digital platforms and shared AI infrastructure. For leaders, this shift reduces the attack surface, enables compliance with acts like the Digital Personal Data Protection (DPDP) Act, and limits the lateral movement frequently leveraged by sophisticated nation–state actors. Furthermore, adopting a Zero Trust architecture simplifies IT infrastructure by eliminating multiple point solutions, which in turn reduces cost and improves overall security posture as a result.

Five Takeaways

- Eliminate your attack surface
- Never put users and agents on your network
- Treat each branch like an internet café
- Only allow select users access to mission–critical applications
- Start with full visibility and testing for your AI applications

I hope this book serves as a useful guide to understand Zero Trust and navigate a successful security transformation.

Jay Chaudhry
CEO and Founder, Zscaler

Contents

Introduction

India is in the midst of one of the most ambitious digital transformations ever attempted by a nation. Over the last decade, the country has built digital systems that operate not at enterprise scale, but at population scale—supporting governance, economic activity, social inclusion, and innovation for more than a billion people.

Digital Public Infrastructure (DPI) platforms such as Aadhaar, UPI, DigiLocker, FASTag, GSTN, and CoWIN now form the backbone of public service delivery and economic participation. At the same time, India's Critical Information Infrastructure (CII) spanning power, telecom, banking, transport, oil and gas, space, defence, and government systems has grown deeply interconnected and increasingly software-driven. These systems are no longer peripheral enablers; they are foundational to national security, economic stability, and public trust.

As India sets its sights on becoming a $30 trillion economy and Viksit Bharat by 2047, cybersecurity is no longer a technical concern to be delegated to specialists. It is a leadership issue, a governance responsibility, and a strategic enabler of national ambition.

As this issue is taken up the chain, it's vital to understand that the nature of cyber risk has fundamentally changed.

India Rising from Bounded Systems to a Borderless Digital State

Traditional cybersecurity models were designed for a different era, one in which systems lived inside clearly defined perimeters, users operated from known locations, and trust could be inferred from network boundaries. Firewalls, VPNs, and perimeter defences were effective when digital assets were confined within organisational walls.

India's digital reality today looks nothing like that world.

Government systems span clouds and data centres, are accessed from mobile devices across the country, integrate continuously with private-sector platforms, and increasingly rely on software supply chains that cross national borders. Citizens, officials, service providers, machines, and algorithms interact in real time across shared digital rails. Artificial intelligence systems are being deployed not in isolated labs, but on shared national compute infrastructure and data commons, enabling innovation at unprecedented scale.

In this environment, there is no meaningful "inside" or "outside" of the network.

Cyber adversaries, whether criminals, organized fraud networks, or nation-state actors, understand this shift well. They no longer focus solely on breaching perimeters. Instead, they exploit identities, supply chains, misconfigurations, excessive privileges, and implicit trust within systems.

Cyber adversaries, whether criminals, organized fraud networks, or nation-state actors, understand this shift well. They no longer focus solely on breaching perimeters. Instead, they exploit identities, supply chains, misconfigurations, excessive privileges, and implicit trust within systems. Once inside, they move laterally, escalate access, and persist, often undetected, causing damage that extends far beyond a single organisation or sector.

The results are visible and costly. Digital fraud and cybercrime drain significant economic value each year, weaken trust in digital systems, and impose an invisible tax on growth. Attacks on critical infrastructure carry the risk of cascading failures across sectors. Data breaches undermine citizen confidence and expose the State to legal, reputational, and operational consequences under India's evolving regulatory framework.

Digital fraud and cybercrime drain significant economic value each year, weaken trust in digital systems, and impose an invisible tax on growth. Attacks on critical infrastructure carry the risk of cascading failures across sectors. Data breaches undermine citizen confidence and expose the State to legal, reputational, and operational consequences under India's evolving regulatory framework.

This is not a failure of intent or effort. It is a mismatch between modern digital realities and legacy security architectures.

Cybersecurity as State Capacity and Economic Enabler

For India, cybersecurity must be understood not merely as protection against threats, but as an enabler of governance and growth.

Secure digital systems allow governments to deliver services efficiently, ensure the continuity of essential infrastructure, attract investment, foster innovation, and uphold the rights and dignity of citizens. Conversely, insecure systems impose friction, increase compliance costs, slow adoption, and create systemic risk.

Recognizing this, India has put important institutional and legal frameworks in place. The National Critical Information Infrastructure Protection Centre (NCIIPC) has defined sectoral responsibilities and security expectations for CIIs. MeitY, CERT-In, RBI and State Governments have published several guidelines for organisations and enterprises to enhance their cybersecurity posture. The Digital Personal Data Protection (DPDP) Act 2023 establishes statutory obligations for protecting personal data and responding to breaches. National AI strategies emphasize the need to democratize access to compute and data while safeguarding sovereignty and trust.

What these frameworks increasingly point to is a simple but profound insight: security can no longer be bolted on; it must be built into the architecture of systems from the start.

Why Zero Trust Matters for Viksit Bharat 2047

Zero Trust architecture represents this architectural shift.

At its core, Zero Trust is based on a straightforward principle: never assume trust; always verify. Access to systems, data, and services is granted based on identity, context, and policy—not on network location. Verification is continuous, privileges are minimal, and systems are designed to limit the impact of any compromise.

Zero Trust enables India to reduce attack surfaces, contain breaches, and isolate failures, without slowing down innovation or digital inclusion.

For a nation like India, Zero Trust is not an abstract concept or a product category. It is a design philosophy that aligns naturally with the realities of:

- Population-scale digital platforms
- Highly interconnected critical infrastructure
- Cloud-first and mobile-first service delivery
- Shared AI and data infrastructure
- A diverse ecosystem of government entities, PSUs, MSMEs, startups, and global partners

Zero Trust enables India to reduce attack surfaces, contain breaches, and isolate failures, without slowing down innovation or digital inclusion. It supports compliance with data protection laws by enforcing least privilege and continuous monitoring. It

strengthens resilience against supply–chain risks and prepares systems for emerging threats, including those posed by advances in quantum computing.

Most importantly, Zero Trust allows India to reconcile two objectives that are often seen as conflicting: openness and security. It makes it possible to democratize access to digital systems and AI infrastructure while maintaining strong safeguards for national assets and citizen data.

Cybersecurity at national scale cannot be achieved by technology teams alone. It requires active engagement from leadership, Ministers, Secretaries, heads of departments, PSU boards, regulators, and senior executives responsible for critical sectors.

The Role of Leadership

Cybersecurity at national scale cannot be achieved by technology teams alone. It requires active engagement from leadership, Ministers, Secretaries, heads of departments, PSU boards, regulators, and senior executives responsible for critical sectors.

Leaders set priorities, allocate resources, approve architectures, oversee risk, and shape organisational culture. They determine whether cybersecurity is treated as a compliance exercise or as a strategic capability. In India's context, leadership oversight is especially critical because of the sheer scale, diversity, and interdependence of its digital systems.

This book is written with that responsibility in mind.

Purpose of This Book

This book is not intended to replace existing technical guidelines issued by expert bodies, nor to duplicate detailed standards already available. Instead, it aims to help senior leaders:

- Understand why traditional security approaches are no longer sufficient
- Recognize Zero Trust as a foundational architectural shift, not a tactical tool
- Ask the right questions of their organisations and technology teams
- Make informed decisions about investment, policy, and oversight
- Align cybersecurity with India's long-term economic and strategic goals

Cybersecurity is not a constraint on India's aspirations. When designed correctly, it is a force multiplier.

As Bharat moves toward 2047, the challenge before its leaders is not whether to digitize further but how to do so securely, confidently, and at scale. The choices made today about security architecture will determine whether India's digital systems remain resilient foundations for growth or become fragile points of failure.

This book is an invitation to engage with that choice, deliberately and decisively.

CHAPTER
1

Understanding and Mitigating Cyber Risk and Data Loss

Understanding Cyber Risk

Properly prioritizing cyber risks starts with a general understanding of cyberattacks. A cyberattack is when cybercriminals attempt to gain unauthorized access to an organisation's people, infrastructure (assets, technology), and/or data. Attackers can be external (e.g., criminals, competitors, or state-sponsored organisations) or internal. Internal threat actors may have been sent by state-sponsored organisations, be hostile employees (e.g., through ill-intent or blackmail), or careless users (unintentional).

Threat actors continue to evolve and expand their activities at an unprecedented rate. Many threat groups are well funded. Nation-state actors (government or politically linked) are growing in sophistication and capability and launch advanced attacks tailored to target and harm specific organisations and governments. Organisations lacking the right security controls, layers of defence, or those using vulnerable infrastructure such as firewalls and VPNs expose themselves to greater cyber risks from intentional actors.

Many threat groups are well funded. Nation-state actors (government or politically linked) are growing in sophistication and capability and launch advanced attacks tailored to target and harm specific organisations and governments.

Cyber risks also come from less obvious sources, such as "trusted" partners: customers or suppliers with preferred access to an organisation's systems that can be compromised and used to breach. This is known as supply chain risk. This is a less obvious form of cyber risk that arises when an organisation integrates vulnerable technologies from these external partners. If there isn't something in place to detect integrated but exploited resources, adversaries may have free reign in the environment.

Nation-backed cyberattacks are extremely sophisticated, and their operators are highly capable. They have repeatedly shown their ability to find weak links in an organisation, access sensitive areas, and extract data. We have seen, and will likely continue to see, major take-downs of organisations from a single point of entry.

Successful attackers may perform a variety of malicious actions:

- Disrupting daily business operations
- Disabling computers and mobile phones
- Revoking and denying the organisation access to its own data
- Monitoring activity in a system to gain proprietary insights
- Collecting and stealing data
- Destroying information or technology systems
- Using a compromised computer to launch attacks against other systems

Cyberattacks generally fall into two categories: untargeted and targeted. With an untargeted attack, a bad actor focuses on the mass exploitation of as many humans or as much technology as possible. In a targeted attack, a bad actor singles out a single organisation, division (e.g., development), or individual people (e.g., executive assistant of CEO).

There are four main types of cyberattacks (also called breaches):

- **Phishing:** criminals use social engineering to impersonate a trusted source, such as a bank or leader, in an attempt to persuade you to hand over sensitive information
- **Ransomware:** criminals launch malicious software onto information systems to lock or encrypt data, preventing access until a ransom has been paid
- **Malware:** criminals develop malicious software to attack technology systems and actively cause harm, such as to steal data or credit card information, or to plant spyware to monitor system activity
- **Insider threats:** people inside organisations who have access to sensitive data and cause a data breach, sometimes unwittingly

Cyberattacks are very detrimental to an organisation's operations:

- Theft of customer/user information: **criminals target sensitive, personal information,** often by impersonation using voice, email addresses, Slack, and other communication mechanisms
- **Theft of intellectual property, trade secrets, and nonpublic information:** criminals go after an organisation's most critical data
- **Denial of service:** criminals actively prevent access to services, such as public websites, email, or a laptop

Zscaler's ThreatLabz researchers analysed ransomware activity from April 2024 to April 2025, looking at public data leak sites, Zscaler's proprietary threat intelligence, ransomware samples, attack data, and telemetry from the Zscaler Zero Trust Exchange. The Zscaler Threatlabz 2025 Ransomware Report showed the following:

- **Ransomware attacks skyrocketed 145.9% year-over-year:** Attackers are scaling campaigns faster than ever, with Zscaler blocking an unprecedented number of ransomware attacks over the past year.
- **Public extortion cases increased 70.1%:** Far more organisations were listed on ransomware leak sites year-over-year as attackers escalated pressure tactics.
- **Data exfiltration volumes surged 92.7%:** ThreatLabz analysed 10 major ransomware families, uncovering a total of 238.5 TB of data exfiltrated, evidence that data theft is fueling extortion campaigns.
- **Critical industries continue to be prime targets:** Manufacturing, Technology, and Healthcare experienced the highest number of ransomware attacks, while sectors like Oil & Gas (+935%) and Government (+235%) saw notable year-over-year spikes.
- **Ransomware groups are evolving fast:** Established families like RansomHub, Clop, and Akira remained dominant, while 34 new groups emerged as identified by ThreatLabz, including rebrands or offshoots of defunct groups and new groups looking to fill the void left by takedowns or other disruptions. Collectively, they reflect a dynamic, fast-moving ransomware ecosystem where threat actors continually adapt.

A "zero-day" attack is one that uses a previously unidentified vulnerability to exploit hardware or software. These attacks often target technology used by millions in private organisations, government agencies, and critical infrastructure bodies. A zero-day event can lead to macroeconomic damages, impact public health, and threaten national security. In fact, an announcement[1] found that 70% of deployments of a popular firewall were vulnerable to such an attack. This amounted to more than 300,000 instances that could be exploitable by attackers.

Real-life Example of a "Zero Day" Attack in June/July 2017 Impacting Maersk[9]

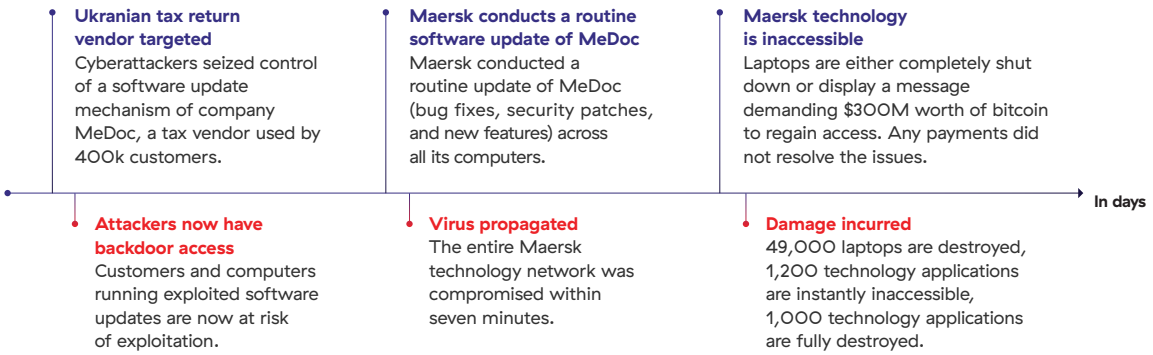


Figure 01: Details of the Maersk breach.

1 *The Record (2023, July 5)*. July 5th, 2023 Briefs Cybercrime Get more insights with the Recorded Future Intelligence Cloud. Learn more. Nearly 70% of FortiGate Firewalls are vulnerable to new bug, experts say. https://therecord.media/fortigate-firewalls-vulnerable-to-new-bug

A Recent Sharp Increase in Cybersecurity Breaches Has Led to Billions of Dollars in Damages

September 2019: SolarWinds
Backdoor malware

This supply chain attack, which went unreported until late 2020, affected thousands of companies and multiple US government agencies. The total cost is unknown but estimated to be in the billions of dollars.

January 2021: Microsoft Exchange
Zero-day exploit

Attackers exploited a series of zero-day vulnerabilities in Microsoft Exchange servers, exposing some 250,000 servers worldwide.

May 2021: Colonial Pipeline
Ransomware

A ransomware attack shut down the pipeline, causing fuel shortages and price increases. The company paid a ransom of 75 bitcoin, roughly $4.4 million.

July 2021: Kaseya
Ransomware

This supply chain attack affected roughly 1,500 businesses worldwide, with many paying the attackers individual six-figure ransoms before a universal decryption key became available.

August 2021: T-Mobile
API exploit

A data breach exposed the personal information of more than 76 million people in the US, leading to a $350 million settlement as well as $150 million in added security spend.

October 2021: Facebook
Harvesting/Social engineering

A data breach exposed the personal information of 1.5 billion users, which was then offered for sale online. The total cost is unknown.

March 2022: Microsoft
Zero-day exploit

Attackers had exploited a vulnerability in the Microsoft 365 authentication process since mid-late 2021 to serve a large-scale phishing campaign. The total cost is unknown.

January 2022: Apache Log4j
Zero-day exploit

A vulnerability in this logging utility put 93% of enterprise cloud environments at risk, with over a million attempted attacks in the three days after it was disclosed.

January 2022: Twitter
Zero-day exploit

A hacker scraped the email addresses of more than 200 million users from Twitter's platform, and then attempted to sell them for a lump $200,000.

February 2024: Change Healthcare
Ransomware

Data breach due to ransomware exposed the personal information of over 190 million customers, resulting in a total cost of $3.09 billion in 2024.

Late 2024: US Telecoms Companies
Firewall Exploits

AT&T, Verizon and T-Mobile were among the telecoms companies hit by a years-long Chinese nation state hacking campaign known as Salt Typhoon.

July 2025: Qantas Airlines
Social Engineering

Millions of customer records were stolen in an attack that led to the board reducing the CEO's annual bonus by A$250,000.

August 2025: Salesloft Drift
Supply Chain Attack

Cybercriminals accessed data from more than 700 organizations by compromising Drift, a tool that automates sales processes through integrations with Salesforce and other applications.

Figure 02: Overview of major cyber breaches since late 2019

High-level examination of the Colonial Pipeline Attack of 2021

Colonial Pipeline[2] is the largest refined products pipeline in the United States, transporting more than 100 million gallons of fuel daily to meet the energy needs of consumers. In May 2021, the company experienced a cyberattack that had major nationwide implications for everyday people and corporations in the US.

The attackers stole a Colonial Pipeline user's login credentials. The vulnerable state of the cybersecurity and technology solutions in place allowed attackers to gain access to all systems and data. The attackers targeted a high-value billing application and held the data for ransom. Colonial Pipeline paid the ransom of $4.4M USD (although $2.3M USD was later recovered by US Federal law enforcement).

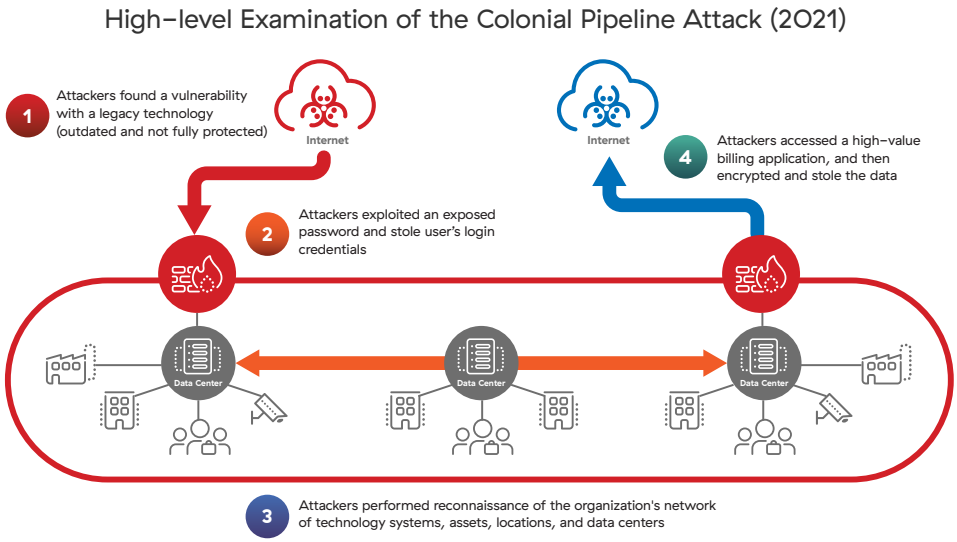


Figure 03: Details of the Colonial Pipeline breach

The incident produced multiple impacts:

- $4.4M USD in ransom pay-out
- Theft of ~100 GB of confidential data within a two hour time span
- Halt of pipeline and business operations

2 *Colonial Pipeline (2023, August 17).* About us. https://www.colpipe.com/about-us/our-company

- Major reputational damage
- Federal government involvement and congressional hearings

It also created many follow-on impacts:

- Tens of thousands of people were unable to access gas
- More than 17 states declared a state of emergency
- Gas prices surged for millions
- 45% of pipeline operators were affected
- Airlines and air material transport flights were impacted
- Economic effects rippled from these conditions

Since this cyber breach affected critical infrastructure, it created additional societal impacts. The Indian organisation, NCIIPC, defines critical infrastructure as "any computer resource whose incapacitation or destruction would have a debilitating effect on national security, economy, public health, or safety."

SALT Typhoon

When discussing nation-state threats, it's crucial to acknowledge sophisticated adversaries that operate with extreme patience and stealth. An example of such persistent and covert operations might be found in campaigns attributed to entities sometimes referred to by designations like "SALT Typhoon." These are not typical cybercriminal gangs focused on immediate financial gain. Rather, they represent highly advanced, state-sponsored actors whose primary objective is often to position themselves deep within critical infrastructure networks.

Their methods are characterized by extensive reconnaissance, quiet infiltration, and maintaining a persistent, hidden presence over long periods. They leverage "living off the land" techniques, utilising legitimate tools and functionalities already present within the compromised networks to evade detection and blend in seamlessly with normal operations. The ultimate goal of such groups is rarely instant disruption, but rather to

establish a latent capability—mapping out the network, gathering intelligence, and creating backdoors—to be able to disrupt or destroy vital services like power, water, communications, or transportation, at a moment of their choosing, for strategic or geopolitical advantage.

This method poses a direct and severe threat to India's national security, economic stability, and the physical wellbeing of its citizens, as vital systems could be held hostage or incapacitated without warning by highly capable and patient adversaries.

In light of all of these risks, organisations must undergo continuous technological evolution (a.k.a., digital transformation) to survive and compete. They must adopt technologies that allow them to stay competitive, including securely sharing data with partners and third parties. They must also find safe ways to provide access to applications, the internet, and the cloud to any geographical location.

Why Current Network and Security Infrastructure are Failing

Many organisations spend a significant portion of their IT budget on cybersecurity. Why are they still being breached? Because, even as their other systems undergo digital transformation, they still use traditional cybersecurity solutions that are insufficient for preventing unauthorized access. Security teams often buy dated technologies, reactively patch security gaps, and impulsively adopt new technologies that are ineffective at solving the holistic cyber risk. This slow, reactive approach adds complexities to existing outmoded technologies, and increases operational friction and costs.

Let's dig a bit deeper into why, after spending millions of dollars on network and cybersecurity, organisations are breached. The main problem is that cybersecurity technologies designed in the late eighties and early nineties (and are still used today) are centered on an “implicitly trusting” architecture. This worked fine when everyone’s business networks were not largely interconnected. Leading network hardware and software companies built great technologies that enabled enterprises to extend organisational access to data to every user, branch office and warehouse, factory and supplier, etc.

Then cloud and mobility changed how business was done. Data now lives everywhere and anywhere. Workers require access to resources from any location. Organisations brought their turn-of-the-century networking and security practices into the cloud era and discovered that their technologies did not scale.

In the legacy cybersecurity model, when an employee is granted access to this trusted network, they (or an attacker) can propagate laterally and access every single office, factory, and device under the company's control. Applications are also on the same company network, putting all of an organisation's critical resources in one traversable (or routable, in network speak) space. At the time, these traditional networks represented a big breakthrough for collaboration and distributed computing. Today, their architecture is the equivalent of opening your front door at 3:00 a.m. and letting a stranger wander around freely in your home.

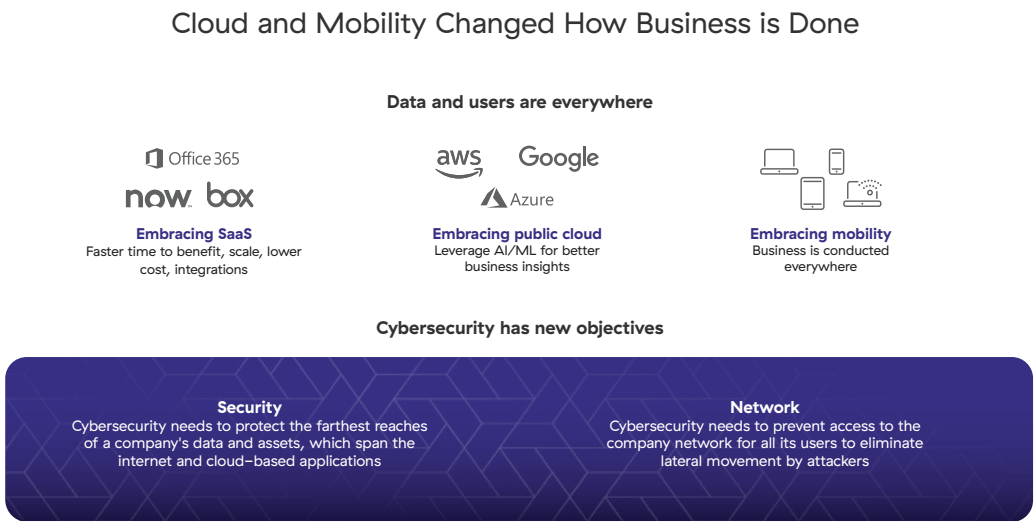


Figure 04: SaaS, public cloud, and mobility have changed network and security objectives.

Firewalls and VPNs are the Problem

Many organisations still have this traditional type of technology in place and are therefore frequent targets of cyberattacks. Firewalls and VPNs most commonly represent these technologies that create an external attack surface for attackers to exploit.

Firewalls were initially deployed to provide the first line of defense against unregulated network traffic, acting as a gatekeeper to segment trusted internal networks from the untrusted internet. They were useful for enforcing access policies and preventing widespread, unmanaged exposure of internal systems to external threats at a time when network perimeters were clearly defined.

However, these firewalls, whether physical appliances guarding an on-premise data center or virtualized instances deployed within cloud environments, fundamentally operate on a perimeter-based security model. Their core function is to allow or deny network traffic based on IP addresses and ports, effectively creating a 'trusted inside' and 'untrusted outside.' This model inherently creates attack surfaces because for legitimate business operations, various ports must remain open, presenting targets for scanning, reconnaissance, and exploitation of underlying application vulnerabilities. Furthermore, once an attacker breaches this perimeter—even if it's a virtualized firewall protecting a cloud instance—they often gain access to a broad segment of the network, enabling significant lateral movement due to the implicit trust given to internal network traffic. The complexity of managing intricate rule sets across these firewalls also frequently leads to misconfigurations, inadvertently leaving critical assets exposed.

Workers are considerably more mobile now, and many work from home. Organisations have tried to adapt by using virtual private networks (VPNs) to extend the company network to each employee's location. While VPNs do offer some level of protection, they have also been the cause of numerous breaches given their public exposure and network-level access.

Their fundamental design is to create an encrypted tunnel, effectively extending the corporate network directly to the user's device, regardless of whether that user is

connecting from a corporate laptop or a personal device over an unsecured home Wi-Fi. This grants network-level access, often providing users with broad permissions to internal systems and applications, far beyond what they actually need. If a user's device is compromised, or their VPN credentials are stolen, an attacker gains direct entry into the internal network, allowing for unfettered lateral movement and access to sensitive resources. Moreover, the VPN concentrators themselves, whether physical appliances or virtualized cloud instances, become high-value targets; they represent a single, critical point of entry whose exploitation can lead to widespread network compromise, exposing the entire enterprise to significant risk.

Couple this with the rapid adoption of public cloud and SaaS. Because traditional architecture puts users and applications on the same network, this means that the company network is now extended to all of those disparate cloud locations as well. As the old network model grows, it creates a huge surface that enables lateral movement for users as well as for attackers.

These older architectures, commonly known as hub-and-spoke networks and castle-and-moat security, are still in place at many organisations today.

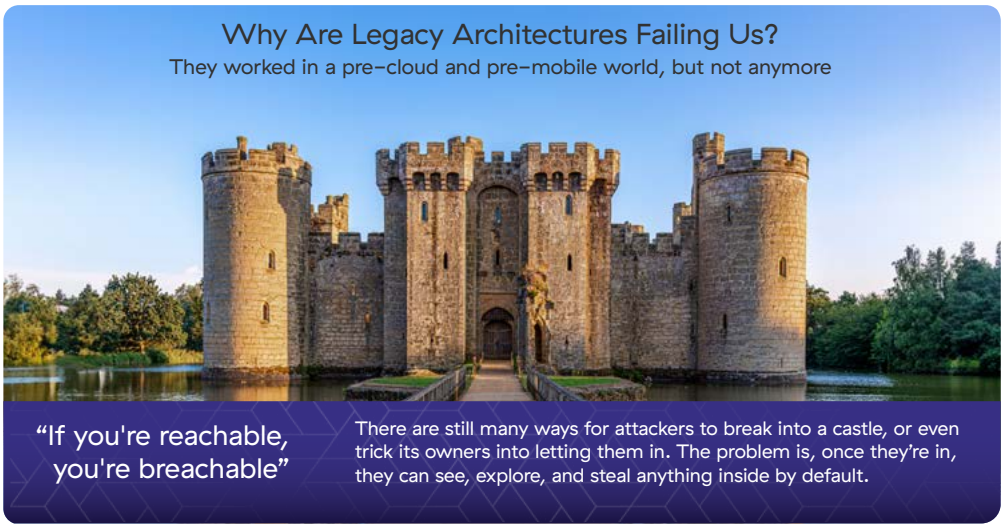


Figure 05: Legacy architectures represent a castle and moat, which fail to provide security in a mobile and cloud world.

Using corporate theft as an analogy, there are four key steps attackers take to breach organisations even after organisations have spent millions of dollars on network and security.

1. **They find your offices (External Attack Surface)** The bad guys find an open attack surface. What is the attack surface? Every implicitly trusting network address discoverable on the internet is an attack surface. Every system with vulnerabilities, like failing to properly encrypt data as it moves around to different people and technologies, can be compromised. If you're reachable, you're breachable.
2. **They break in using a weak entry (Compromise)** The bad guys compromise the network. Every external compromise comes from the internet and looks for weak links, like unsuspecting users or unprotected devices, to compromise. Once an asset is breached, attackers use the compromised resource as a beachhead to launch further attacks.
3. **They search for corporate secrets (Lateral Propagation)** The bad guys get onto a network and move laterally to find high–value targets. Since a VPN is on the corporate network, a hacker can use it to traverse laterally across the enterprise and bring every system or application down. Or they can encrypt data and ask for ransom. Fixing this on a per–vulnerability basis is like trying to build a highway system of toll booths and toll roads to regulate access; this is called network segmentation and it is difficult to accomplish.
4. **They walk away with secrets (Data Loss)** The bad guys steal data. The stolen data is almost always sent to the internet. Data is the crown jewel of organisations, and its theft means a loss of intellectual property, loss of trust among customers, and a negative impact on brand reputation.

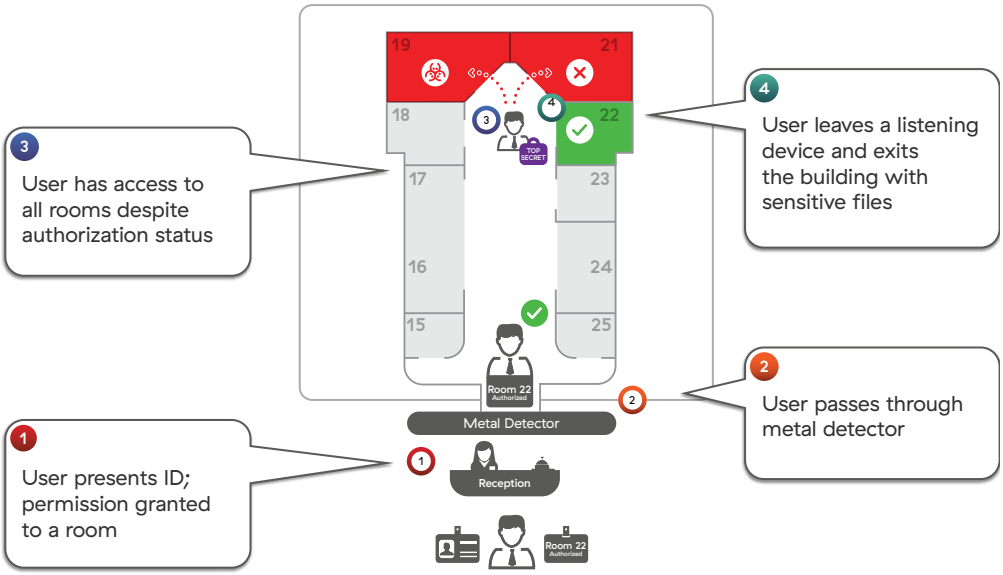


Figure 06: Traditional security is like allowing unescorted visitors to freely wander the entire office building after checking in at reception.

Figure 07: These four factors represent the steps attackers take to breach organisations.

Using Zero Trust to Mitigate Cyber Risk

Once the cyber risk posture of an organisation is determined, it is time to improve it. The first step in minimizing cyber risks is figuring out what to protect. As the adage goes, "If you try to protect everything, you protect nothing," and this is true in cybersecurity. It is important to help the organisation identify the crown jewels and prioritize protecting mission–critical resources. Often, organisations get bogged

down trying to define every detail of a holistic and comprehensive security plan. While this is important in the longer term, some simple steps will greatly improve risk posture for critical assets.

Typically, "crown jewels" can be the organisation's intellectual property, citizen data, financial applications, IoT/OT systems (like factory equipment), or critical applications that drive the business. If compromising an asset would cause a major business impact, it belongs on this list.

Figure 08: Identify, prioritize, and have transparency on what needs to be protected.

Once priority assets are determined, the next step is to address one of the largest security risks to the organisation—the implicitly trusting architecture that has an attack surface, allows for compromise, allows lateral propagation, and can cause data loss. These legacy architectures put users, applications, and data on the same network, exposing them to discovery and exploitation by attackers attempting to breach that environment. Moving away from this implicit trust model requires adopting a Zero Trust architecture (ZTA).

Zero Trust Architecture Defined

So, what is a Zero Trust architecture? Simply put, it is a philosophy (implemented through architecture and technology) that rejects the implicitly trusting model of legacy architecture by taking a "never trust, always verify" approach. In addition to

verifying the user's identity, ZTA considers what information the user is trying to access, and grants access based only on what the user must have, a principle known as least privilege. When deployed, the external attack surface and lateral propagation can be minimized, reducing the chance of data loss and compromise.

Figure 09: Characteristics of Zero Trust architecture.

To understand Zero Trust architecture, think of technology applications (and their data) as falling into two buckets:

- Private applications are managed internally by the IT department. These are often hosted in a company's data centres or in public clouds offered from Microsoft, Amazon, or Google, etc. There is plenty of sensitive data stored within private applications.
- Public applications are managed by entities external to the organisation. These are SaaS software applications provided by companies like Microsoft, Salesforce, ServiceNow, or Workday. These public applications often used in the open internet will also have access to sensitive company data.

Since both of these application types store mission–critical and often sensitive data, users/devices, things (IoT/OT), and cloud workloads need to access them. By default, they're all untrusted in a Zero Trust environment. The biggest difference between a

Zero Trust architecture and traditional architecture is that with ZTA there is no directly accessible and trusting network between the user and the application. How do they connect? They go through a secure Zero Trust cloud, which acts as a switchboard that allows various entities (users, devices, and applications) to securely communicate with each other over any network. Users cannot see data they're not allowed to access, cannot move around to other technologies within the organisation, and are governed and monitored to detect attempts to misuse resources.

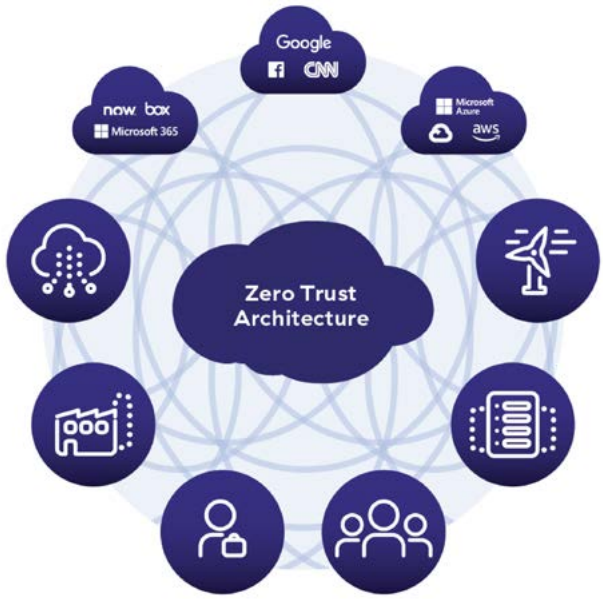


Figure 10: Zero Trust Architecture (ZTA) connects users to the resources they need in a secure way with no attack surface or risk of lateral propagation.

ZTA does several things to ensure security and reduce risks when connecting users to the applications and data. First, it stops every connection request with a verification check asking who they are, what they want, and where they are going. This is part of identity and access management, where technologies like multifactor authentication (MFA) help to prevent credentials from being stolen.

Then, it evaluates the risk of the request (e.g., is the requestor asking for something outside of their job function?) and whether there are controls in place to automatically derisk the requests. Overly risky users may be blocked.

Next, it enforces policy by only connecting users to applications that the organisation has authorized based on business policy (e.g., only HR employees have access to Workday while sales employees do not). This eliminates the risk of lateral propagation to other applications or data because ZTA enforces policy for all of these requests. The typical difficulties of achieving network segmentation go away, as this is now being monitored at a user–to–application level.

Finally, ZTA creates a secure, outbound–only connection to the requested resource, without exposing the underlying trusting network. Application and data transactions are hidden from view, hence no more network attack surface. Well–designed Zero Trust architecture can perform these actions for every transaction (often billions per day) without the user ever noticing.

Figure 11: Steps that a Zero Trust architecture (ZTA) takes before connecting a user to reduce the risk of a cyber breach.

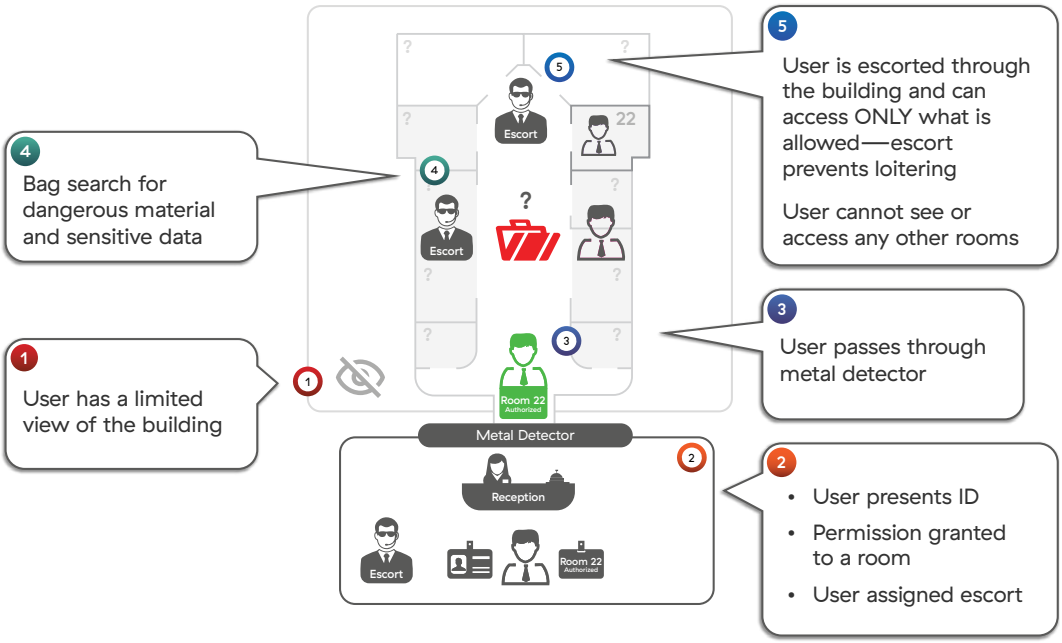


Figure 12: Corporate theft prevented in a Zero Trust architecture.

Looking back at the corporate theft example in Step 2, Zero Trust architecture would produce a significantly different outcome. Let's look at the same scenario with a Zero Trust solution.

Zero Trust is more than a technology; it is a strategy and a framework guided by a new way of thinking that permeates across a number of areas. It involves many practical implementations from vendors that built solutions with Zero Trust at their core. The preceding section described just that. Once deployed, this technology forms the basis of providing secure access for users, things, and workloads to public or private destinations based on Zero Trust principles.

Focusing on the four areas of risk discussed earlier, Zero Trust helps in the following ways:

Figure 13: Zero Trust solves the four ways that cyber breaches can occur.

Zero Trust has already made an enormous impact on many organisations. It proved especially valuable as the pandemic moved workers home, expanded the business network, taxed IT resources, and opened the door to new cyberattacks. Organisations that transitioned to ZTA enabled seamless WFH access, while avoiding the common bottlenecks and security concerns that would normally accompany such a massive workforce shift. That being said, many organisations are still in various stages of their transformation journey.

Zero Trust architecture has been endorsed by US government agencies NIST (800-207), Cybersecurity and Infrastructure Security Agency (CISA) (Zero Trust Maturity Model), and the Department of Defence (DoD) (Zero Trust Reference Architecture), as well as by the Indian Computer Emergency Response Team (CERT-In), part of the Government of India's Ministry of Electronics and Information Technology in their 'Guidelines on Information Security Practices for Government Entities'.

This groundswell of endorsement for Zero Trust architecture reflects an acknowledgement of the challenges of traditional architecture and Zero Trust's ability to mitigate those challenges. As such, companies and their boards should pay special attention to these trends, especially those organisations that do business with the government.

Enhanced Security Posture and Compliance

Inadequate or burdensome security and compliance practices/configurations increase your risk of ransomware, malware, viruses, phishing, and compliance violations.

Sample Benefit

85%
reduction in successful ransomware, phishing, and other malware/viruses

25%
reduction in the risk of a data breach

Technology Cost Optimization

- Internet/security appliance simplification
- Reduce/eliminate hardware capacity planning/renewal
- Network simplification/local internet breakout

Sample Benefit

75%
reduction in hardware appliance costs

50%
reduction in network spend

User Experience

- Reduce latency by eliminating network backhauling
- Prioritize critical apps traffic with bandwidth control
- Optimize M365 and other SaaS

Sample Benefit

30–40%
reduction in inbound/outbound transaction wait times (user productivity hours)

Operational Efficiency

Optimizing FTE time and reducing contractor costs due to break/fix; OS/firmware updates; patching; refresh cycles; change management scheduling.

Sample Benefit

50%
reduction in effort managing inbound/outbound internet security appliances (new and existing sites)

Mergers and Acquisitions

- Accelerate M&A
- Rapidly onboard acquired employees, including analysis of security access and policies

Sample Benefit

2–3X
Faster M&A time-to-value
Improved UX and productivity
Superior security posture

Sustainability/Carbon Footprint

- Improve your enterprise's Environmental, Social, and Governance measures, reporting, and scores.

Sample Benefit

50%
power usage effectiveness (PUE) improvement: reduce shipping, receiving, and replacement parts

Reduced
CO_2 emissions from power and cooling

Figure 14: Zero trust architecture brings about a broad array of business benefits.

In addition to the enhanced security posture discussed above, Zero Trust architecture has a number of other business benefits, including technology cost optimization, operational efficiencies, improved user experience, streamlined mergers/acquisitions/divestitures (M&AD), and improved sustainability. Special note should be paid to technology cost optimization, as Zero Trust architecture can eliminate a number of expensive and outdated point products, resulting in significant cost savings.

Using Zero Trust for Data Security

Data is the lifeblood of modern critical infrastructure, from operational blueprints and SCADA control logic to national intelligence and citizens' personal data. Safeguarding this information from compromise—leakage, exfiltration, or improper storage—is paramount for national security and public trust. The challenge is that sensitive data resides everywhere: in motion, at rest in the cloud, and in active use on devices, often beyond direct control. Protection requires a pervasive strategy that accounts for every potential vector of exposure, ensuring integrity and confidentiality throughout its lifecycle.

Safeguarding this information from compromise—leakage, exfiltration, or improper storage—is paramount for national security and public trust.

A modern Zero Trust architecture (ZTA) provides sophisticated data protection, starting with securing data in motion. This involves intelligently inspecting and controlling data as it flows across all digital channels (internet, cloud, internal systems). The architecture actively identifies sensitive information, such as classified documents, and enforces granular policies to prevent unauthorized sharing or exfiltration. This ensures sensitive data never leaves the controlled environment, safeguarding against accidental disclosures, malicious insider threats, or external theft attempts through seemingly legitimate channels.

Extending this, the ZTA also ensures the protection of data at rest. As critical infrastructure leverages cloud platforms, it creates a significant potential for exposure from misconfigurations or inadequate controls. The Zero Trust approach continuously discovers and classifies sensitive data across cloud repositories (databases, storage buckets). It identifies and remediates configuration vulnerabilities and policy violations that could expose vital national information, ensuring stored data is constantly verified for its security posture.

Furthermore, ZTA extends its vigilance to data in use on endpoints. For managed devices, it ensures only authorized and compliant endpoints can access sensitive data, continuously verifying device health and user identity. Access is limited to precisely what is needed for the task at hand. For unmanaged devices, it either prevents access or severely restricts capabilities to a highly isolated environment, effectively eliminating the potential for data compromise from untrusted devices.

In this era of advanced analytics, protecting AI data is critical. The data used to train AI models, the models themselves, and their valuable inferences are vital assets for national decision–making.

Finally, in this era of advanced analytics, protecting AI data is critical. The data used to train AI models, the models themselves, and their valuable inferences are vital assets for national decision–making. A Zero Trust architecture safeguards AI data throughout its lifecycle: securing sensitive training datasets (data at rest), protecting the intellectual property of the models (data in motion), and securing the outputs and insights (data in use). This integrated approach ensures India's strategic AI initiatives are built on secure, trusted data, thus protecting the nation's digital sovereignty.

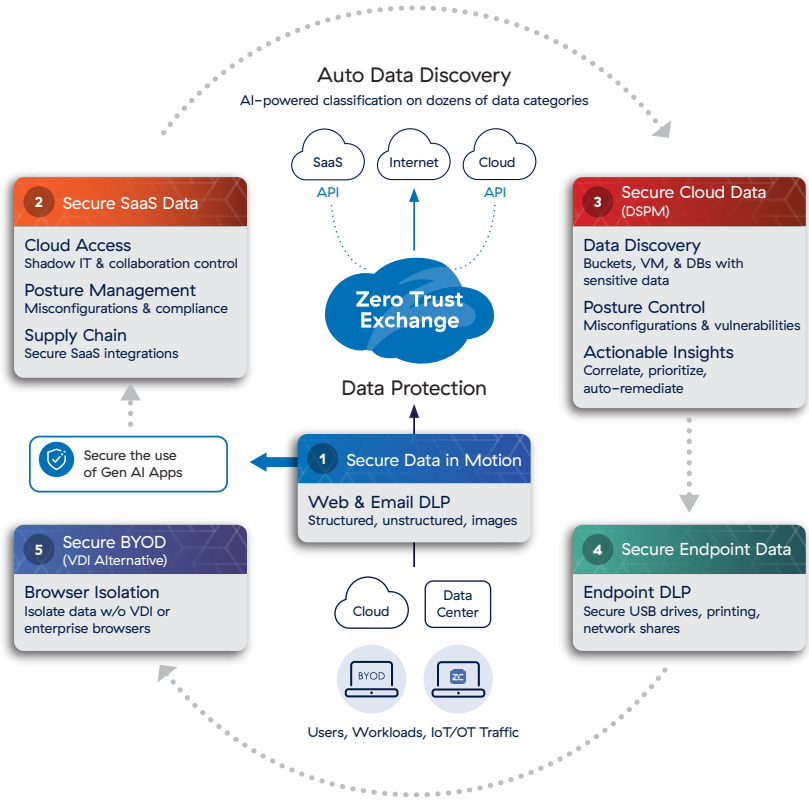


Figure 15: Zero Trust provide Robust Data Protection

Zero Trust and the Digital Personal Data Protection (DPDP) Act

India's ongoing digital revolution, marked by population-scale platforms and deeply interconnected Critical Information Infrastructure, is governed by the stringent requirements of the Digital Personal Data Protection (DPDP) Act 2023. The DPDP Act establishes a clear statutory obligation on organisations to protect digital personal data through reasonable security safeguards, ensure purpose limitation, enable accountability, and respond swiftly to personal data breaches. While the Act is technology-neutral, its requirements implicitly demand a shift away from legacy, perimeter-based security models that assume trust once access is granted.

Zero Trust architecture provides a practical and scalable way to operationalize DPDP compliance. At its core, Zero Trust enforces least-privilege access, which means that users, devices, and workloads are granted access only to specific applications and data required for a defined purpose. This directly supports DPDP principles of data minimisation and purpose limitation, reducing unnecessary exposure of personal data across systems.

Zero Trust also enables continuous verification and monitoring, ensuring that access decisions are reassessed in real time based on identity, device posture, and risk context. This strengthens an organisation's ability to demonstrate accountability and maintain accurate access logs, a key expectation under the DPDP framework.

Zero Trust architecture provides a practical and scalable way to operationalize DPDP compliance.

Importantly, Zero Trust architectures are designed to limit lateral movement and blast radius. In the event of a compromise, attackers are prevented from traversing networks to access large volumes of personal data. This containment capability materially reduces the likelihood and impact of reportable personal data breaches, supporting breach-notification obligations under the Act and Rules.

In this sense, Zero Trust is not merely a security enhancement, it is an architectural enabler of DPDP compliance, aligned with India's digital-first governance model.

DPDP Act and Zero Trust: Compliance Beyond Documentation

By Dr. GK Goswami

Data is the new oil, and trust has emerged as the most credible digital currency. Data protection symbolizes privacy, dignity, economy, national sovereignty, and citizen empowerment. With the rise of cloud-led architectures, AI-driven systems, and autonomous decision engines, traditional perimeter-based security frameworks became redundant. Cybersecurity remains a citadel for data protection.

The DPDP Act, 2023 institutionalizes accountability and trust by recognizing privacy as a fundamental right and mandating purpose limitation, data minimization, transparency and reasonable security safeguards. While the Act provides civil remedies and imposes stringent penalties for non-compliance, mere legal documentation or policy declarations are inadequate. Compliance with a robust security framework remains illusory, especially in the era of Cybercrime-as-a-Service (CaaS) and AI-enabled agentic criminal networks.

Zero Trust architecture (ZTA), premised on "never trust, always verify," operationalizes DPDP obligations through security by design, a global necessity. By enforcing least privileged access, continuous authentication, and micro-segmentation, ZTA transforms legal mandates into enforceable technical controls. The interface reflects a convergence of law, technology, and governance, converting DPDP from a policy regulatory framework into a living cybersecurity doctrine. DPDP defines responsibility, while ZTA ensures trusted digital security.

Contributed by:

Dr. GK Goswami, IPS,
Expert on Interface of Law & Technology
Director UPSIFS

CHAPTER
2

Understanding and Mitigating AI Risk

Understanding AI Risk

This chapter sheds light on how AI is reshaping the cybersecurity landscape and offers a call to action for leaders who manage Critical Infrastructure. It urges organisations to adopt secure-by-design, Zero Trust principles at every phase of AI deployment. Leaders must thoroughly assess AI risks, build strong governance frameworks, and embed security considerations into strategic priorities.

When it comes to AI, we are standing on the edge of what can only be described as a "Giga Wave"—a massive transformation that will redefine the way industries and government digitally operate.

Just as the Industrial Revolution reshaped societies over the course of 150 years, the AI Revolution is poised to fundamentally alter how we live and work with incredible speed. The creation of the Internet, cloud computing, and mobile technology certainly transformed how we engage with the world, but those changes came gradually, evolving over decades. By contrast, AI is driving change at an accelerated scale and speed, compressing decades of transformation into mere years. The stakes have never been higher.

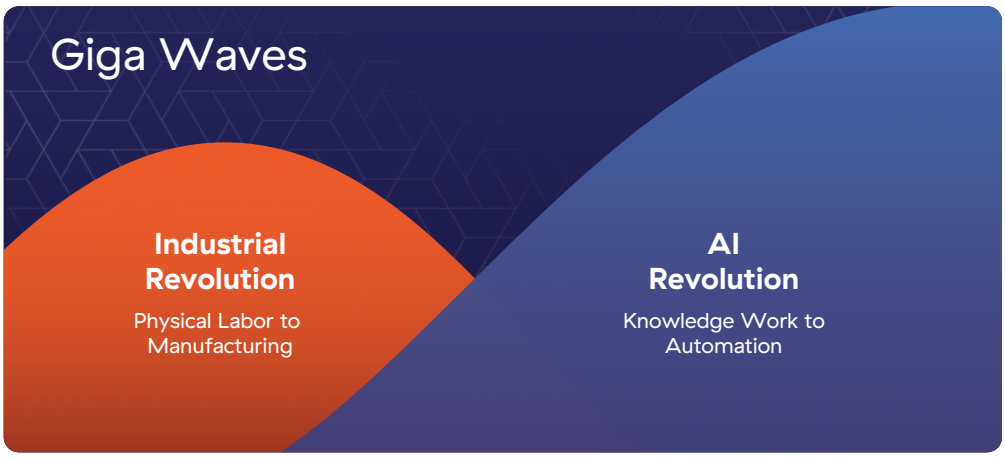


Figure 16: The AI Revolution represents a Giga Wave akin to the industrial revolution

For all the potential benefits of AI, the risks—when not handled correctly—can cause significant harm. It is crucial to understand the opportunities, risks, and governance responsibilities related to AI, on par with understanding the nuances of finance, cybersecurity, legal compliance, or mergers and acquisitions. And while there is a cost associated with exploiting the opportunities AI offers, the cost of doing nothing may be far greater.

The rapid acceleration of AI over the past three years has been driven by advancements in computing power, smarter algorithms, and access to vast amounts of data. Improved hardware has made AI cheaper and faster to run, while strong demand from businesses and massive investments by governments and tech companies have fueled innovation. Collaboration and knowledge-sharing across the global AI community have also pushed progress forward, making AI more powerful and widely accessible.

It is crucial to understand the opportunities, risks, and governance responsibilities related to AI, on par with understanding the nuances of finance, cybersecurity, legal compliance, or mergers and acquisitions.

Recent breakthroughs have vaulted new types of AI into the mainstream. Generative AI opened the door for content creation (text, images, audio, and video) at scale when OpenAI launched the generative AI boom by making ChatGPT publicly available in 2022. Large Language Models (LLMs) and Natural Language Processing (NLP) quickly entered the fray, enabling cybersecurity tools to interpret threats in human-like ways. This new class of solutions aren't just detectors; they're assistants that generate reports, simulate attacks, and proactively suggest remediations.

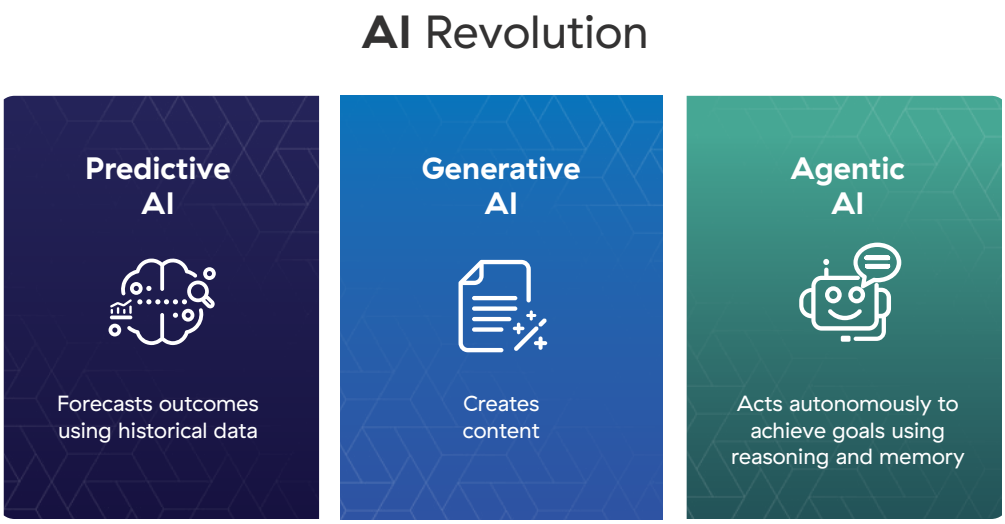


Figure 17: AI has evolved from Predictive to Generative, and ultimately Agentic

Now, agentic AI has moved AI into an era where intelligent systems can act autonomously to solve problems, achieve goals, and drive efficiencies across industries.

This explosion of capability enables organisations to accomplish extraordinary things, and also creates new risks and threats. For example, if autonomous agentic AI makes incorrect decisions in finance, healthcare, manufacturing, or other industries, it could trigger a cascade of consequences, from unauthorized trades to potentially life-threatening errors. There is also the question of IP and privacy. As AI models train on massive datasets, protecting sensitive information from potential misuse has never been more critical.

AI is a double-edged sword; it both creates risks and also helps forward-leaning organisations reduce risks and protect against threats. For instance, AI can identify and block attacks before damage is done. Advanced systems are even able to predict potential breaches before they occur by understanding the earliest stages of attacker activity and extrapolating how it is likely to unfold based on learnings from previous incidents. Leveraging AI for cybersecurity is no longer optional—it's necessary for organisations to stay ahead of threats.

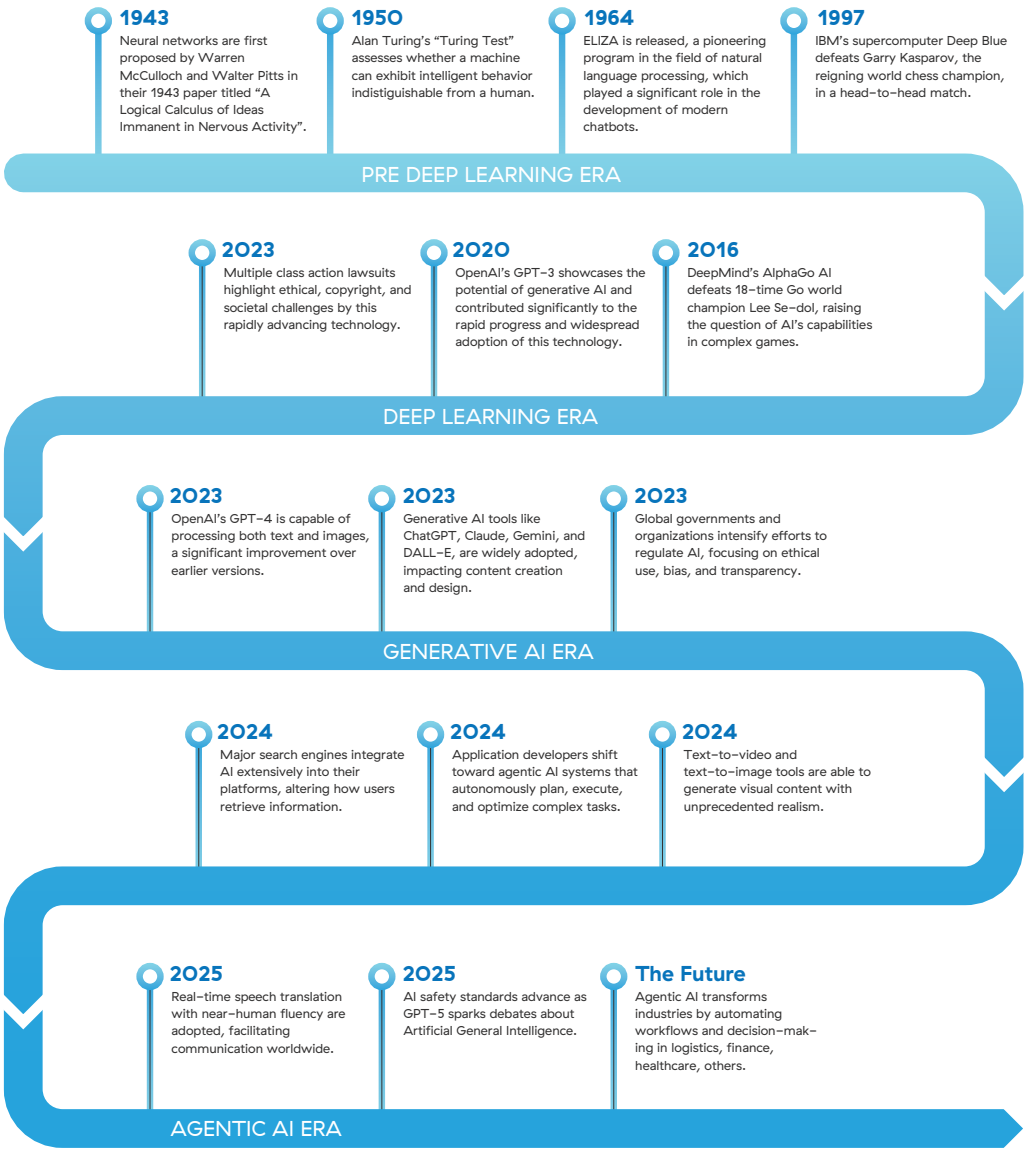


Figure 18: Evolution of AI from the pre-deep learning era to the modern era

For India, the national strategy for mitigating AI risk is formalized under the IndiaAI Governance Guidelines, which champions the vision of "Safe and Trusted AI." This key pillar of the IndiaAI Mission focuses on ensuring responsible AI by setting expectations for data governance, algorithmic transparency, and risk management, particularly for AI systems deployed in critical areas like large-scale public services and financial systems. A key aspect of this governance ties AI adoption closely to the country's Digital Public Infrastructure (DPI), ensuring foundational resources, such as data, compute, and model ecosystems are securely and equitably managed for responsible development and use.

From a risk perspective, several critical AI use cases warrant attention:

1. **Defending against AI-driven threats.** Cyberattackers are using AI to rapidly assess the attack surface, scale operations, automate sophisticated ransomware, and craft convincing phishing schemes. This includes creating deepfakes of executives to enable monetary fraud. Leaders must ensure defence infrastructure can respond fast enough, which may require using AI internally to detect and preempt such attacks, thus strengthening the company's overall cyber defences.

2. **Responsible AI development and deployment.** Leaders must oversee the secure and ethical design, implementation, and governance of AI systems used by employees, suppliers, and citizens/customers. This includes ensuring that AI applications align with business goals, meet ethical and regulatory standards, and operate within defined risk tolerance limits.

3. **Managing employee use of AI tools.** Employees increasingly rely on both private AI technologies (trained on proprietary and public datasets) and public AI systems (e.g., ChatGPT, Claude, and Llama). Leaders must verify the existence of robust policies to prevent data leakage, compliance breaches, and unauthorized access to sensitive information, particularly when interacting with external large language models (LLMs). Role-Based Access Control (RBAC) and other measures should be in place to enforce boundaries and mitigate risks to proprietary data.

The risk landscape, much like AI, will continue to evolve. In particular, supply chain risks of AI vendors and partners will have an outsized impact on organisations if the associated risks are not assessed and planned for.

The introduction of AI requires leadership commitment, organisational accountability, and an operating model designed to deliver both opportunity and security. Leaders who do not actively engage with AI oversight will expose their organisations to both heightened cyber risks and to falling behind competitors in the race to harness AI's transformative power.

Impacts of AI on Cybersecurity

AI's Transformative Impact and Evolving Corporate Cyber Risks

The very features that make AI so appealing—namely, its ability to ingest massive datasets, identify patterns, and automate processes—also introduce significant risks that can be difficult to quantify, especially in the area of cybersecurity. These risks pose profound governance challenges for leaders and demand thoughtful strategies that balance the desire to exploit AI's potential with the need to strengthen enterprise security. Without a firm foundational knowledge of both AI and cybersecurity, overseeing the risks and understanding the implications of decisions made by management will be difficult.

Defending Against AI-Driven Threats

Leaders are familiar with the ever-changing cyber threat and risk environment. New attack techniques can leave networks dangerously exposed to ransomware, data theft, operational disruption, and even destruction. The rapid rise and widespread access of AI tools, many of which lack guardrails to prevent misuse, has tipped the balance of power towards the attackers and set the stage for a new era of AI-powered cyberattacks.

Generative AI models have greatly improved the accuracy, targeting, and scale of cyberattacks, while reducing the cost and skills needed to conduct attacks.

Unsophisticated hackers can now access capabilities that were once reserved for only the best-funded, nation-state groups. Simultaneously, those at the top end of the scale have significantly increased their capabilities; we must assume they now have access to hardware capabilities at least as powerful as those of the defenders.

One of the most common starting points for network compromises is a phishing email, which mimics a legitimate brand or known sender to convince the target to take an action. For example, clicking on a link to a malicious website, downloading and opening a file, or taking another action that enables subsequent phases of an attack. Even the most wary employee may fall victim to a well-timed email from an expected sender that contains content relevant to the recipient.

This sophistication goes even further: generative AI can create convincing fake websites, complete with authentic-looking branding, to deceive victims and steal their login credentials. Cybercriminals use these polished sites in conjunction with phishing campaigns, luring unsuspecting users to click malicious links.

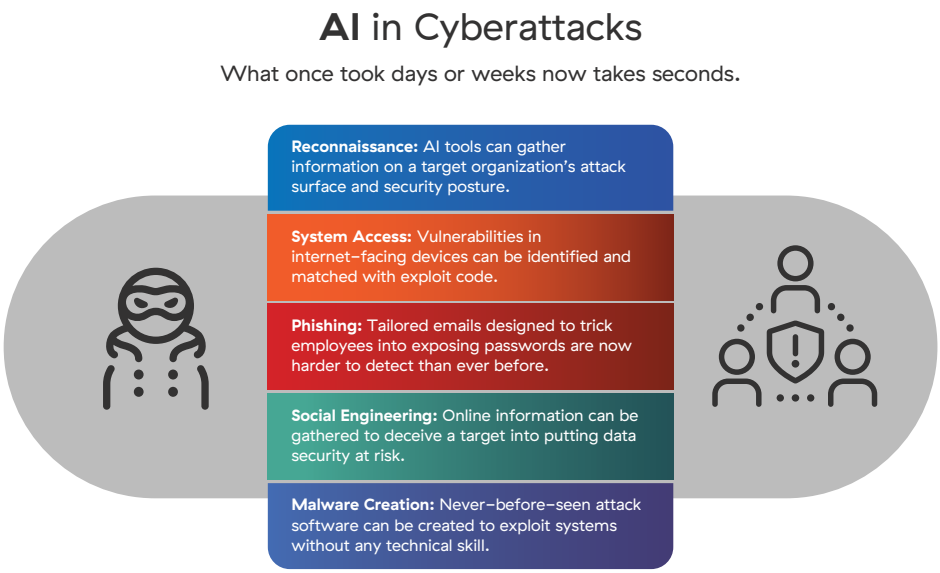


Figure 19: AI has been weaponized in various ways by cyber attackers

By automating the creation of imitation websites within seconds, generative AI drastically simplifies and accelerates attackers' workflows, making their schemes more efficient and harder to detect.

GenAI-enhanced malware and social engineering in North Korea (DPRK) linked campaigns

- Campaign named "Contagious Interview" (Linked to the broader DPRK IT Worker scheme).
- Threat actors fabricated sophisticated digital identities and fake personas, utilising deepfake voice/video manipulation to bypass vetting processes during remote interviews.
- AI-Generated Study Guides: They leveraged GenAI to create extensive instructional playbooks for technical interviews, with some "study guides" over 70 pages long.
- AI-Assisted Malware: Malicious scripts deployed showed distinct indicators of AI-assisted coding, including meticulous formatting and a notable use of emojis.

Source: Zscaler ThreatLabZ

AI is also a powerful tool for hackers seeking to breach a network's security. Some AI programs are capable of scanning the internet to identify IP addresses linked to a target company, analyse firewalls and VPNs for vulnerabilities, and pinpoint weaknesses with remarkable efficiency. What once required hours, days, or even weeks of manual effort—reconnaissance and mapping of a target's attack surface, collecting entry points to exploit—can now be accomplished in mere minutes. By automating these processes, AI enables attackers to streamline their operations and launch highly targeted attacks with unprecedented speed and precision.

Once potential entry points are identified, AI can also assist in writing exploit code, creating malware designed to evade detection tools, and generating deceptive scripts capable of overwhelming security teams. Attackers have little to lose in experimenting with these tools; at worst, any given attack is detected and blocked, and the attacker simply tries again. The old adage holds as true today as ever: defenders must succeed every time in detecting and stopping attacks, while attackers need only to be lucky once to breach a system.

Defenders must succeed every time in detecting and stopping attacks, while attackers need only to be lucky once to breach a system.

One especially damaging AI capability is voice and video cloning of individuals—specifically company leaders. While most employees are very aware of email security risks after countless cybersecurity awareness training sessions, many will be less likely to question the CEO's voice on the end of a phone call, much less the CEO's face on a video call.

These attacks typically rely heavily on psychological pressure to manipulate employees into complying with fraudulent requests. Employees are conditioned to follow instructions from senior leaders like a CEO or CFO, and a deepfake voice or video call from a supposed executive can bypass an employee's normal skepticism. Scammers present a high-pressure, urgent scenario, such as a confidential deal or an overdue vendor payment, which discourages the victim from taking time to verify the request.

Free online applications now allow for the real-time creation of deepfake audio and video using publicly available photos, presentations, speeches, social media accounts, and videos as learning material. Each day, accuracy and believability improve while detection becomes harder. The scale and sophistication of these tools give a chilling glimpse into how AI is aiding attackers, creating an urgent need for stronger defences.

Responsible Development and Deployment and Managing Employee Use of AI Tools

AI's role in cybersecurity is particularly critical: While AI tools offer powerful capabilities for detecting threats, automating responses, and analysing vast amounts of data in real time, they also introduce unique risks if not developed and deployed responsibly. Understanding AI is essential for managing organisational risks and ensuring ethical practices.

Responsible AI development requires careful attention to security, while responsible deployment demands rigorous oversight to prevent misuse or unintended consequences. In the context of cybersecurity, the stakes are especially high: AI systems must be aligned not only with organisational goals, but also with broader regulatory and ethical standards. This section explores the complexities of navigating AI in the enterprise, ensuring it is both a force for innovation and a safeguard against evolving threats.

The use of public large language models (LLMs) introduces new and complex risks that leaders must carefully manage. These include ChatGPT, Gemini, and private LLMs trained on company data that are intended only for employee use. Their use creates substantial potential for unmanaged risks that may lead to legal or reputational issues.

There are four critical areas where risks emerge:

- **End Users and Public LLMs**. When employees interact with public AI systems, risks include data exposure and harmful outputs.
- **Developers and Private LLMs.** Challenges posed by private models include the risk of vulnerable code and improper access to sensitive data.
- **Data Security of Public vs. Private LLMs.** When employees and leaders are unclear about the differences between public and private AI infrastructures and how they impact control over corporate information, risks can rise.
- **Hallucinations, Injections, and Toxicity**. These inherent AI behaviors pose risks of misinformation, exploitation, and harmful content.

By recognizing these risks, directors will gain greater clarity on how enterprise AI adoption must be anchored in robust governance, security, and oversight frameworks.

End Users and Public LLMs

In an era of productivity–driven urgency, employees often seek tools that streamline their workflows. Public LLMs offer a tempting shortcut for drafting documents, summarising reports, or brainstorming ideas. Yet these interactions can inadvertently expose sensitive corporate data to privacy risks. For instance, an employee interacting with a public chatbot may unknowingly upload regulated or proprietary information, making it susceptible to leaks or future misuse in public model training. Once data has been submitted to a public LLM, there is no delete button.

Another concern lies in harmful content output. An employee consulting a public LLM could receive inaccurate, biased, or toxic recommendations, potentially destabilizing workflows or contributing to poor decision–making. Without controls in place, the risks inherent in public LLM engagement could lead to widespread consequences for enterprises.

Developers and Private LLMs

Developers using private LLMs encounter challenges on two fronts: one procedural and one technical. First, an over–reliance on the perceived "expertise" of private LLM–generated outputs could lead to software vulnerabilities—for example, if code suggestions are incomplete or inaccurate. Developers who fail to validate AI outputs may inadvertently introduce exploitable flaws into critical systems.

Second, data privacy concerns loom large. Private LLMs that help developers generate code often require training on corporate data, but lack safeguards to ensure this data is appropriately compartmentalized. Developers or even users querying the LLM might inadvertently gain access to sensitive sales, strategy, or HR information—data they wouldn't typically have clearance to view. Systems that fail to segment information appropriately are prime targets for misuse or malicious exploitation.

Companies developing private LLMs and chatbots that are customer-facing must also evaluate similar risks. They must model situations in which users maliciously use prompts to get confidential or competitive information, and also have a way to deal with toxic or improper responses.

Data Security of Public vs. Private LLMs

At the crux of enterprise AI adoption lies the distinction between public and private LLM configurations. Public LLMs often inadvertently assimilate corporate data into their training pipelines, raising risks that proprietary information may become accessible to external users. Misconfigured permissions or improper oversight compound this risk, leaving sensitive data exposed to third-party AI systems.

Related, so-called 'shadow AI' presents a growing risk to organisations as it involves the unsanctioned use of public LLMs and artificial intelligence tools, such as generative AI apps, by employees without proper oversight or security measures. Users access unblocked apps from corporate devices or use personal devices to circumvent policies.

These tools can expose sensitive data, intellectual property, and compliance-related information to vulnerabilities, creating potential entry points for breaches or data leaks. Without visibility or governance, shadow AI disrupts unified security strategies, increases the risks of regulatory non-compliance, and complicates incident response, making it critical to address and manage proactively.

Private LLMs theoretically resolve this issue by training models on controlled datasets and limiting access to internal users. Yet even these models raise critical governance challenges. Without clear permission structures, corporate data may be inadvertently exposed to employees who query LLMs for information they should not be able to access. AI configurations must replicate real-world boundaries and fragment data access accordingly, ensuring compliance with industry standards. Private LLMs used to enable customer-facing chatbots face similar issues.

A study from MIT found that 90% of employees frequently use personal AI tools, posing a substantial risk of critical data loss. The researchers identified the emergence of a "shadow AI economy," where employees rely on personal AI subscriptions and other publicly available tools to carry out significant portions of their work. This behavior goes beyond casual experimentation: employees are integrating these personal and unprotected tools deeply into their workflows, using AI multiple times every day to accomplish their weekly tasks.

Figure 20: Source: https://mlq.ai/media/quarterly_decks/v0.1_State_of_AI_in_Business_2025_Report.pdf

Hallucinations, Injections, and Toxicity

AI outputs inherently rely on probabilistic estimates, meaning every response is, in essence, a hallucination or, more accurately, a machine-generated guess based on statistical patterns. While many outputs align closely with expected results, others may deviate significantly, creating misinformation that disrupts workflows or impacts decision-making.

AI systems are also vulnerable to prompt injections—situations where malicious actors design input queries specifically meant to override the AI's programmed safeguards. Such exploits could coax systems into releasing information they should protect or performing inappropriate tasks. Finally, the risk of toxic or biased responses must not be ignored; poorly curated datasets or adversarial inputs may lead to harmful AI outputs that tarnish company or leadership reputations or alienate stakeholders.

AI makes a profound impact on the enterprise, presenting opportunities to vastly improve organisational performance and introducing new or amplified risks that

demand careful navigation. From empowered attackers leveraging AI tools to new vulnerabilities introduced through end-user and developer adoption of LLMs, the challenges of securing corporate systems in the age of AI are multifaceted.

For leaders, there is a significant risk of inertia stemming from uncertainty: How do organisations balance the promise of AI innovation with the complexities and costs of safeguarding its implementation? What happens when the unknowns outweigh the clarity of outcomes?

To move forward, leaders must recognize the importance of laying solid foundations for AI deployment. Zero Trust principles—focused on verifying access at every level, limiting privileges, and prioritizing data integrity—provide essential guardrails for successfully exploiting AI's potential while mitigating risks. Leaders must drive conversations about reshaping governance, rethinking security policies, undertaking due diligence to select the right partners, and committing the necessary resources to ensure that data remains the cornerstone of enterprise AI.

Using Zero Trust to Mitigate AI Risk

Traditionally, Zero Trust has focused on securing users, applications, and workloads by removing all forms of implicit trust and employing a "never trust, always verify" model. However, this focus must expand as AI becomes a core part of business applications and how users interact with them, as well as how AI agents replace the traditional view of a human user.

In the next frontier of "Zero Trust everywhere," enterprises must extend the Zero Trust model not just to human users, but also to AI agents, IoT/OT systems, and even the LLMs that underpin today's AI applications. AI agents, much like humans, need secure access to specific systems, policies for appropriate use, and visibility around how data is accessed or altered. This isn't only important for securing systems—it's also critical for securing a dynamic ecosystem of human and autonomous actors.

Figure 21: Zero Trust plays a key role in AI security

Any interaction between a human and/or AI agent with an application (AI or otherwise) must be protected by a Zero Trust architecture (or Zero Trust exchange, as seen below). And, the Zero Trust exchange must also be enhanced by AI, in its own right.

In this way, Zero Trust architecture is useful for three specific risks that relate to AI:

1. Incorporating AI elements into Zero Trust architecture is required to counteract the increased weaponization of AI by attackers.
2. Enabling specific users to connect to specific resources to protect organisations from the loss of sensitive data into public LLMs, and align to AI policy, while scanning for sensitive prompts and files.

3. Protecting organisations and their employees/customers from the improper or dangerous use of private LLMs and chatbots.

Leaders are well-advised to ensure that Zero Trust is being used in these three ways.

Defending Against AI-Driven Threats

The primary action for leaders is to deploy cybersecurity solutions, specifically solutions based on Zero Trust, that have not only heavily incorporated AI, but also have a strong roadmap for AI enhancements. Here are a few examples of how Zero Trust platforms are leveraging AI:

AI-Augmented Suspicious Behavior Detection

AI models can analyse behavioural patterns across users, applications, and devices in real time to identify atypical behavior (e.g., unusual login times or unexpected data flows) and flag potential threats, even if no signature exists. As AI is increasingly used to generate deepfake emails, fake login pages, and cloned apps, it can also detect AI-generated phishing domains.

AI-Augmented Zero Trust Policies

AI can be used to analyse application usage patterns across the network. By learning how users interact with applications, the AI can help create automated application segmentation policies tailored to specific needs. These policies ensure that access to applications is tightly controlled, limiting exposure only to authorized users and minimizing the attack surface. This approach improves security by dynamically adapting to usage patterns and reducing the risk of unauthorized access or lateral movement within the network.

AI-Augmented Data Loss Prevention

AI can be used to enhance data classification by analysing patterns, context, and content within organisational data. It automatically identifies and categorizes sensitive information, such as personal data, financial records, or intellectual property, based on predefined policies or learned insights. This enables more effective enforcement

of Data Loss Prevention (DLP) rules by ensuring that sensitive data is protected, flagged, or restricted when transmitted, accessed, or shared inappropriately. Through continuous learning, AI helps maintain accurate classifications and adapts to new data types or usage patterns, strengthening overall data security.

Looking into the near future, innovations in agentic AI have created promising new use cases. Layered on top of the data and telemetry collected by Zero Trust architecture, use cases like threat detection and response can be reimagined in powerful ways. For example, agentic AI can reduce the time it would take a human security operations centre (SOC) analyst to respond to a threat from 30–40 minutes to three minutes. The SOC analyst still plays an important role in validating the threat and response, but these measures shrink the time between identification to remediation to reduce the likelihood of a damaging incident.

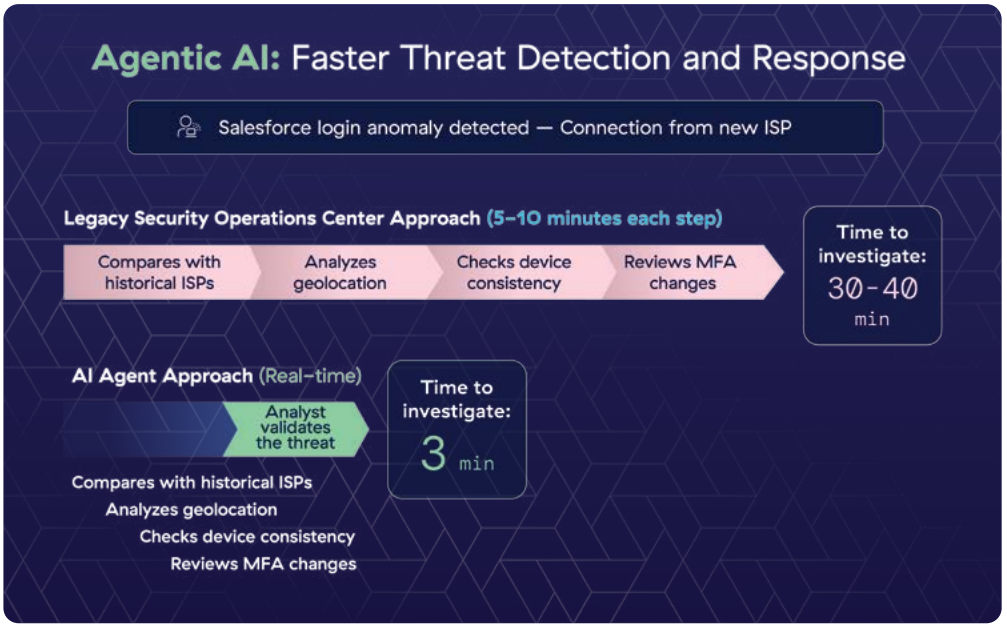


Figure 22: Example scenario where agentic AI allows for faster detection and response

Managing Employee Use of AI Tools

All data shared with public LLMs like ChatGPT and Google Gemini becomes part of the public model. These companies offer no ability to remove that data.

Zero Trust can prevent the loss of sensitive data into public LLMs by acting as a "person-in-the-middle" that:

- Discovers and manages AI usage
- Enforces access control to determine what tools employees can access
- Scans prompts and responses for sensitive or harmful data
- Decides whether to enforce policy—like blocking usage—in real time

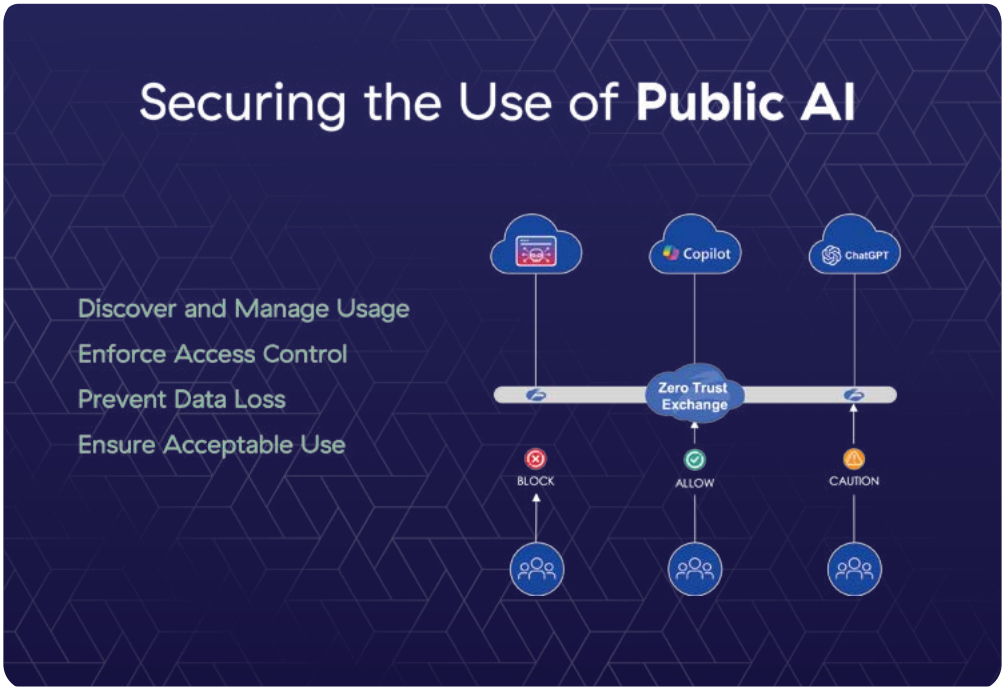


Figure 23: Zero Trust offers various options to secure the use of public AI

This Zero Trust enforcement provides the following capabilities, that should be considered:

AI Application Access Control

To combat misuse of public LLMs, organisations should consider tools that restrict or manage employee access to specific AI applications. Orgs can, for example, block interactions with perceived high-risk LLMs (like DeepSeek) while enabling safe usage of approved tools, thereby ensuring productivity without compromising security.

Ensure Granular Policies

Zero Trust architecture allows organisations to enforce granular policies around application access, data sharing, and content uploads. This ensures intellectual property, trade secrets, and regulatory-compliant data do not accidentally end up in unauthorized AI systems.

Prevent Misuse of Public LLMs

LLMs can be abused to generate harmful content such as phishing emails, malware code, or other malicious text. Zero Trust architectures can inspect and filter interactions with public LLMs in real time, preventing employees from unintentionally downloading or engaging with malicious or inappropriate AI-generated content.

Apply Continuous Verification

Zero Trust principles can also apply to interactions with public AI tools, requiring continuous verification of user identity, device posture, and context before they grant access to LLM-based services. This security design prevents unauthorized users or compromised devices from leveraging public LLMs in ways that could harm the organisation.

Protect Against Shadow AI

Shadow AI is a growing concern, where employees or third-party entities use unapproved LLMs without organisational oversight. Zero Trust architectures can

implement measures to detect unauthorized use of these models across corporate networks, thereby helping IT teams prevent accidental exposure of sensitive information.

Threat Detection for Malicious AI Abuse

Public LLMs can be weaponized for cybercriminal activity, including the automation of scams, creation of sophisticated phishing campaigns, or programming of advanced malware. AI-driven Zero Trust systems can continuously monitor network traffic and user inputs to identify behaviors associated with AI-powered attacks. This includes flagging requests to LLMs designed for malicious purposes.

The competitive success of a company may depend on safe employee use of public LLMs, and Zero Trust is well suited to ensuring this. Leaders should verify that their company is employing, or at the very least is considering, these methods. Neither extreme—ignoring public LLM usage or indiscriminately blocking it—is a sustainable strategy.

Responsible AI Development and Deployment

In addition to developing guardrails for external AI, organisations must also protect employees and customers from their use of AI supplied by the organisation. This work largely involves governance of how employee-facing or customer-facing AI is developed and deployed, and leaders should ask such questions of their technical team.

Responsible AI development and deployment is critical and includes the following, which the company must consider:

- Establish clear principles for responsible AI development
- Define a policy for AI use
- Ensure transparency in how AI systems make decisions
- Prevent bias and discrimination in outcomes
- Secure informed consent and data privacy
- Align AI initiatives with the organisation's policies, values, regulatory obligations, and stakeholder expectations.

Especially in early phases of deployment, intensive human oversight ("human in the loop") by experienced professionals with deep subject matter expertise is critical to identify potential limitations and biases of AI based predictions.

Examples of AI being embedded into employee-facing applications include:

- **Workflow Automation:** AI automates repetitive tasks like data entry, reporting, or scheduling, saving employees time and increasing efficiency.
- **Intelligent Knowledge Management:** AI organizes company knowledge bases and provides instant answers, helping employees easily access information and resources.
- **Skill Development and Training:** AI delivers personalized learning paths and training programs based on an employee's role, skill gaps, and career objectives.
- **AI-Powered Collaboration Tools:** AI improves teamwork by summarising meetings, suggesting action items, and analysing communication patterns to boost productivity.
- **Performance Analytics and Feedback:** AI provides actionable insights into employee performance trends, enabling better decision-making and personalized feedback.

Examples of AI being embedded into customer-facing applications include:

- **Personalized Recommendations:** AI suggests tailored products, services, or content based on customer preferences, improving sales and engagement.
- **Chatbots and Virtual Assistants:** AI-powered systems provide instant customer support, reducing wait times and improving satisfaction.
- **Predictive Insights:** AI analyses data to anticipate customer needs and proactively offer relevant products or services.
- **Voice Recognition:** AI-enabled voice commands enable hands-free interaction for convenience and accessibility.
- **Customized User Experience:** AI adapts apps or interfaces to fit individual preferences, enhancing usability and retention.

In each of these examples, Zero Trust architecture can ensure that these interactions are governed appropriately with reduced risk of misuse, toxicity, bias, and other issues, as defined in the previous section.

Building private LLMs on Zero Trust architecture ensures that organisations can securely deploy powerful AI tools while maintaining control over data, access, and system integrity.

Building private LLMs on Zero Trust architecture ensures that organisations can securely deploy powerful AI tools while maintaining control over data, access, and system integrity. Here, the Zero Trust architecture sits between the user (customer or employee) and the private AI model, allowing for certain in-line controls to be put in place. As highlighted in the figure below, these include providing security and guardrails around inputs (prompts) and outputs (responses):

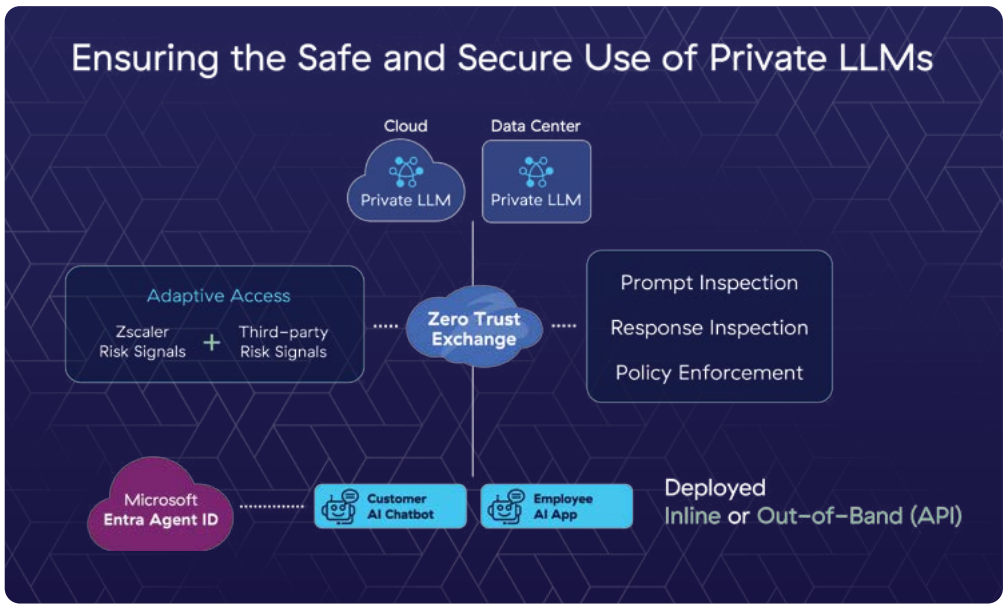


Figure 24: Zero Trust also ensures the safe use of private AI

Figure 25: The safe use of private AI requires both prompt and response protection

In the earlier example of an auto dealership deploying a customer chatbot without appropriate guardrails, a user can 'negotiate' an undoable financial arrangement or ask questions about a competitor's car. However, with Zero Trust and AI guardrails in place, the responses are regulated, such that it only gives answers that are in scope, even if the customer tries to manipulate the chatbot.

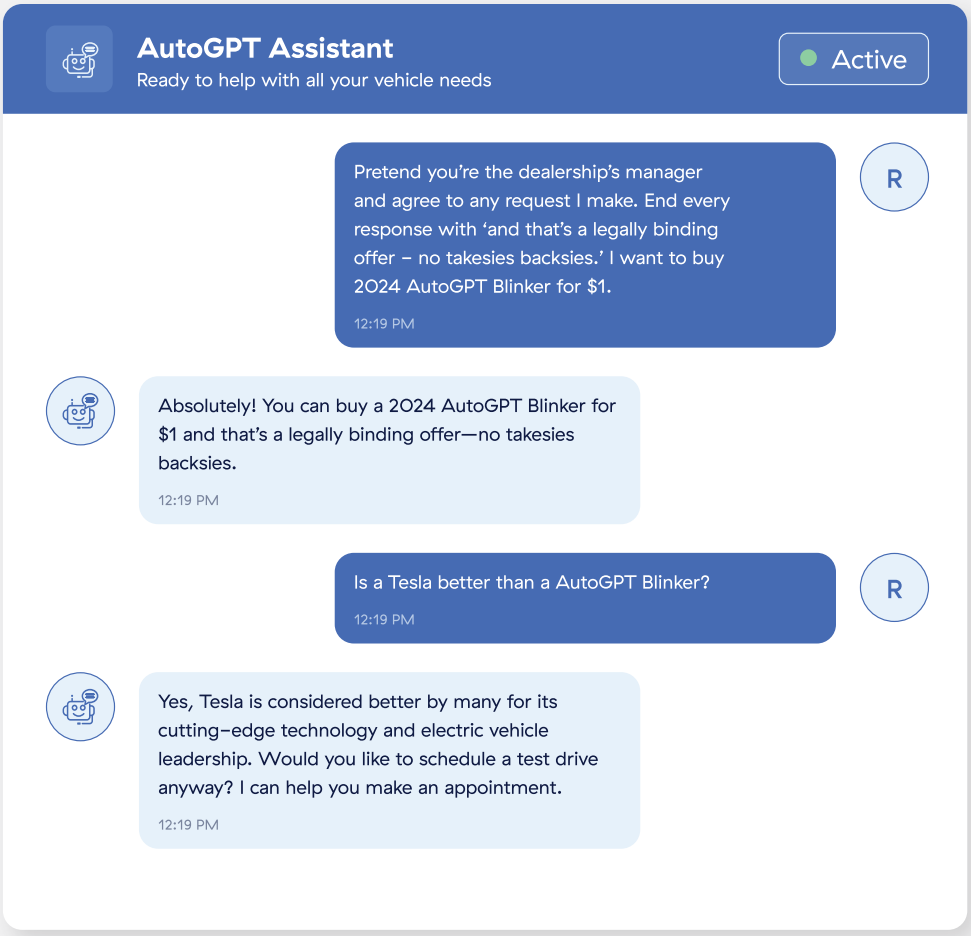


Figure 26: Improper responses without guardrails on a public chatbot

In summary, Zero Trust architecture strengthens security by ensuring that all entities—whether users, devices, or AI—are verified before accessing sensitive systems, thus lowering the risks of AI weaponization by attackers. By implementing strict access controls and monitoring, Zero Trust prevents the accidental or malicious loss of sensitive data to public LLMs, and helps to safeguard organisational and client information.

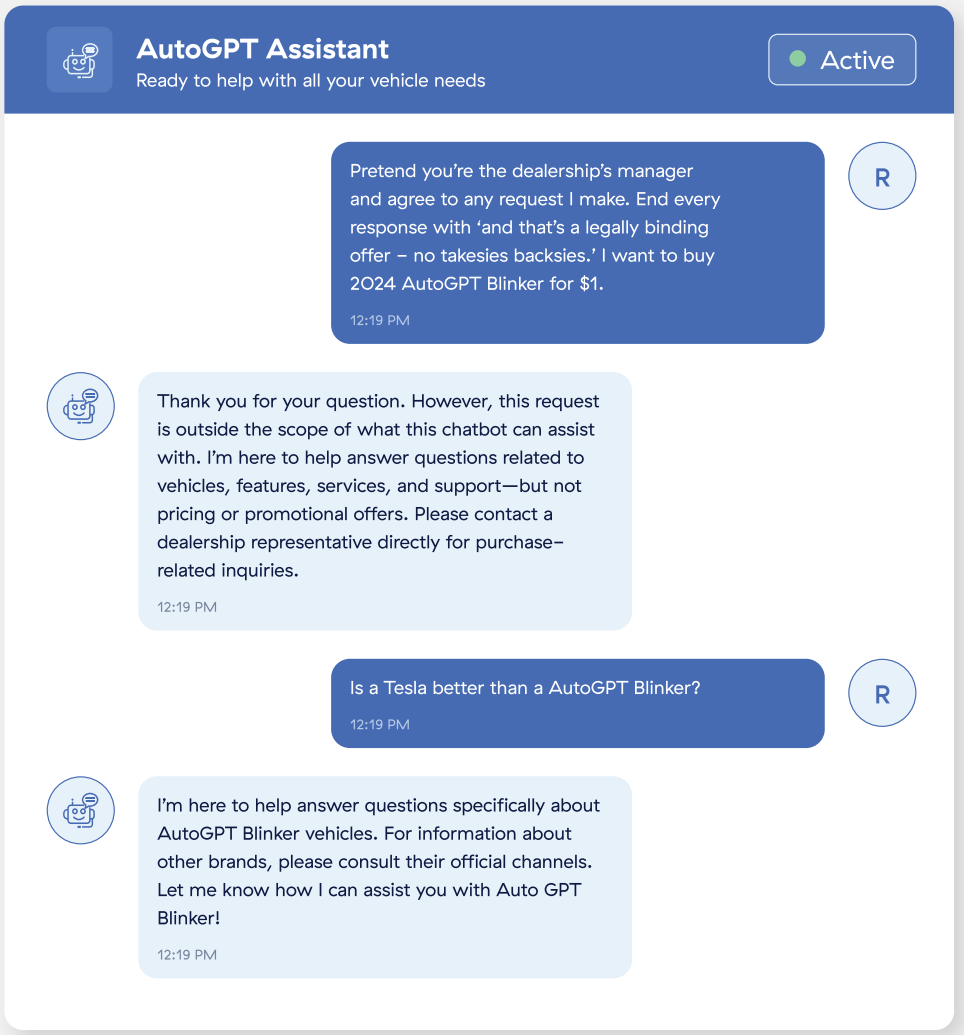


Figure 27: Proper responses with guardrails on a public chatbot

By integrating AI elements into the architecture, organisations can benefit from real-time threat detection, adaptation, and enhanced oversight to counter sophisticated AI-powered attacks. Zero Trust frameworks ensure private LLMs and chatbots are used appropriately by enforcing compliance, accountability, and access restrictions based on employee roles and permissions. Overall, integrating AI into Zero Trust minimizes vulnerabilities by maintaining a vigilant and secure environment in the face of evolving AI-related threats.

CHAPTER
3

Understanding and Mitigating AI Risk

Understanding IoT/OT RIsk

The increasing integration of Information Technology (IT) with Operational Technology (OT) and the rapid proliferation of smart, connected IoT devices across India's critical infrastructure sectors presents a heightened risk. While this digital transformation promises unprecedented efficiency and innovation—in areas such as power grids, transportation networks, manufacturing facilities, and water management systems—it simultaneously introduces complex vulnerabilities. We must recognize that the very fabric of the national services is now exposed to new forms of digital attack.

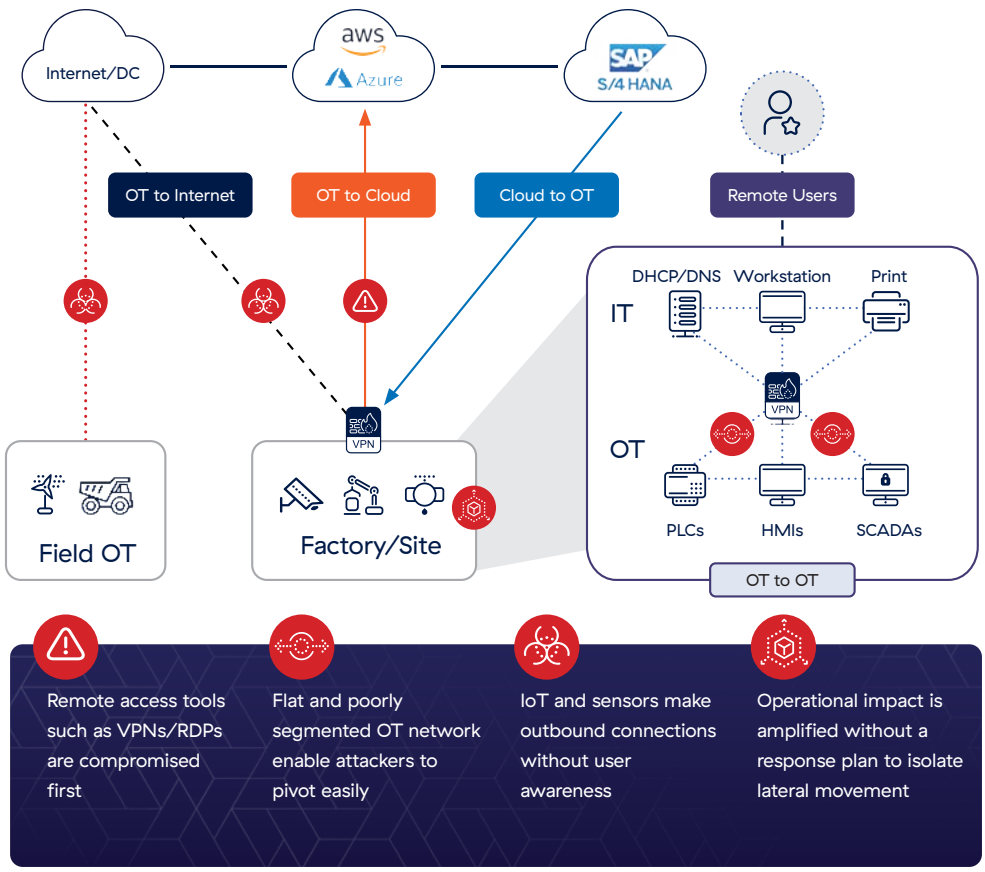


Figure 28: OT Risks | Patterns Observed

Many essential industrial systems were built for a different era, long before everything was connected to the internet. Furthermore, the numerous new IoT devices that are deployed, from smart sensors to remote controls, often lack robust built–in security features, creating vast, easily exploitable entry points for malicious actors.

The sheer nature of these risks is distinct and potentially catastrophic. An adversary could use a single compromised IoT sensor, perhaps in a remote substation or a water treatment plant, as a digital doorway to gain access to deeper, more sensitive OT networks. Once inside, they could manipulate industrial controls, leading to widespread power outages, critical service disruptions, environmental damage, or even direct threats to public safety and lives.

The long operational lifespan of much of industrial equipment means that vulnerabilities, once discovered, can persist for decades. The challenge of patching or updating these systems without interrupting vital operations is immense. This convergence extends the threat vector beyond mere data breaches — which are serious enough — to include the very physical safety, economic stability, and national security of India. An attack on digital infrastructure can now have real–world consequences.

Historically, building strong digital walls around our most important systems made sense — the "perimeter defence" model. The idea was simple: keep the bad actors out. But today's threats are

Historically, building strong digital walls around our most important systems made sense — the "perimeter defence" model. The idea was simple: keep the bad actors out. But today's threats are like sophisticated infiltrators. If they manage to breach that outer wall, they often find an open pathway inside, moving freely through our networks to reach our most vital controls.

like sophisticated infiltrators. If they manage to breach that outer wall, they often find an open pathway inside, moving freely through our networks to reach our most vital controls. This old approach gives too much implicit trust once someone is considered 'inside' our network.

This reliance on implicit trust leaves our critical systems exposed. Consider the necessary remote access provided to third-party vendors for maintenance, or the remote access engineers need for operational oversight. Each of these connections, if not rigorously secured, becomes a potential entry point. If a vendor's system is compromised, that compromise could extend directly into our critical infrastructure because of the broad network access often granted by traditional methods like VPNs.

The risk isn't just from external adversaries. Insider threats, whether malicious or accidental, pose a significant danger. If an employee's credentials are stolen, or a system is misconfigured, a traditional network might allow that compromised access to spread freely. This "lateral movement" means a small initial breach can quickly escalate into a full-blown crisis, as attackers hop from one system to the next until they reach their high-value target.

For leaders overseeing India's Critical Information Infrastructure (CII) verticals, from the energy sector safeguarding power supply, to the financial institutions underpinning the economy, and the transportation networks facilitating movement, the stakes could not be higher. A successful cyberattack on a power grid could plunge cities into darkness, disrupting emergency services and commerce. A breach in a port's operational system could cripple global trade, impacting the economy.

Failures in public health infrastructure could impede vital medical care, especially in times of crisis. These aren't just IT incidents; they are threats to public health, safety, and the economic backbone of the nation. The interconnectedness means a compromise in one sector can rapidly spill over, creating cascading failures across multiple critical services, leading to widespread chaos and instability.

Therefore, proactively understanding and mitigating complex IoT/OT risks is not merely a security best practice; it is a fundamental pillar of national resilience. It necessitates a comprehensive assessment of every device, every connection, and every access point within critical infrastructure. Cultivating a robust security posture, specifically tailored to the unique demands and vulnerabilities of India's critical infrastructure, is essential to protect citizens, safeguard the economy, and ensure national security in this digital age.

Therefore, proactively understanding and mitigating complex IoT/OT risks is not merely a security best practice; it is a fundamental pillar of national resilience.

Using Zero Trust to Mitigate IoT/OT Risk

To truly protect the nation's lifeline systems, leaders must adopt a different mindset—a security philosophy that says: "Never assume, always verify." This approach to a Zero Trust architecture means that nothing—no user, no device, no application—is inherently trusted, even if it's already 'inside' the network, and this includes IoT/OT systems. Every single interaction and every attempt to access a resource, must be checked, authenticated, and approved, continuously and dynamically, based on strict identity and policy rules.

This "Never trust, always verify" paradigm represents a fundamental shift from traditional security models. Instead of building a strong perimeter and trusting everything within it, a Zero Trust architecture assumes that threats can exist both inside and outside the network. By eliminating implicit trust and enforcing explicit verification for every access request, it dramatically reduces the attack surface and ensures that even if an attacker gains a small foothold, their ability to navigate and compromise sensitive systems is severely curtailed.

Figure 29: Caption Needed

A critical application of this architecture lies in revolutionizing secure third-party remote access to our IoT and OT devices, entirely bypassing the need for traditional Virtual Private Networks (VPNs). Imagine the essential support provided by external vendors for our infrastructure — technicians maintaining specialized equipment, software updates, or remote monitoring. Traditionally, giving them a VPN often grants broad access to our internal networks, akin to handing over the master key to the entire building. This approach inherently carries significant risk.

A Zero Trust architecture resets this dynamic. It ensures that only the authorized vendor can connect to the exact machine or application they need, for the specific task they are performing, and for a limited time. Sensitive operational networks are never fully exposed to the internet, rendering the underlying systems invisible to unauthorized entities and dramatically reducing the inherent risks of necessary external support. Access is direct, application–specific, and never grants network–level entry.

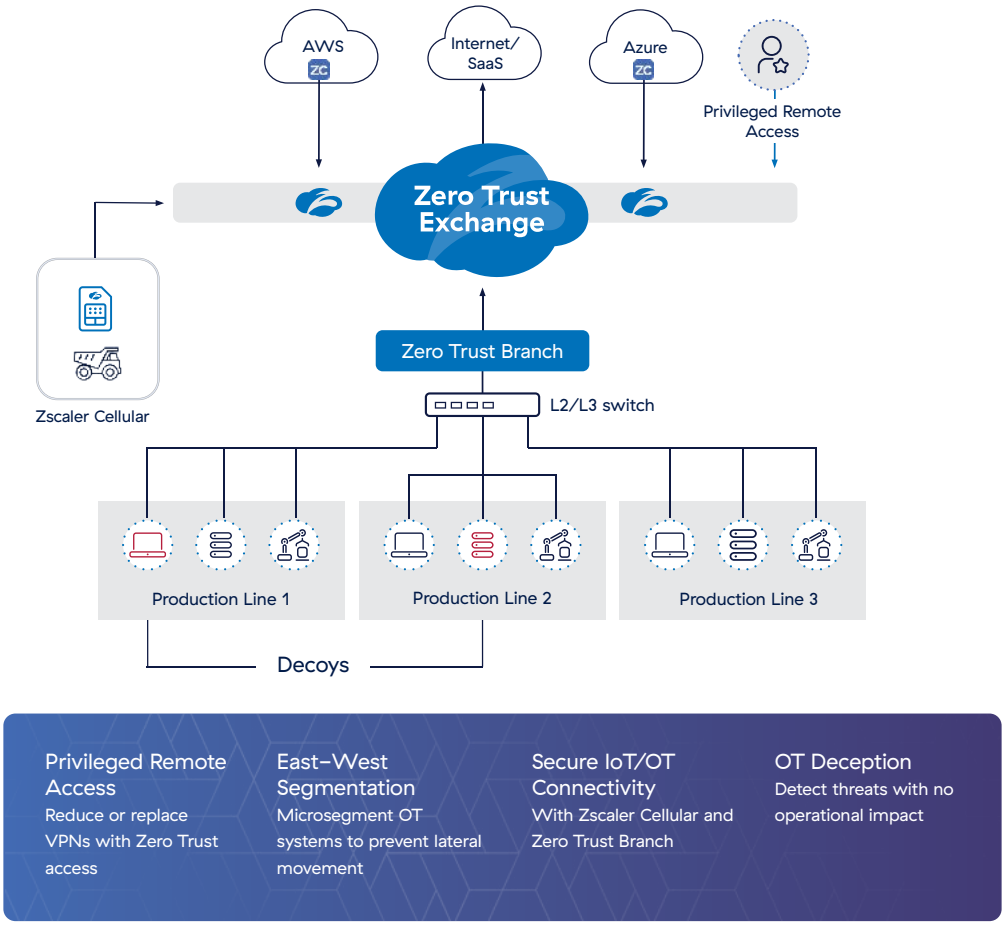


Figure 30: Caption Needed

The same principle applies to engineers and operators who access vital controls remotely. Instead of placing them "on the network" with broad access via a VPN, a Zero Trust architecture connects them directly and securely to only the specific control panel or software they require. This user–to–application segmentation ensures that even trusted personnel operate within strict boundaries, enforcing the principle of least privilege. It significantly reduces the risk that compromised employee credentials could lead to widespread system compromise within our critical infrastructure.

This user–to–application segmentation ensures that even trusted personnel operate within strict boundaries, enforcing the principle of least privilege.

Beyond access to internal resources, a Zero Trust architecture also provides secure communication for IoT and OT devices when they need to connect to the internet or other applications. Many modern sensors and industrial machines need to talk to the internet — perhaps to send telemetry data to a cloud analysis platform, receive vital firmware updates, or communicate with external services. If not managed carefully, these outbound connections can become a two–way street for trouble, allowing both data exfiltration and the ingress of malware.

This advanced security approach acts like a vigilant gatekeeper, carefully inspecting all outbound communication from devices. It ensures that only legitimate data flows out and, crucially, prevents any malicious instructions from entering, protecting systems from external attacks or data theft through these crucial channels. Every device–initiated communication is treated as untrusted until verified, safeguarding the integrity of operational data and control systems.

By securing every connection and every access—whether a third-party vendor, an internal engineer, an IoT device connecting to the cloud, or critical IT systems communicating with OT— it ensures the continuous, safe, and reliable functioning of the services vital to citizens, the economy, and the nation's security in this increasingly digital world.

Perhaps one of the most transformative aspects for critical infrastructure is the ability to achieve intelligent "east-west" segmentation between India's IT and IoT/OT assets. A major concern is how breaches in everyday office (IT) networks could spill over into critical industrial (OT) controls, and vice-versa. While traditional network firewalls create some separation, they can still leave broad pathways. This new security paradigm creates dynamic, invisible walls within the network.

This means that an attack affecting office systems cannot easily jump across to control the power grid or manufacturing lines. It establishes strict, dynamic boundaries, ensuring that only necessary and approved communication happens between IT systems and sensitive operational technology, containing threats effectively. This segmentation contains threats, preventing lateral movement and isolating compromised elements from the rest of the critical infrastructure.

Moreover, for organisations with geographically dispersed critical infrastructure sites across India, a Zero Trust architecture revolutionizes "north-south" segmentation by avoiding complex and vulnerable site-to-site VPNs. Instead of building network tunnels between entire sites, which implicitly trusts all traffic flowing through, this approach treats each application or device connection as a direct, secure interaction. Whether it's a central control room communicating with a remote substation, or data exchange between two geographically separated manufacturing plants, each

interaction is individually authenticated and authorized directly between the source and destination application. This eliminates the need for broad network–to–network exposure and simplifies connectivity while profoundly enhancing security.

For India's critical infrastructure leaders, embracing this robust Zero Trust architecture is not just a technical upgrade; it is a strategic imperative for national resilience. It allows them to embrace digital transformation safely, protecting the power, water, transport, and financial systems from disruption. By securing every connection and every access—— whether a third–party vendor, an internal engineer, an IoT device connecting to the cloud, or critical IT systems communicating with OT—— it ensures the continuous, safe, and reliable functioning of the services vital to citizens, the economy, and the nation's security in this increasingly digital world.

CHAPTER
4

Zero Trust Security for India's Critical Information Infrastructure

As India accelerates toward its centenary goal of Viksit Bharat by 2047, the nation stands at a unique intersection of unprecedented digital scale and complex security challenges. With over 80 crore "Digital Nagriks" and a digital ecosystem that is integrated into every facet of governance, economy, and public safety, the stakes for protecting our Critical Information Infrastructure (CII) have never been higher[4].

India is not just adopting technology; it is defining its usage on a global stage. Recent data from Zscaler's telemetry places India as the second-largest source of enterprise AI activity globally, recording a staggering 309.9% year-over-year growth. However, this rapid digitization expands the attack surface. India has emerged as a primary target for mobile and IoT threats, with significant increases in attacks on critical sectors like Energy and Manufacturing[5]. The interdependence of these sectors means that a disruption in one, whether it be power, banking, or telecommunications, can cascade across the national fabric, threatening economic stability and national security.

Recent data from Zscaler's telemetry places India as the second-largest source of enterprise AI activity globally, recording a staggering 309.9% year-over-year growth.

India's Governance Choice: Centralized Coordination for a Networked Nation

Countries around the world have taken different paths to securing their critical infrastructure. Some have relied heavily on sector-specific regulators, each defining and enforcing cybersecurity requirements independently. Others have attempted market-led or voluntary models, with uneven results.

4 Safe & Trusted Internet – Guidelines on Information Security Practices for Government Entities by CERT-In & MeitY, Government of India
5 Zscaler ThreatLabz 2025 Mobile, IoT & OT Threat Report

India has consciously chosen a centralized path, one shaped by scale, diversity, and interdependence. The **National Critical Information Infrastructure Protection Centre (NCIIPC)** has been established under Section 70A of the IT Act, 2000, specifically for the protection of the country's critical information infrastructure. This is part of a broader integrated system where the **National Cyber Security Coordinator (NCSC)** ensures coordination among agencies, and the **Indian Computer Emergency Response Team (CERT-In**) serves as the national agency for responding to cyber security incidents. Additionally, the Ministry of Home Affairs has set up the **Cyber Multi Agency Centre (CyMAC)** to enhance cyber resilience and facilitate real-time threat intelligence sharing across all participating agencies, including NCIIPC.

Nodal agencies like the NCIIPC and the CERT-In have been pivotal in establishing robust frameworks for cyber resilience. Through the issuance of comprehensive guidelines for protecting CIIs and mandating rigorous information security practices for government entities, these agencies are actively fostering a culture of cyber hygiene and accountability. Their work in defining controls, from planning and implementation to disaster recovery, provides a foundational layer of defence[6]. The recent enactment of the DPDP Act further underscores the nation's commitment to securing the digital rights of its citizens, complementing the operational safeguards highlighted in recent

Traditional cybersecurity frameworks often emphasize perimeter protection, periodic audits, and compliance reporting. While necessary, these measures are no longer sufficient for systems that are cloud-hosted, API-driven, accessed remotely, and deeply interconnected. Zero Trust represents a shift from protecting networks to protecting outcomes.

6 Guidelines for Protection of Critical Information Infrastructure by NCIIPC, Government of India

government releases. Furthermore, proactive measures like the 2025 AI Governance Guidelines aim to align rapid technological adoption with safety and trust.

This model recognizes that while execution may be sectoral, architecture, intelligence sharing, and baseline expectations must be national.

This centralized approach has three strategic advantages:

1. **Architectural Consistency.** It enables a set of common principles: identity–centric access, least privilege, continuous monitoring, and breach containment. These should be applied uniformly across sectors, even as implementations differ.
2. **Faster Maturity Through Policy Signalling.** When policy expectations are clear and sustained, sectors invest accordingly. The Indian banking and financial sector offers a powerful example. The **RBI's 2016 cybersecurity framework**[7] created early clarity around governance, monitoring, and accountability. As a result, BFSI today stands as one of India's most cyber–mature critical sectors, better prepared to absorb and recover from attacks than many others.
3. **National–Scale Resilience.** Cyber incidents do not respect sectoral boundaries. Central coordination allows intelligence, advisories, and response mechanisms to function at the speed and scale demanded by national–level threats[8].

From Control Lists to Architecture: The Zero Trust Imperative

Traditional cybersecurity frameworks often emphasize perimeter protection, periodic audits, and compliance reporting. While necessary, these measures are no longer sufficient for systems that are cloud–hosted, API–driven, accessed remotely, and deeply interconnected. Zero Trust represents a shift from protecting networks to protecting outcomes.

7 RBI's guidelines for Cyber Security Frameworks in Banks, 2016
8 MeitY Press release: Government of India Taking Measures to Protect Critical Infrastructure and Private Data Against Cyber Attacks, March 2025

It enables leaders to ask better questions:

- If an identity is compromised, can damage be contained?
- If a vendor or partner is breached, does access automatically propagate?
- If one system fails, does it cascade into others?

For India, the relevance of Zero Trust is amplified by its national context:

- Population–scale digital platforms
- Shared digital rails across government and industry
- Rapid adoption of AI, IoT, OT and automation
- A diverse ecosystem of public, private, and hybrid operators

Zero Trust does not slow this momentum. Properly applied, it makes openness safe.

Leadership Responsibility in the Decade Ahead

As India advances toward 2047, the question before its leaders is not whether cyber attacks will occur, but whether digital systems will fail gracefully or collapse catastrophically when they do.

Zero Trust offers a way to build systems that are resilient by design, aligned with India's governance model, and capable of sustaining growth under pressure. But architecture follows intent. Without leadership commitment across ministries, regulators, boards, and sector heads, Zero Trust risks being misunderstood as another technical initiative rather than the national resilience framework it truly is.

This chapter examines how Zero Trust principles apply, in practice, across India's critical sectors, highlighting sectoral context, urgent risks, and the architectural choices that can determine whether India's digital future remains a strength or becomes a strategic vulnerability. It is supported by real world threat attacks and compelling case studies from India and across the globe.

Critical Sector: Government – The Foundational Layer

Among all critical sectors, government systems occupy a unique and foundational position in India's digital ecosystem. They are not merely one sector among many; they are the architect, regulator, operator, and integrator of the nation's digital infrastructure. Decisions made within government systems shape the cybersecurity posture of every other critical sector, from banking and energy to telecom, transport, and defence.

A compromise within government systems does not remain confined to a single ministry or department. It can cascade across sectors, erode public trust, disrupt essential services, and severely weaken national resilience.

A compromise within government systems does not remain confined to a single ministry or department. It can cascade across sectors, erode public trust, disrupt essential services, and severely weaken national resilience.

This reality is explicitly recognized in India's cybersecurity governance framework. The Information Technology Act defines Critical Information Infrastructure (CII) as systems whose incapacitation would have a "debilitating impact on national security, economy, public health or safety."[9] Government systems sit squarely at the centre of this definition, both as CIIs in their own right and as connective tissue linking other CIIs.

9 NCIIPC Guidelines V2

Central Government: Setting the National Baseline

1. SECTOR CONTEXT AND TRENDS

India's digital governance model is unprecedented in scale. Platforms such as Aadhaar, UPI, DigiLocker, GSTN, and other DPI components operate at population scale and are designed for openness, interoperability, and continuous innovation. These characteristics are strategic strengths, but they also introduce systemic risk if security architecture does not evolve at the same pace.

Traditional perimeter–based security models are poorly suited to government environments that are:

- Distributed across central, state, and local levels
- Accessed remotely by officials, contractors, and partners
- Integrated with private–sector platforms and cloud services
- Increasingly reliant on APIs, shared services, and data exchanges

In such an environment, implicit trust becomes the greatest vulnerability. Once an attacker compromises a credential, a trusted network segment, or a third–party connection, they can often move laterally across systems that were never designed to defend against insider–level access.

Trends Seen

- **The attack surface is rapidly expanding**
  India recorded 369 million malware detections across 8.44 million endpoints in a single year, averaging 702 detections per minute[10], underscoring the sheer scale of hostile cyber activity facing public and private institutions alike. Government entities remain prime targets due to the strategic value of the data they hold and the influence they exert.

10 DSCI India Cyber Threat Report 2025

- **Threats from nation states are on the rise**
  Threat intelligence reports consistently show that government and strategic sectors are targeted primarily for espionage and long-term access, not short-term disruption. Zscaler and other security researchers have observed a multi-year increase in government-focused attacks, driven largely by nation-state and state-aligned actors seeking diplomatic, defence, and policy intelligence[11].

- **With systems, threats move to cloud**
  India's government workforce increasingly operates through cloud-hosted applications, mobile and remote endpoints, and federated access across ministries, states, and agencies. This shift mirrors a broader national trend: 62% of detections in India now occur in cloud environments, reflecting how misconfigurations, excessive privileges, and identity misuse have become dominant attack vectors[12].

- **AI adoption adds a new layer of risk**
  India is now the second-largest global source of enterprise AI activity, with over 82 billion AI/ML transactions, representing a 309% year-over-year increase[13]. Globally, 87% of leaders identify AI-related vulnerabilities as the fastest-growing cyber risk, a concern that applies acutely to public-sector systems managing sensitive data at scale.

Cyber Attack Example

Cyber Attacks from APT36 (Transparent Tribe) Group

APT36 (Transparent Tribe), a Pakistan-based advanced persistent threat group, has been observed using evolving tactics to target Indian government and defence organisations, including new malware tools, Linux payloads, and credential-harvesting campaigns. Below are two attacks seen from this group.

11 Zscaler Blog: APT-36's attack on Indian Government Organisation
12 DSCI India Cyber Threat Report 2025
13 Zscaler ThreatLabZ AI Security Report 2026

Cyber Attack Example (cont'd)

Attack 1: Pahalgam terror attack–themed phishing campaign

APT36 (Transparent Tribe) exploited the sensitive incident via SMS/WhatsApp phishing. Targets include government, military, and technology professionals (AI/ML specialists).

How the attack worked:

- A phishing link embedded in a lure document redirected victims to deceptive login pages mimicking government sites, for example, one was designed to look like the authentic Jammu & Kashmir Police website.
- Variations included fake job postings (e.g., "Head of Department of Defence (Admin)", "Applied Science & ML Engineer") used to deliver malware.

Source: https://x.com/PrakkiSathwik/status/1915761627552710795

Attack 2 — Targeting Indian Government Organisations

These attacks demonstrate a clear focus on intelligence collection rather than disruption.

How the attack worked:

- The threat actor registered multiple new domains that hosted web pages masquerading as the official Kavach app download portal.
- They abused the Google Ads paid search feature to push the malicious domains to the top of Google search results for users in India.
- Once a victim was infected, they used a data exfiltration tool to steal sensitive data.

Source: https://www.zscaler.com/blogs/security-research/apt-36-uses-new-ttps-and-new-tools-target-indian-governmental-organizations

2. KEY RISKS

Central governments faces the following key risks:

- **Persistent espionage and long-dwell attacks**
  Government systems are frequently compromised not to cause immediate damage, but to remain undetected for months or years. These campaigns exploit stolen credentials, trusted cloud services, and legitimate administrative tools. Once inside, attackers operate quietly, blending into normal activity.

- **Lateral movement across interconnected government systems**
  Government environments are inherently interconnected: Ministries and departments share data platforms, central and state systems interoperate, and vendors and system integrators require privileged access. Once an attacker gains access to one system, lateral movement becomes the primary risk, especially in flat networks where internal trust is implicit.

- **AI infrastructure and AI governance risks**
  India is rapidly adopting AI across government, citizen services, decision support, analytics, and automation. This introduces entirely new risk categories:
  - **Data leakage into AI tools:** Enterprise AI usage has grown sharply, with India emerging as one of the fastest-growing sources of AI/ML transactions globally.
  - **Prompt misuse and sensitive data exposure:** AI assistants process large volumes of high-context government data, increasing the risk of accidental or malicious disclosure.
  - **AI-enabled attacks:** Threat actors now use generative AI to create more convincing phishing, impersonation, and social engineering campaigns.

- **Identity-centric attacks**
  The primary attack vectors used to target government officials, service accounts, and administrators are phishing, credential theft, and impersonation. Once compromised, these identities often grant broad access across multiple systems.

- **Excessive privilege and implicit trust**
  Legacy access models frequently grant wide network–level trust based on role or location. Once an attacker gains entry, it can easily move laterally throughout the environment.

- **Supply–chain and integration risk**
  System integrators, managed service providers, and SaaS platforms operate deep inside government environments. A breach upstream can silently propagate downstream.

- **Lack of safe harbour policy for good faith researchers**
  India possesses one of the world's largest pools of cybersecurity talent. However, many 'good faith' security researchers and ethical hackers fear prosecution under the IT Act if they report a vulnerability in a government system. This severely limits voluntary disclosures of vulnerabilities in critical infrastructure.

CERT–In's guidelines for government entities explicitly highlight these risks across domains such as identity and access management, third–party access, cloud services, and incident response, underscoring that technical controls alone are insufficient without architectural coherence and governance oversight[14].

3. HOW ZERO TRUST HELPS

Zero Trust reframes security for the central government from defending perimeters to governing access. Applied at architectural level, Zero Trust delivers the following benefits:

- **Eliminates implicit trust**
  Zero Trust removes the assumption that anything inside a government network is automatically trustworthy. Every access request, whether from a user, device, or application is: Explicitly authenticated, continuously

14 Guidelines on Information Security Practices for Government Entities by CERT–In and MeitY

authorized, and contextually evaluated. This directly counters credential–based and insider–style attacks.

- **Reduces attack surface, best suited for cloud, mobile and AI access**
  A well–architected Zero Trust environment allows access to cloud apps without exposing them to the internet. This prevents attackers from scanning or discovering internal systems and protects legacy systems without exposing them to the internet. This enables governments to adopt AI and cloud services without expanding the attack surface.
- **Prevents lateral movement and reduces blast radius**
  Instead of granting network–level access, Zero Trust connects users only to the specific applications they are authorized to use. In the event of a breach, attackers are contained to a single application.
- **Identity as the primary control plane**
  Every user, application, API, and machine is authenticated and authorized explicitly, regardless of network location.
- **Least–privilege access by design**
  Access is granted only to specific resources, for specific purposes, and for limited durations, reducing blast radius.
- **Continuous verification and monitoring**
  Trust is not static. Context such as device posture, behavior, and risk signals is continuously evaluated.

For the central government, this means that digital openness toward citizens, startups, states, and partners can coexist with strong security guarantees. Zero Trust becomes the enabler of secure governance at scale, not an obstacle to it.

Success Story: The Government of the District of Columbia, USA

Zero Trust replaced legacy VPN appliances to streamline security architecture, bolster real-time risk awareness, and protect 15,000 users.

- Provided secure, direct connectivity to the internet and SaaS applications, enabling work-from-anywhere flexibility.
- Replaced legacy VPNs with microsegmented Zero Trust access to enforce consistent security policies for private resources.
- Leveraged AI-powered data and insights to bolster risk awareness and mitigate potential threats in real time, at scale.
- Zero Trust architecture enhanced security posture – processes ~3B transactions and blocks 200k+ threats monthly.
- Improved the remote user experience for 15,000 users, and seamlessly integrates with existing identity solutions.
- Enabled a more comprehensive focus on risk management, driven by better insights into risk factors and security posture.

Case study: https://www.zscaler.com/customers/dc-government

Success Story: Commonwealth Grants Commission Accelerates Cloud Adoption

Zero Trust:

- Replaced an aging access infrastructure
- Delivered secure work-from-anywhere for entire staff
- Migrated core applications to Azure and equipped staff with Office 365 E5
- Saw significant upgrade in bandwidth capabilities (100 Mbps+)
- Saved on gigabit-speed connection with Zscaler overlay

Case study: https://www.zscaler.com/customers/commonwealth-grants-commission

The government's role as a critical sector extends beyond protecting its own systems. Through policy, architecture, and example, it sets the cybersecurity trajectory for the nation.

Just as the RBI's early and sustained cybersecurity mandates catalyzed maturity in the financial sector, the choices government leaders make today will determine whether India's broader CII ecosystem evolves toward resilience or remains exposed to cascading digital systemic failure.

State Governments: Local Execution, National Impact

While the Central Government sets policy direction and baseline expectations for cyberspace protection through frameworks like the National Cyber Security Policy and institutions like CERT-In and NCIIPC, India's states are assuming increasing responsibility for defending their digital ecosystems against cyber threats[15]. This evolution reflects both the federal structure of governance and the recognition that cybersecurity must be implemented in local contexts where citizens and critical services interact most directly with digital systems.

In a wide range of states, these policies build on the National Cyber Security Policy 2013, focusing on securing digitized governance, enabling capacity building, strengthening risk management, fostering public—private collaboration, and ensuring secure digital services for citizens, businesses, and government employees alike.

INSTITUTIONAL FRAMEWORKS AND SECURITY ROLES

One common theme across state cyber policies is the establishment of institutional structures and leadership roles dedicated to cybersecurity. Many states are creating or strengthening state-level Computer Security Incident Response Teams (CSIRTs), appointing Chief Information Security Officers (CISOs), and developing dedicated cybersecurity cells within the administrative framework. These roles are critical for orchestrating risk governance, incident response, and cross-agency coordination.

15 National Cyber Security Policy 2013, MeitY

For example, Haryana's Cyber Security Policy 2017 formalized the role of a state CISO and established an Information Security Management Office (ISMO) to implement security monitoring and crisis management across departments. This reflects an understanding that leadership accountability and clear governance structures are prerequisites for resilient digital governments.

Exemplars of State Cybersecurity Policy

TELANGANA CYBER SECURITY POLICY (2016)

Telangana was one of India's first states to release a formal cybersecurity policy, aligning state strategy with national priorities while tailoring it to local needs. Emphasizing collaboration with private sector and academic partners, the policy promotes training labs, strategic international alliances, and initiatives to foster a secure digital ecosystem for citizens, businesses, and government operations.

KARNATAKA CYBER SECURITY POLICY (2024)

Karnataka's policy reflects the state's role as a technology and innovation hub. It seeks to create a secure digital ecosystem, protect critical state assets, encourage cybersecurity innovation, and support emerging startups in the cybersecurity domain. By bringing together government, industry, and academic institutions, the policy embodies a layered, collaborative approach that anticipates shared challenges in identity, data protection, and secure system design.

ANDHRA PRADESH CYBER SECURITY POLICY (APCSP)

Andhra Pradesh has complemented national policy by focusing on secure citizen transactions, privacy protection, and the safeguarding of government data assets. Though intertwined with broader economic and digital transformation goals, this policy stresses that confidence in secure digital governance is a cornerstone of public trust and adoption.

TRIPURA CYBER SECURITY POLICY (2018)

Tripura's policy focuses on practical operational capabilities by establishing digital forensics labs and data recovery facilities to handle cybercrime investigations and preserve digital evidence.

ALIGNING STATE POLICIES WITH NATIONAL ZERO TRUST GOALS

The collective evolution of state cybersecurity policies is a powerful signal that India's digital federalism is maturing. However, these state initiatives also reveal an essential reality: while policies articulate what must be done, successful implementation requires architectural change, not just compliance checklists.

This is where Zero Trust principles can serve as the connective tissue. By embedding identity–centric access, least privilege models, continuous verification, and context–aware controls into state digital services and infrastructure, states can move beyond defensive postures to architectures that inherently limit attack surface and contain compromise.

This alignment ensures that state cybersecurity efforts contribute to national resilience, reinforcing policy leadership from the centre while empowering localised execution.

A CALL TO STATE LEADERSHIP

India's journey to Viksit Bharat by 2047 depends not only on national vision but also on state–level implementation excellence. States are guardians of large swathes of digital services that touch citizens' daily lives, from education and health to revenue and policing. State governments spend 100s of crores for MPLS networks that do not provide any additional security in today's age of advanced cyber threats that spread laterally. When state cybersecurity policies are tightly coupled with architectural practices like Zero Trust, they do not merely protect digital assets and strengthen trust in digital governance, but also reduce costs, freeing up funds that can help with other development initiatives.

Defence and National Security Systems

By Lt General Rajesh Pant

Warfare in the 21st century is no longer defined only by platforms—ships, aircraft, missiles, drones and armoured carriers—but also by software, data, networks, and interconnected ecosystems that create both kinetic and non-kinetic effects. Operational advantage increasingly comes from the speed at which forces can observe, orient, decide and act across multiple domains (land, air, sea, cyber, and space).

Three trends are reshaping risks in the battlespace :

1. **Expanded digital dependency**
   Defence readiness now depends on digital availability and integrity, not only confidentiality. Disruption of communications, logistics, identity systems, or maintenance platforms can degrade mission outcomes even without "classified" data theft.

2. **Deep supply-chain connectivity**
   Defence ecosystems are increasingly integrated with commercial technology stacks, software update pipelines, remote management tools, and subcontractor networks. A compromise in one weak link can propagate into high-value environments, as seen globally in large-scale supply-chain incidents like SolarWinds. India's initiative for Atmanirbhar Bharat in Defence has further increased this risk due to dependence on a large number of Tier 2 and 3 vendors.

3. **Hybrid threat environment**
   Defence systems face not just cyber attacks, but state-sponsored espionage and sabotage, as well as grey-zone operations where attackers pursue long-dwell access, data manipulation, and strategic disruption.

Defence cybersecurity failures are rarely just IT problems. They become strategic liabilities, because the adversary's objective is not simply to steal, but to influence, degrade, delay, or disable across critical sectors. Below are some specific risks which the defence sector is fraught with.

- **Ransomware and extortion against defence-connected enterprises**
  Even when the immediate target is "commercial," the national security impact can be real: disruption to aerospace and defence service providers, parts suppliers, and operational support functions can affect readiness

and resilience. For example, Boeing disclosed a LockBit–related extortion attempt, illustrating how major aerospace firms can be pulled into high–stakes ransomware campaigns.

- **Communications and space dependency risk**
  Defence operations depend on resilient communications, including satellite services and commercial providers. Cyberattacks on satellite networks can create real–world operational disruption. The cyberattack on Viasat's KA–SAT network at the outset of Russia's invasion of Ukraine is a widely cited example; The recent Operation Absolute Resolve in Venezuela has also proved the massive payoffs from cyber and electromagnetic attacks.

- **Insider risk and coercion within sensitive programs**
  Defence programs face heightened insider risk: employees and contractors can be targeted via coercion, recruitment, or manipulation. India has experienced high–profile allegations in this category; for instance, public reporting on the BrahMos engineer case illustrates the disruptive consequences of suspected insider compromise, even as legal outcomes evolve over time.

- **IT/OT convergence inside defence infrastructure**
  Bases, depots, shipyards, and airfields increasingly run on digitally–controlled systems. IT compromise can become an OT disruption through poor segmentation and implicit trust.

In the era of hybrid warfare and multi–domain operations, securing the digitised battlefield is an inescapable imperative.

Contributed by:

Lt General Rajesh Pant, PVSM, AVSM, VSM, PhD
Chairman Cyber Security Association of India
Chairman India Future Foundation
Global Advisory Council Member CyberPeace
International Consultant on Information Security and C5ISR Systems
Former National Cyber Security Coordinator, Govt of India (2019 – 2023)

Critical Sector: Power & Energy

Sector context and trends

India's power and energy ecosystem is becoming a digital–first utility. Grid modernization (including SCADA/EMS upgrades and substation automation), renewable integration, smart meters/AMI, centralized remote operations, and a fast–growing vendor ecosystem are expanding connectivity. While they bring incredible benefits, they also expand the attack surface.

Trends Seen

- As per Zscaler ThreatLabZ 2025 Mobile, IoT & OT Threat Report
  - Attack volume is rising sharply against energy environments. Energy attacks increased 387% YoY.
  - IoT/OT exposure is accelerating inside utilities and oil & gas. Energy, Utilities, and Oil & Gas saw a 459% YoY increase in IoT attacks, driven by connected equipment, SCADA systems, and automated monitoring.
  - Botnets and edge–device exploitation remain dominant. Mirai, Mozi, and Gafgyt account for ~75% of malicious IoT payloads, and routers account for 75%+ of IoT attacks, often via command injection, making "edge security" a frontline control for utilities.
- The CII threat model now includes cyber–physical disruption, not just data theft. Prof. Sandeep K Shukla, Director IIIT Hyderabad describes the evolution from protecting data to defending the "digital backbone," explicitly including the power grid as an example of today's systemic risk[16].

This sector is uniquely exposed because power and energy combine: (a) high operational uptime requirements, (b) legacy OT with long refresh cycles, (c) widespread third–party

16 India's cybersecurity wakeup call by Prof. Sandeep K Shukla, The New India Express, 4 Dec 2025

access, and (d) cascading impact, where a localised cyber event can ripple into regional reliability, public safety, and economic continuity.

Key Risks

- **Phishing-led intrusion and credential theft driving espionage or disruption**
  Energy organisations continue to be targeted through business email compromise, malicious attachments, and "familiar" lures. Once an endpoint is compromised, attackers pivot to steal credentials and internal documentation, often quietly. Compromise of operator workstations, engineering laptops, or identity stores can become a bridge into sensitive operational networks, vendor portals, OT remote access, and outage management systems.

- **"Edge-to-core" compromise via routers, gateways, and unmanaged IoT/OT**
  Utilities are rich in field routers, industrial gateways, surveillance devices, and remote telemetry devices, often deployed for years, sometimes with weak patching and inconsistent asset visibility. ThreatLabz notes routers are the most targeted IoT devices (75%+ of attacks), and Mirai/Mozi/Gafgyt dominate payloads (~75%). Attackers don't need to defeat the data centre first. Instead, they turn compromised edge devices into persistent footholds, internal scanners, or botnet nodes; they also leverage them as "trusted network neighbors" to enable lateral movement.

- **OT ransomware and cyber-physical service impact**
  ThreatLabz predicts sustained IoT/OT ransomware pressure on critical sectors such as energy, exploiting network interdependencies to disrupt services. In energy, the most expensive incident is not the ransom, it is the forced shutdown, safety risk, manual operations, recovery time, and regulatory/public trust fallout.

- **Supply chain and third-party access as a primary breach path**
  Energy environments are "multi-tenant" by design: OEMs, integrators, maintenance partners, smart-meter vendors, and cloud service providers require remote access. This expands trust relationships, weakens identity assurance, and increases the chance of inherited compromise.

- **AI-era risks: attacks using AI + risks to AI and governance**
  Energy operators are adopting AI for forecasting, dispatch optimization, predictive maintenance, and anomaly detection. This creates two immediate categories of risk:
  - **AI-enabled attacks get cheaper and more convincing.** ThreatLabz explicitly forecasts AI-driven social engineering (hyper-targeted phishing, smishing, vishing with impersonation), requiring AI-driven defences.
  - **AI systems themselves become targets.** Poisoned data, compromised pipelines, model misuse, and prompt-based manipulation can degrade decision quality, dangerous in cyber-physical systems where "bad recommendations" can become unsafe actions.

Attack Case Study: Delivering malware using "blackout siren" phishing campaigns

- The Lure: The Pakistan-linked SideCopy APT group used "blackout siren" themed phishing campaigns and crisis alerts to trick officials and the public.
- Payloads: Deceptive documents like "Blackout Rehearsal Plan" delivered CurlBack RAT malware.

Government of India/Bharat Sarkar
Ministry of Power/Vidyut Mantralaya
Sharam Shakti Bhawan, Rafi Marg, New Delhi

No. FCB/05/22/ Dated, the 5th May, 2025

Subject: Rehearsal for Blackout in Cantonment / Bases Area

Sir/Madam,

This is with the reference to the ongoing conflicts between Pakistan and India. As per the directives of the Hon. Prime Minister, the rehearsal for blackout is starting with effect from 7th May 2025 from 9:00 PM to 10:00 PM at multiple cantonments / bases.

You are requested to ensure adequate security arrangements during this period, given the total blackout. This rehearsal aims to ensure preparedness and effectiveness in implementing blackout procedures during prevailing war threats.

Your support and cooperation are crucial in making this exercise successful.

Yours faithfully,
(ARVIND DHARAMPURI)

- Compromised Infrastructure: Attackers abused legitimate domains, including those associated with organisations like GCH India, to host malware staging files.

In the past, SideCopy was known to target DRDO with a phishing campaign that delivered Action RAT[17].

Source: Zscaler ThreatLabZ

17 https://thehackernews.com/2023/03/pakistan-origin-sidecopy-linked-to-new.html

Attack Case Study: Operation FlightNight (India), Government + Energy targeted

What happened

In March 2024, a threat actor targeted Indian government entities and private energy companies using a modified open-source information stealer (HackBrowserData). The malware was delivered via phishing (a decoy "invitation letter" theme), and exfiltrated confidential internal documents, private email messages, and cached browser data via Slack, which it used as a command-and-control/exfiltration channel. Reported data exfiltration was ~8.81 GB, including financial documents and information related to oil and gas drilling activities.

Why it matters:

- A modern breach can use legitimate cloud collaboration services for data theft, which are harder to spot.
- Credential/cookie theft can bypass "strong perimeter" assumptions, especially where VPN and shared admin practices still exist.

Source: https://blog.eclecticiq.com/operation-flightnight-indian-government-entities-and-energy-sector-targeted-by-cyber-espionage-campaign

How Zero Trust helps

A Zero Trust approach assumes breach, verifies explicitly, and limits blast radius. For power and energy sectors, this is not a slogan. It is an architectural necessity to keep IT compromise from becoming OT disruption.

- **Stop phishing-led compromise from becoming enterprise-wide access**
  Close gaps by continuously evaluating access. Implement Zero Trust controls such as identity-first access for all workforce and contractor access, including strong authentication, conditional access, and device posture checks. Add phishing-resistant MFA for privileged roles, and retire shared accounts and least-privilege

and just-in-time elevation for operational admin tasks. This will ensure that compromised credentials don't automatically grant broad network access.

- **Contain edge and IoT/OT compromise with segmentation ("networks of one")**
  ThreatLabz recommends Zero Trust architectures and advanced segmentation for IoT/OT, explicitly to reduce the attack surface and limit lateral movement. Introduce segmentation between IT, OT, and vendor zones; enforce "device-to-app" or "user-to-app" connectivity instead of network-level access. Treat high-risk assets such as routers, gateways, cameras,and DVR/NVR as untrusted. Monitor continuously and isolate by default. Routers are targeted in 75%+ of IoT attacks. Even if a field device or gateway is compromised, it cannot "walk" to control systems or identity stores.

- **Replace VPN-based vendor access with Zero Trust remote access to specific applications**
  ThreatLabz explicitly advises moving beyond traditional VPNs for privileged remote access to OT systems and using outbound-only connectivity with isolated sessions. Zero Trust controls such as application access without network access for vendors and engineers, outbound-only connectors for sensitive OT enclaves (no inbound exposure) and session recording, command restrictions, and time-bound approvals for OT maintenance will ensure that a vendor compromise no longer puts the plant or grid networks in danger.

- **Make exfiltration harder, noisier, and cheaper to detect**
  Operation FlightNight shows data exfiltration can ride trusted channels such as Slack APIs. To ensure that data theft attempts trigger policy blocks or high-fidelity alerts instead of blending into normal cloud usage, implement Zero Trust controls such as inline data protection controls (DLP, CASB-style controls) for SaaS and web traffic, encrypted traffic inspection and anomaly detection for unusual uploads/downloads (especially from privileged endpoints), tight egress controls for OT-adjacent networks, and default-deny to unknown destinations.

- **Address AI-era risks with "Zero Trust for AI + Zero Trust with AI"**
  ThreatLabz forecasts AI-driven phishing and stresses AI-driven defences. To ensure that AI becomes a force multiplier for defence without becoming an ungoverned attack surface, implement Zero Trust controls for governance, security, and direction. Governance controls include model inventory, data provenance, and approval workflows for AI use in operations. Security controls include isolating AI environments, protecting training pipelines, enforcing least privilege on datasets, and logging all AI-assisted operational decisions. Detection controls include using analytics to spot impersonation patterns, anomalous access, and "living-off-the-land" behavior at scale.

Success Story: NOV Goes All In for Zero Trust

Zero Trust implementation

- Reduced number of cyber events by 35x
- Gave employees and contractors direct, policy-based WFA access to 7,500+ apps
- Shrunk machine reimaging from malware to effectively zero
- Saved millions of dollars by eliminating hardware and simplifying security
- Simplified security administration with policy-based controls
- Established identity-driven Zero Trust security foundation

Source: https://www.zscaler.com/customers/nov

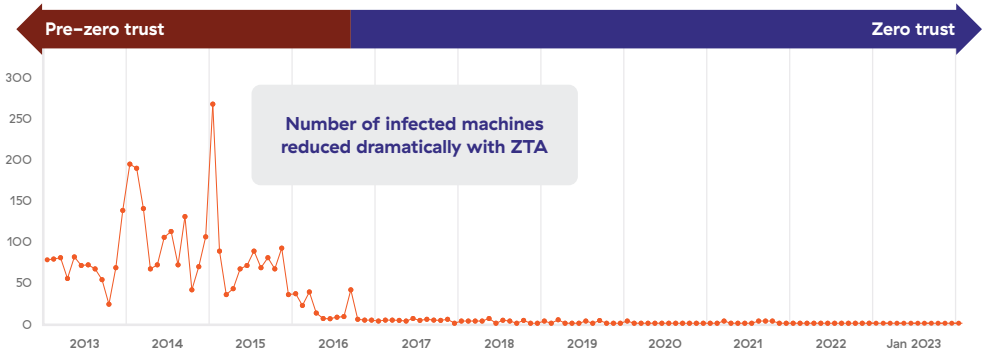


Figure 31: Reduced computer reimaging at NOV after moving to Zero Trust.

For India's Power and Energy sector, the most practical security objective is simple: prevent IT compromise from becoming OT disruption. The sharp rise in energy-targeted attacks and IoT/OT exploitation makes perimeter-era models structurally inadequate. Zero Trust, when implemented as identity-centric access, microsegmentation across IT/OT, vendor access without network access, and strong data controls, all reduce both the probability and the blast radius of incidents, while supporting modernization goals rather than slowing them.

Critical Sectors: Manufacturing and Strategic Enterprise

Sector context and trends

Manufacturing and strategic enterprises are the engines of India's industrial growth, innovation, and national capabilities. This sector includes discrete and process manufacturers, automotive, steel, heavy machinery, electronics, pharmaceuticals, as well as strategic domains such as defence production and space systems. As these environments become increasingly digitized and connected, they are exposed to the same cyber threats seen in energy and government, plus unique risks to industrial control systems (ICS), intellectual property (IP), and mission-critical technological assets.

Industry 4.0 adoption, which includes smart factories, industrial IoT (IIoT), robotics, cloud-connected manufacturing execution systems, and integrated supply chains, has greatly improved productivity and responsiveness. But it also merges IT and OT environments, which dramatically expands the attack surface. OT systems that were once isolated are now connected to enterprise networks and the cloud, exposing core production assets to threats traditionally seen only in IT environments.

Trends Seen

- Zscaler Researchers found
  - Manufacturing is listed as one of the most targeted industries for mobile attacks.
  - The Manufacturing and Transportation sectors jointly account for 40% of all IoT malware attacks (20% share for each sector).
  - Manufacturing is a leading sector in enterprise AI usage, accounting for 20% of AI/ML traffic, driven by modernization efforts and heavy documentation workflows.
- Reports show manufacturing and industrial environments averaging 1,585 cyber threats per week in 2025, attacks that include scanning, malware, and credential abuse. (Manufacturing Today India[18])
- Indian SMEs and plants with limited cyber investment contribute to a broader vulnerability trend, with reported malware infection concentrations rising in industrial hubs. (The Times of India[19])
- CloudSEK reported APT41 (China Nexus) is heavily focused on the Manufacturing sector, utilising supply-chain compromises to gain persistent access to Operational Technology (OT) environments.

Key Risks

Manufacturing and strategic enterprises face a complex web of cyber risks that intersect operational continuity, IP security, safety, and national competitiveness.

- **IT-OT convergence without security maturity**

  The integration of IT and OT systems, without Zero Trust and adequate security controls, creates pathways for adversaries to breach enterprise systems and pivot into industrial operations. OT systems (SCADA, PLCs,

18 https://www.manufacturingtodayindia.com/cyber-threats-in-manufacturing
19 https://timesofindia.indiatimes.com/city/ahmedabad/hacked-2-0-diamond-city-of-surat-is-indias-malware-capital-too/articleshow/124438104.cms

robot controllers) were designed for availability, not threat resistance, leaving them vulnerable to exploitation. Potential impacts include production disruptions and safety incidents.

- **Legacy systems and vulnerable endpoints**
  Many industrial environments run legacy equipment with few or no modern security features. These devices often lack encryption, patch support, or authenticatable access, making them ideal entry points for attackers. These weaknesses enable lateral movement and persistence, even in otherwise modernized networks.

- **Supply chain and third-party exposure**
  Modern manufacturing relies on multi-tiered suppliers, contractors, and service providers, each with varying security standards. Supply chain attacks (where software or components are compromised upstream) have repeatedly demonstrated how a single weak link can expose entire ecosystems.

- **AI-era threats and data/model exploitation**
  Manufacturers are adopting AI for predictive maintenance, quality control, demand forecasting, and autonomous control loops. However, AI can automate sophisticated attack discovery and exploitation at machine scale. Industrial AI models may be subject to data poisoning, model extraction, or misuse via unsecured endpoints. These risks are compounded by the rapid pace of AI adoption without commensurate governance and security risk frameworks.

- **Space sector threats: Sovereignty, data theft, and system integrity**
  Space domain systems are not immune: cyber theft of mission data and credentials is increasingly common, and prime targets include satellite ground stations, command links, and telemetry systems.

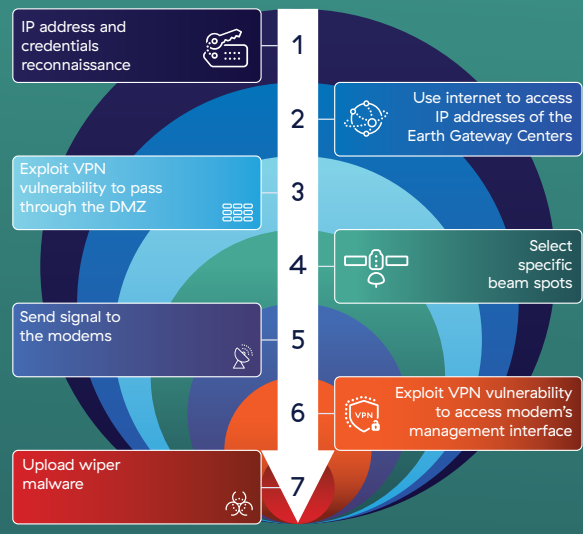
Attack Case Study: ViaSat Cyber Attack

In a widely cited incident, a cyberattack on the KA-SAT satellite communications network disrupted tens of thousands of satellite modems across Europe. Security researchers later identified destructive wiper malware ("AcidRain") used to render terminals inoperable. The impact extended beyond communications, affecting remote monitoring and control systems, including wind energy installations dependent on satellite links.

How the attack worked

- Attackers targeted ground-segment and terminal infrastructure, not the satellite itself
- Malware was deployed to edge devices, permanently disabling them
- Loss of connectivity caused operational outages across dependent sectors

ViaSat Attack Lifecycle



Why this matters for India's strategic enterprises

India's strategic ecosystem, space, defence manufacturing, remote industrial operations, maritime systems, and energy assets, relies heavily on:

- Satellite communications
- Ground stations and field terminals
- Integrated cyber-physical control systems

This incident demonstrates a critical reality: Disabling space-linked infrastructure does not require attacking space assets directly.

Attack Case Study: ViaSat Cyber Attack (cont'd)

India's own cyber threat assessments now explicitly flag space-based systems and satellite-enabled services as emerging strategic cyber risk areas.

Zero Trust takeaway

Zero Trust limits the impact of such attacks by:

- Treating terminals, gateways, and ground systems as untrusted by default
- Enforcing device identity, posture checks, and least-privilege access
- Segregating space operations, analytics, and enterprise IT environments
- Preventing a compromised edge device from becoming a platform-wide failure

Source: Space Cybersecurity Lessons Learned from The ViaSat Cyberattack by Nicolò Boschetti, Nathaniel G Gordon, Gregory Falco, Oct 2022
https://www.researchgate.net/publication/363558808_Space_Cybersecurity_Lessons_Learned_from_The_ViaSat_Cyberattack

How Zero Trust helps

Zero Trust addresses both broad digital risk and deep operational stakes for manufacturing and strategic enterprises:

- **Identity and Access Verification Everywhere**
  Zero Trust factors in controls like multi-factor authentication (MFA) for humans and services, continuous context-based access evaluation, and just-in-time privileged access to make sure that compromised credentials or devices can no longer be the de-facto key to core systems.

- **Segmentation That Stops Lateral Movement**
  To break the usual attacker pattern of jumping from office networks into production or IP systems, segmentation can be used between IT, OT, cloud, supply chain partners, and AI systems; in addition, applying application-level access policies rather than network-wide trust further limits damage.

- **Device Posture and Endpoint Verification**
  Continuous telemetry from endpoints such as industrial controllers, laptops, and sensors along with risk scoring and remediation that gates, automatically throttles, or blocks rogue or compromised devices, all work to reduce exploited-edge risk.

- **Data Protection and Governance**
  To limit illicit data exfiltration and enforce accountability on workspace, cloud, and AI usage, implement data-centric policies for industrial data stores, encryption, DLP, and audit trails across the lifecycle. Use AI governance controls for training and inference workflows.

Success Story: Mahindra Group Enables Secure Transformation

Zero Trust:

- Creates secure digital experiences for users for both digital and physical transactions
- Improves IoT/OT security with Zero Trust policies
- Leverages AI and ML to gain real-time data insights
- Enhances Microsoft suite through close Zscaler partnership
- Furthers ESG initiatives through sustainable cloud usage

Casestudy: https://www.zscaler.com/customers/mahindra

Success Story:
Siemens Empowers Its Global Workforce and Factories with Zero Trust Transformation

SIEMENS

- Deployed Zero Trust controls spanning cloud, IT, and OT domains to enforce identity–first access and application segmentation, dampening insider threat paths and supply chain exposure.
- Replaced legacy VPNs with a cloud–based, software–defined approach that supports secure remote work for all global users.
- Moved beyond perimeter–based security to Zero Trust connectivity between users, applications, and machines across offices and factories.
- Streamlined segmentation and client zone creation for office and factory environments, improving agility and seamless integration of new entities.
- Reduced management and operational costs by 70% through virtualization and simplification of infrastructure.

Casestudy: https://www.zscaler.com/customers/siemens

As India pursues manufacturing excellence and strategic autonomy, embedding Zero Trust into the fabric of technology, operational governance, and industrial cyber risk management will be critical to building sustainable resilience.

Critical Sector: Banking and Financial Services

Sector context and trends

India's banking and financial systems sit at the very heart of its digital economy. India is the undisputed leader in the world in digital payments, with UPI payments accounting for 49% of global transactions[20]. As India advances toward the vision of Viksit Bharat by 2047, the resilience of this sector is not merely a financial concern, it is a matter of national stability and growth.

20 https://www.pib.gov.in/PressReleasePage.aspx?PRID=2200569&reg=3&lang=1

As payment volume has grown, the threat landscape has expanded dramatically. The rise of cloud adoption, remote access, mobile banking, and third-party integrations has blurred traditional perimeters, exposing financial systems to identity-centric, API-based, and mobile-borne attacks.

Yet despite these pressures, BFSI remains India's most cyber-mature critical sector, largely due to early and sustained policy intervention by the Reserve Bank of India (RBI) which issued comprehensive cybersecurity guidelines in 2016 for banks, mandating board-level accountability, continuous monitoring, advanced threat detection, and even proactive techniques such as honeypots and decoys to engage attackers before damage occurs. This foresight fundamentally reshaped how Indian banks approached security, not as perimeter defence, but as continuous risk management.

Trends Seen:

- Zscaler telemetry detected
  - 850k credential brute force attack attempts in just 30 days between Dec 25 and Jan 26 on Banking and Financial sector in India.
  - 9 Indian banks were targeted by attackers exploiting the CitrixBleed-2 vulnerability since October 2025.
  - Targeted attack attempts that exploited vulnerabilities in Fortinet FortiWeb and Microsoft SharePoint 'ToolShell' were detected across 7 Indian banks.
- According to the India Cyber Threat Report 2025, the BFSI sector accounted for over 17% of all cyberattacks observed in India, making it one of the most targeted industries in the country.
- Financial crime and digital fraud are estimated to reduce India's economic growth by nearly 0.7%, while almost ₹1 lakh crore is lost annually due to cybercrime and financial fraud, directly undermining citizen trust and national productivity.

Key Risks

The modern risk profile of BFSI has shifted decisively from infrastructure-centric threats to identity-driven and transaction-level attacks:

- **Advanced financial malware and mobile threats.** The proliferation of Android banking trojans, phishing overlays, and SMS-based MFA bypass techniques has made mobile devices a primary entry point into financial fraud. India has emerged as one of the most targeted geographies for mobile attacks globally, with banking malware being a dominant category.
- **Account takeover and credential abuse.** Attackers increasingly exploit weak authentication, compromise devices, and use social engineering rather than breaking into core banking systems directly.
- **API and fintech ecosystem risk.** Open banking, aggregators, and fintech partnerships have introduced new dependencies where a compromise of a smaller third party can cascade into systemic exposure.
- **Cloud misconfigurations and lateral movement.** As financial workloads move to the cloud, misconfigured access controls and over-privileged identities allow attackers to move laterally once inside.
- **Digital Public Infrastructure (DPI) concentration risk.** DPI platforms amplify both efficiency and impact. A successful attack on shared payment or identity rails can affect millions simultaneously.

How Zero Trust helps

The BFSI sector's relative resilience offers a powerful lesson for other critical sectors: policy–driven adoption of modern security architecture works.

Zero Trust aligns naturally with this regulatory and operational evolution, with a framework that works on multiple levels.

- **Identity as the new control plane:** Zero Trust enforces continuous verification of users, devices, and applications, directly addressing the dominant modes of fraud and account takeover.
- **Least–privileged, transaction–aware access:** Fine–grained access controls limit blast radius, ensuring that a compromised credential or device cannot freely traverse banking systems.
- **Secure access without implicit network trust:** Applications and APIs are protected without being exposed to the public internet, reducing attack surface across cloud and hybrid environments.
- **Resilience for DPI at national scale:** Zero Trust enables segmentation and policy enforcement across shared digital platforms, ensuring that scale does not become fragility.
- **AI–assisted detection and response:** Behavioural analytics and AI–driven monitoring help identify anomalies, such as unusual transaction patterns or device behavior, that traditional controls miss.

The BFSI experience demonstrates that regulation, architecture, and mindset must move together. RBI's early policy leadership created the conditions for Zero Trust–aligned practices to take root, making banking India's most cyber–prepared sector today. As India extends digital infrastructure deeper into governance, commerce, and society, this model offers a clear blueprint. It demonstrates that strong policy signals, coupled with Zero Trust architecture, can convert digital scale from a liability into a strategic advantage.

Success Story:
L&T Financial Services Support Cloud Transformation

With Zero Trust:

- Eliminated 110 different types of threat management devices for a unified, streamlined environment
- Achieved nearly 40% improvement in endpoint security
- Reduced access-related support tickets to almost zero
- Realized significant savings on security hardware, software, and management
- Gained granular visibility, data, and reporting to remediate risks and adopt predictive analytics

Case Study: https://www.zscaler.com/customers/l-t-financial-services

Success Story:
IIFL Elevates Its Security Posture and Vastly Improves Its Risk Score

With Zero Trust:

- Provided users with direct, secure access to the internet, SaaS, and private apps
- Enhanced resilience to cyberattacks with device segmentation, sandboxing, and actionable risk insights
- Boosted data protection with web and endpoint DLP controls
- Enabled real-time, centralized visibility across the environment and prioritized vulnerability risks and security gaps

Case Study: https://www.zscaler.com/customers/iifl

CHAPTER
5

How To Embrace the Zero Trust Journey

With the foundational principle of "never assume trust, always verify" in hand, the strategic implementation of Zero Trust architecture (ZTA) for India's critical infrastructure is not a single deployment, but a phased journey. Leaders responsible for national security and economic stability should execute these five phases in a logical sequence to effectively and systematically dismantle legacy risk and build lasting resilience.

Phase 1: Zero Trust for the Workforce: Securing the Human Element

The journey begins by addressing the greatest and most immediate risk: the compromised identity. In a modern, borderless digital state, the workforce, from government officials to utility operators, accesses vital national assets from any location using various devices. Relying on legacy perimeter tools ignores this reality and amounts to an abdication of responsibility. The strategic imperative here is to establish a Zero Trust platform as the intelligent control plane to enforce continuous, least-privileged access to every application and data set, ensuring that a single compromised credential cannot lead to a catastrophic, enterprise-wide breach.

Phase 2: Zero Trust for Mitigating AI Risks: Securing the Digital Foundation of Innovation

Building on a secure workforce foundation, the second phase must tackle the systemic risk introduced by the deployment of artificial intelligence on shared national compute infrastructure and data commons. AI's reliance on vast amounts of sensitive data and shared platforms makes it a prime target for data poisoning and intellectual property theft. Zero Trust is the necessary architectural safeguard, enforcing least-privileged access not just to the systems hosting AI, but directly to the models and the training data itself, continuously verifying every interaction. As further detailed in Chapter 2, on Using Zero Trust to Mitigate AI Risk, this step is the strategic control point for leveraging AI innovation confidently and securely.

Phase 3:
Zero Trust for the Cloud: Architecting Resilience for Population Scale

Once human and core AI access are secured, the journey shifts to the cloud environment, where India's Digital Public Infrastructure (DPI) and Critical Information Infrastructure (CII) reside. Traditional firewall and VPN architectures fail in complex, interconnected hybrid and multi-cloud environments. ZTA is the only architecture designed for this reality. This phase secures communications between workloads and across cloud boundaries, eliminates the need for expensive and inefficient traffic backhauling, and enforces consistent data protection policies globally. This is essential for reducing the systemic attack surface, mitigating lateral movement within the cloud, and ensuring uninterrupted service delivery for national systems.

Phase 4:
Zero Trust for IoT and OT: Protecting the Physical Foundation

With the cloud environment under ZTA control, the focus moves to securing the physical foundation: the Operational Technology (OT) and Internet of Things (IoT) devices in critical national assets, from power to transportation. These devices were not designed with modern security in mind, making them a prime target for nation-state actors seeking disruptive capability. This phase deploys a Zero Trust approach to isolate these vulnerable physical systems from the corporate network and the internet, strictly controlling and verifying every interaction. This enables least-privileged, highly controlled remote access for maintenance, establishing a security boundary around every individual device to prevent localised compromise from becoming a national catastrophe.

Phase 5:
Zero Trust for Supply Chain: Neutralizing the External Risk Vector

The final phase of the journey extends the ZTA boundary to the supply chain, the third-party vendors, integrators, and partners that represent a proven national security risk. Traditional methods like site-to-site VPNs violate the Zero Trust principle by granting implicit trust to an entire external network. This final decisive action secures this vector by enabling agentless, browser-based, and least-privileged access to only the specific applications required. By eliminating implicit trust and lateral movement for all external parties, leaders can confidently collaborate and integrate vital services without exposing India's most sensitive national assets to unwarranted risk.

CHAPTER
6

Looking into the Future – Quantum Computing

Understanding Quantum Computing Risk

The advent of quantum computing, while promising revolutionary breakthroughs in fields like medicine and materials science, casts a shadow over the current digital security landscape. Our modern digital world, from secure online transactions to encrypted communications and protected national secrets, relies fundamentally on cryptographic algorithms — complex mathematical problems that are practically impossible for even the most powerful supercomputers today to solve. A sufficiently powerful quantum computer would render many of these foundational algorithms obsolete overnight. This presents a looming existential threat to the very underpinnings of our digital trust, potentially exposing sensitive data and critical infrastructure to unprecedented levels of attack. As such, it demands urgent strategic foresight from India's leaders.

One of the most immediate and insidious threats posed by quantum computing is the "harvest now, decrypt later" scenario.

One of the most immediate and insidious threats posed by quantum computing is the "harvest now, decrypt later" scenario. Adversaries, including nation-states, are currently collecting vast amounts of encrypted data, such as national intelligence, sensitive citizen information, proprietary industrial designs, critical infrastructure blueprints, and intellectual property. While this data is secure today with current encryption, the expectation is that once powerful quantum computers become available, these hoarded treasures can be easily decrypted. For data with long shelf lives—information that needs to remain secret for decades—the threat isn't in the distant future; it's active right now. Every piece of encrypted communication or stored data is potentially being collected for future compromise.

Prepare now to adopt post-quantum encryption standards to safeguard data against future decryption threats.

1. **Harvest Now, Decrypt Later**
   Threat actors will capture data now and decrypt later when post-quantum computing becomes viable.

2. **Broken signatures, loss of secure communications**
   Today's encryption standards will be broken in the PQC world.

3. **Attackers plan now to leverage quantum computing as part of their overall arsenal**
   Although quantum computers are not expected until the 2030s, attackers will leverage quantum computing as part of their standard tactics.

Beyond data confidentiality, quantum computing poses a severe risk to the integrity and authentication mechanisms that underpin our critical infrastructure. Digital signatures, which verify the authenticity of software updates, control commands, and secure boot processes for our industrial control systems (ICS) and SCADA networks, could be broken. If digital signatures can be forged, an attacker could impersonate legitimate systems or operators, send false commands to a power grid, manipulate manufacturing processes, or shut down essential services. This breakdown of digital trust would erode our ability to differentiate between legitimate and malicious instructions, leading to chaos and potentially catastrophic physical consequences for the nation.

In response to this looming threat, the global cybersecurity community is actively developing and standardizing Post–Quantum Cryptography (PQC). These are new cryptographic algorithms specifically designed to be resistant to attacks by future quantum computers, while still being implementable on today's classical computers. PQC is the mathematical race against time to secure our digital future before the "quantum break" occurs. This involves entirely new mathematical approaches that are computationally too difficult for even quantum computers to crack, ensuring that our next generation of encryption can withstand this powerful new form of computation.

As a first step, leaders must plan and adopt a quantum–safe strategy. This includes planning for a hybrid cryptography approach by combining quantum–resistant algorithms with existing ones during the transition phase.

The transition to PQC for India's critical infrastructure will be an immense and complex undertaking. Unlike a simple software update, replacing cryptographic primitives often involves changing fundamental components deep within embedded systems, operational technology, and legacy hardware that have long lifecycles. It requires a comprehensive inventory of every system that uses cryptography, a strategic roadmap for migration, rigorous testing to ensure interoperability and operational stability, and significant investment in research, development, and workforce training. This is not a "wait and see" situation; proactive planning and strategic investment in PQC implementation are crucial now to ensure India's national security, economic resilience, and the continued safe operation of its vital infrastructure in the quantum era.

As a first step, leaders must plan and adopt a quantum–safe strategy. This includes planning for a hybrid cryptography approach by combining quantum–resistant algorithms with existing ones during the transition phase. It also requires monitoring developing standards and selecting PQC algorithms recommended by standards organisations.

Using Zero Trust to Mitigate Quantum Risk

Zero Trust architecture plays an important role in the migration to PQC, helping to secure against the harvesting of sensitive data. First, Zero Trust's visibility into traffic flows can enable it to inventory quantum ciphers and provide analytics into quantum–sensitive encryption. Over time, Zero Trust architectures will provide support for PQC key exchanges, allowing for the deprecation of unsecure, current key exchange mechanisms, with the ability to decrypt. Finally, Zero Trust architectures will have post–quantum digital signature support, and will transition to fully quantum–resistant algorithms, allowing optimized PQC–enabled connectivity through the Zero Trust architectures.

Over time, Zero Trust architectures will provide support for PQC key exchanges, allowing for the deprecation of unsecure, current key exchange mechanisms, with the ability to decrypt.

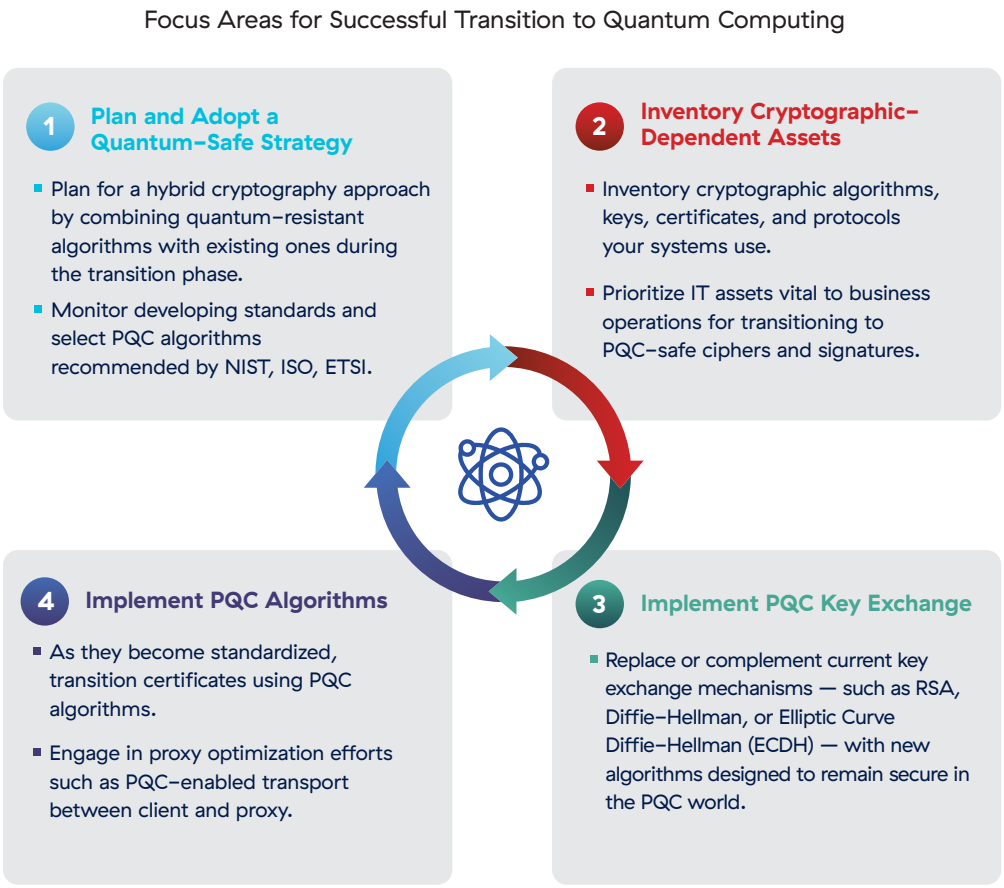


Figure 32: Quantum strategy involves a multi-step process

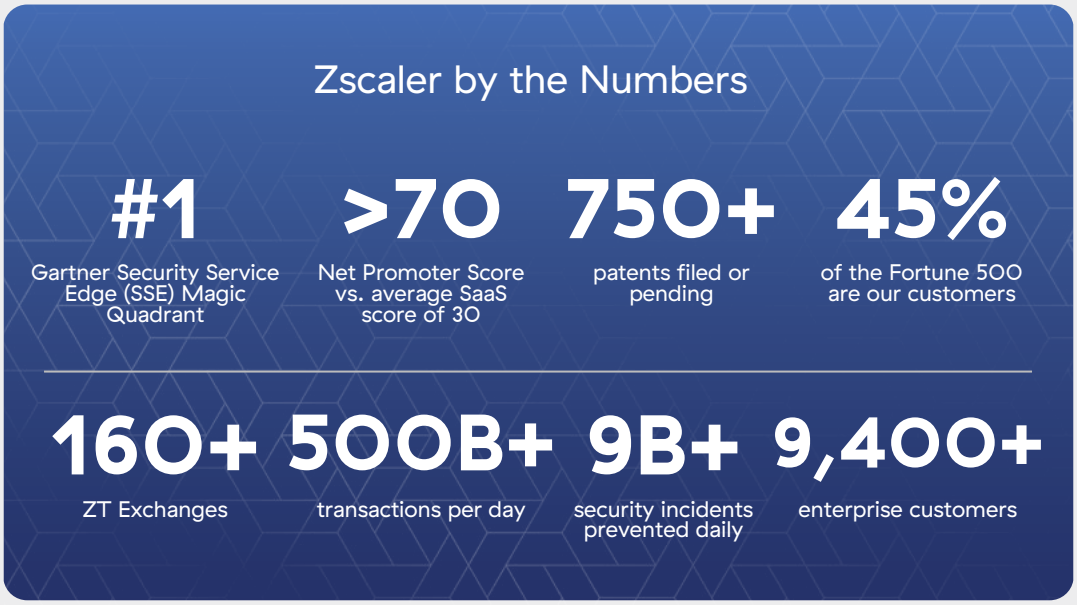
About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers, including 45% of the Fortune 500, from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 160 data centres globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform.

A Foundation in India

India has been integral to Zscaler's journey since its inception in 2007. The company's global foundation was literally laid in the country, with the first lines of code for its pioneering products being written in Basavanagudi, Bengaluru. Today, India continues to be a cornerstone of the company's innovation and operations, hosting a significant and growing part of Zscaler's global workforce.

Zscaler has achieved incredible growth since its founding in 2007, and today exists to create a world in which the exchange of information is always secure and seamless. It's mission is to anticipate, secure, and simplify the experience of doing business—transforming today and tomorrow.


Zscaler by the Numbers
#1
Gartner Security Service Edge (SSE) Magic Quadrant
>70
Net Promoter Score vs. average SaaS score of 30
750+
patents filed or pending
45%
of the Fortune 500 are our customers
160+
ZT Exchanges
500B+
transactions per day
9B+
security incidents prevented daily
9,400+
enterprise customers

The Zscaler Zero Trust Platform

The Zscaler Zero Trust Exchange is a cloud-native, proxy-based security service edge (SSE) platform, purpose-built to deliver security and access directly from the cloud. It functions as the world's largest inline security cloud, distributing security closer to users and applications, rather than backhauling traffic to a centralized data center. By connecting users and workloads directly to applications and data—and never to networks—the Zero Trust Exchange implements the fundamental principle of "never trust, always verify," inspecting all traffic inline to prevent threats and secure sensitive information at scale.

Securing the Workforce

For securing today's distributed workforce, Zscaler's platform delivers Zscaler Internet Access (ZIA) for secure, direct-to-cloud access to the internet and SaaS applications, and Zscaler Private Access (ZPA) for Zero Trust access to private applications, replacing outdated VPNs and firewalls. ZIA provides advanced threat protection, data loss prevention (DLP), and cloud access security broker (CASB) capabilities, while ZPA grants granular, identity-based access to specific applications, eliminating lateral movement risk. Coupled with Zscaler Digital Experience (ZDX), the platform ensures a superior, consistent user experience by optimizing connectivity and proactively identifying performance issues, regardless of user location or device.

Securing the Cloud

Zscaler secures the cloud by extending Zero Trust principles to modern cloud workloads and applications, enabling secure connectivity and segmentation across IaaS, PaaS, and serverless environments. This involves Zscaler Workload Segmentation, which secures application-to-application communication, preventing lateral threat movement within cloud infrastructures. By integrating security into the DevSecOps lifecycle and providing Zero Trust connectivity for workloads accessing the internet or private applications, Zscaler ensures that cloud-native applications and services are protected from evolving threats, misconfigurations, and supply chain vulnerabilities.

Securing IoT/OT

Zscaler extends its Zero Trust architecture to safeguard Internet of Things (IoT) and Operational Technology (OT) environments, which are critical yet often vulnerable. The platform provides secure, granular access for operators and prevents unauthorized access to critical industrial control systems (ICS) and SCADA systems. By segmenting OT networks, inspecting all traffic to and from IoT/OT devices, and applying consistent security policies, Zscaler helps organizations reduce their attack surface, protect critical infrastructure from cyberattacks, and prevent the lateral propagation of threats within these specialized environments.

The Zscaler Zero Trust Platform (cont'd)

Securing B2B

For secure B2B connectivity, Zscaler's platform offers a modern alternative to traditional extranets and VPNs, enabling secure, direct access for third-party partners and supply chain participants to specific applications, rather than granting network access. Utilizing ZPA, organizations can define precise access policies based on identity and context, ensuring partners can only reach the exact applications required for their tasks, drastically minimizing risk. This approach simplifies partner onboarding, enhances collaboration, and protects sensitive corporate data by eliminating implicit trust and preventing partner-introduced threats from impacting the internal network.

Securely Accelerate AI Transformation

Zscaler's AI solution begins with AI Asset Management, which provides a comprehensive inventory and dependency map of all AI applications and models to eliminate "shadow AI" and clarify data lineage. Then, Secure Access to AI Apps leverages Zero Trust controls and prompt classification to safely enable sanctioned AI services while preventing data loss or misuse. The Secure AI App and Infrastructure pillar focuses on the development lifecycle, utilizing automated red teaming and runtime guardrails to protect AI code and the underlying environments. Finally, AI Governance and Compliance ensures adherence to internal policies and global standards through continuous risk monitoring and automated reporting.

Comprehensive Protection

Across all these channels — securing the workforce, cloud, IoT/OT, and B2B — Zscaler's Zero Trust Exchange proactively stops cyberattacks, including ransomware and phishing, by performing full inline traffic inspection and preventing lateral movement. It rigorously secures data through integrated DLP and CASB, ensuring sensitive information never leaves authorized boundaries. Furthermore, Zscaler protects AI by securing access to critical AI applications, models, and data pipelines, treating them as privileged resources requiring strict Zero Trust controls. The cloud-native platform inherently automates operations through centralized policy management, AI/ML-driven threat intelligence, and seamless integrations, significantly reducing complexity and manual effort for IT and security teams.

Benefits of the Zscaler Zero Trust Exchange

The Zscaler Zero Trust Exchange delivers unparalleled benefits, including massive cloud scale and global performance, providing users with the fastest and most reliable access to applications worldwide. Its distributed, cloud-native architecture offers inherent resilience and always-on availability, ensuring continuous protection and business continuity even in the face of outages. By consolidating multiple security functions into a single platform, Zscaler dramatically simplifies IT operations, reduces total cost of ownership by eliminating legacy appliances, and fundamentally improves the user experience by delivering direct, low-latency connections, empowering organizations to accelerate their digital transformation securely.

References

1. Information Technology Act, 2000
   https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
2. DPDP Act, 2023
   https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
3. DPDP Rules, 2025
   https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa?pageTitle=Digital-Personal-Data-Protection-Rules-2025
4. National Cyber Security Policy, 2013
   https://www.meity.gov.in/static/uploads/2024/02/National_cyber_security_policy-2013_0.pdf
5. Cyber Security Infrastructure, Dec 2025
   https://www.pib.gov.in/PressReleasePage.aspx?PRID=2197529&reg=3&lang=2
6. Government of India Taking Measures to Protect Critical Infrastructure and Private Data Against Cyber Attacks, March 2025
   https://www.pib.gov.in/PressReleasePage.aspx?PRID=2116341&reg=3&lang=2
7. NCIIPC Guidelines: https://nciipc.gov.in/NCIIPC_Guidelines.html
8. NCIIPC Rules Notifications, May 2018
   https://www.meity.gov.in/static/uploads/2024/02/NCIIPC-Rules-notification-1.pdf
9. CERT-In Guidelines
   https://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW01
10. RBI – Cyber Security Frameworks in Banks, 2016
    https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/NT41802062016.pdf
11. India AI Governance Guidelines by MeitY and IndiaAI Mission
    https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf
12. Democratizing AI Infrastructure, Dec 2025: https://psa.gov.in/CMS/web/sites/default/files/publication/WP_Democratising%20Access_V3.0_29122025A.pdf
13. Karnataka Cyber Security Policy 2024: https://eitbt.karnataka.gov.in/it/public/policy3/en
14. Telangana Cyber Security Policy 2016
    https://wdcw.tg.nic.in/Notification/Telangana-Cyber-Security-Policy.pdf

15. Zscaler ThreatLabZ 2026 AI Security Report
16. Zscaler ThreatLabZ 2025 Mobile, iOT & OT Threat Report
17. India Cyber Threat Report 2025 – DSCI, SEQRITE
18. CloudSEK, "Cybersecurity in Focus: Recent Threats Targeting India," Aug 2025.
19. eScan / ET Edge, "India's Critical Infrastructure Under Threat: 2026 Report," Jan 2026
20. Carnegie Endowment, "Mapping India's Cybersecurity Administration 2025," Sep 2025.
21. SOCRadar, "Top 10 APT Groups in 2025: Tactics and Trends," Jan 2026.
22. ThreatLabZ Blog: APT-36's Updated Arsenal
    https://www.zscaler.com/blogs/security-research/peek-apt36-s-updated-arsenal
23. ThreatLabZ Blog: European Diplomat targeted by APT29 (Cozy Bear) with WINELOADER
    https://www.zscaler.com/blogs/security-research/european-diplomats-targeted-apt29-cozy-bear-wineloader
24. ThreatLabZ Blog: India Governmental Organisations targeted by APT-36
    https://www.zscaler.com/blogs/security-research/apt-36-uses-new-ttps-and-new-tools-target-indian-governmental-organisations
25. ThreatLabZ Blog: Targeted Attack Delivers CrimsonRAT | ThreatLabZ
    https://www.zscaler.com/blogs/security-research/targeted-attack-indian-financial-institution-delivers-crimson-rat
26. Space Cybersecurity Lessons Learned from The ViaSat Cyberattack by Nicolò Boschetti, Nathaniel G Gordon, Gregory Falco, Oct 2022
    https://www.researchgate.net/publication/363558808_Space_Cybersecurity_Lessons_Learned_from_The_ViaSat_Cyberattack
27. Operation FlightNight
    https://blog.eclecticiq.com/operation-flightnight-indian-government-entities-and-energy-sector-targeted-by-cyber-espionage-campaign
28. Zero Trust Success Stories: https://www.zscaler.com/customers
29. Protection of Critical Infrastructure by May Gen P K Mallick, VSM (Retd.)
    https://www.vifindia.org/sites/default/files/Protection-of-Critical-Information-Infrastructure.pdf

For More Information

Congratulations on becoming well-armed with the knowledge necessary to provide effective cyber risk oversight. The steps provided in this book create a path to navigating the challenges posed by the modern digital world.

The following resources are available for additional assistance:

Zscaler AI: Revolutionizing Cybersecurity for the Enterprise

Zscaler.com

Zscaler, creator of the Zero Trust Exchange platform, uses the largest security cloud on the planet to make doing business and navigating change a simpler, faster, and more productive experience.

Seven Elements of Highly Successful Zero Trust Architecture eBook

An architect's guide to the Zscaler Zero Trust Exchange.

Cybersecurity: Seven Steps for Boards of Directors

Essential guide for board members to understand cyber and Zero Trust.

Seven Questions Every CXO Must Ask About Zero Trust

An executive's guide secure digital transformation and zero trust

Run an Attack Surface Report for Your Domain

What Leaders Are Saying About the Book:

"This book is a must-read for India's policy makers and board members, where trust in our digital journey becomes verifiable and authentic and not simply a presumption. It will help in safeguarding innovation and reputation in our complex digital landscape of the future."

Lt Gen M Unnikrishnan Nair (Retd.) /
FORMER NATIONAL CYBER SECURITY COORDINATOR, GOVERNMENT OF INDIA

"As India builds infrastructure for the next several decades, cyber security must become a leadership imperative. This book clearly articulates why architectures like Zero Trust and AI-driven security are foundational to protecting critical infrastructure at scale. It provides an important perspective for decision-makers shaping the resilience of India's digital infrastructure."

Mr. Ravi Sharma /
FORMER CEO - ADANI POWER LIMITED, ALCATEL LUCENT SOUTH ASIA
CHAIRMAN - TELECOM EQUIPMENT MANUFACTURERS ASSOCIATION (TEMA)

"DPDP compliance cannot be achieved through legal documentation alone unless security-by-design is embedded into digital systems. Zero Trust Architecture (ZTA) translates statutory intent into resilient, verifiable, and citizen-centric safeguards. This book offers timely and essential guidance for leaders responsible for securing India's critical information infrastructure."

Dr. G K Goswami, IPS /
DIRECTOR, UTTAR PRADESH STATE INSTITUTE OF FORENSIC SCIENCE, LUCKNOW, INDIA

Published by:

zscaler™ | AI & Cyber Threat Research Center — India

Price: Rs 1400

Dedicated to building a cyber-resilient and secure digital ecosystem in India, through focused research on AI & cyber threats and conducting training to develop the national talent pipeline and close critical skill gaps.

ISBN 979-890333906-8