Zero trust:

From aspiration to rapid implementation

Capgemini

Zero trust has become an essential cybersecurity philosophy for organizations.

The steady trickle of zero trust security awareness since its principles were formalized in 2004 has built to a flood of adoption today.

The way we work has changed radically, with remote working commonplace and office occupancy rates in the US and UK at record lows.[1] The traditional hard shell/soft interior cybersecurity model that has dominated for decades is virtually obsolete.

Before 2020, when users made requests for flexible remote working, the cybersecurity to support it was often regarded as “too hard”. The global pandemic forced the pace of change and a change in mindset. Organizations now facilitate remote working, support collaborative working with partners and suppliers, and many have moved much of their IT to the cloud. Industry intelligence provider Gartner has predicted that IT spending on cloud-related categories will continue to grow, reaching 51% by 2025.[2] This has implications for the demands such transformation will place on businesses’ cybersecurity.

As cloud adoption continues, cyber-attacks are simultaneously increasing to the point where the cost of cybercrime is predicted to reach $10.5 trillion by 2025.[3] Increased geopolitical tensions too, have increased the number of external cyber attackers, their motivation, and the resources available to them.

Given this context, organizations now realize that there is no longer a clear, easily definable cybersecurity perimeter around their networks, with every device potentially vulnerable Cyber defense can be ramped up by moving protection closer to assets, an approach known as deperimeterization, which is underpinned by the zero-trust philosophy.

The zero trust philosophy: Trust no one

The acceleration towards widespread adoption of zero trust became undeniable when, in 2021, the US government mandated all federal agencies to adopt zero trust principles by 2024.4 The US federal standards agencies, the National Institute of Standards and Technology (NIST), and Cybersecurity and Infrastructure Security Agency (CISA), have set up vendor-agnostic frameworks to help organizations move towards zero trust approaches. In zero trust, the security default is that “everything is broken”, and any part of the system may be compromised, rather than a presumption that a person, device or system can be trusted because they are working in a trusted location. For every access request, a user or device must build up enough trust before access is granted, wherever they are.

Traditionally, a single authentication and authorization decision allowed wide-ranging access to internal systems and data, which was a security risk as a user or device could be compromised at any time. With zero trust, the core principle is the adaptive evaluation of trust. This is dynamic and context-based, and aims to establish information about the user and device through a process of interrogation every time access is requested. The following questions are typical:

- Could the user be accessing from a device that may be compromised?
- Are they accessing within normal working hours, or did they start accessing at midnight and from an unusual location?
- Which network are they using?
- How sensitive is the system or data to which they are requesting access?
- Did the user authenticate using a simple password or a more secure method?
- Is there a known security vulnerability in the service that the user is attempting to access?

[1] Akila Quinio, “*Office space vacancies in US and London reach at least 20-year highs*”, The Financial Times, January 24, 2023

[2] “*Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025*”, Gartner, February 9, 2022

[3] *Cybersecurity Trends & Statistics For 2023; What You Need to Know*, Forbes, March 2023

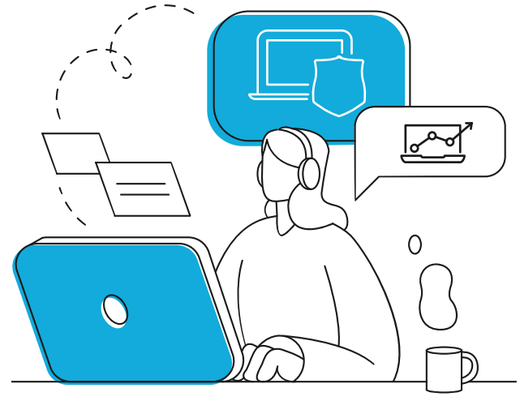
Moving to zero trust: Vision and structure

The complexity and change in organizational behavior required when moving to zero trust is not to be underestimated and will affect the business at all levels. It is a change in approach to cybersecurity governance that feeds into operating models and principles, architecture and design, processes, and, of course, technology.

Buy-in from the C-suite, such as the chief information officer or chief technology officer, and collaboration across towers of the business are essential for success. In creating a vision for transformation, business leaders should apply a full spectrum approach to designing a long- term program for implementation.

This gives a clearer view of the final cost of changing organizational architecture and the best route to zero trust’s full security advantages. Business goals should determine the final technology goals, not the reverse.

If there is no commanding vision of the ultimate destination, costs are likely to mount, as each technology tower, business unit or site moves separately to new models and buy their own solutions, with a strong possibility of compatibility issues and unnecessary costs due to duplication. A rigorously structured change program will deliver a more secure system and lower the total cost of ownership through agreement on a common, consolidated technology stack and approach.



The zero trust organizational structure - upheld by pillars

Responsibility for implementation of cybersecurity measures is often distributed across various groups or towers, for example, between identity, network, operational technology, and engineering teams.

The CISA model for zero trust (figure1) is divided into five pillars: identity, devices, networks, applications, workloads (e.g., virtual machines and containers), and data. These are above three foundational layers: visibility and analytics, automation and orchestration, and governance. Each pillar can generate the signals and metrics used to make smart access control decisions. For example, device posture data, such as OS and browser version, or disk encryption and antivirus status, could indicate that the device is at increased risk of being compromised.

Since zero trust controls are distributed and delegated throughout all five pillars and the organization, this may represent a challenge for those who are used to the established structure and allocation of responsibility for security. This makes change management communication a priority for effective acceptance.

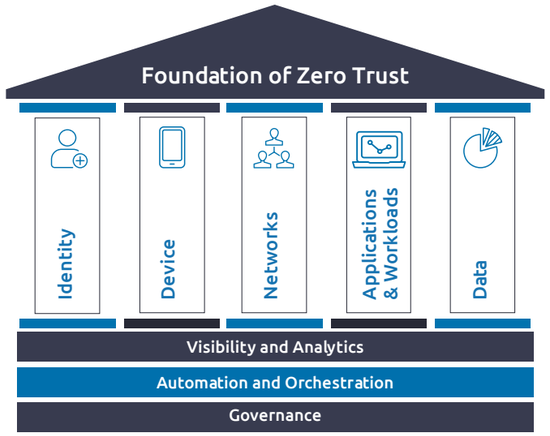


figure 1 Cisa Zero Trust Maturity Model

Faster, smarter, and safer decision

The decision center of zero trust is the policy engine. It is here that trust is defined, metrics are set, and the barrier to access requests is hence established. The availability of ample bandwidth, machine learning and AI, and fast processing at relatively low cost have come together to make zero trust signal analysis viable in real time.

The policy engine relies on a range of data sources to generate signals and finalize an access decision. These can include information on:

- Software components and operating systems;
- Industry compliance.
- Threat intelligence.
- Software flaws or reported attacks.
- Network and system logs.
- Data and system access policies.
- Public key infrastructure.
- Identity management; and
- Security information, such as authentication status.

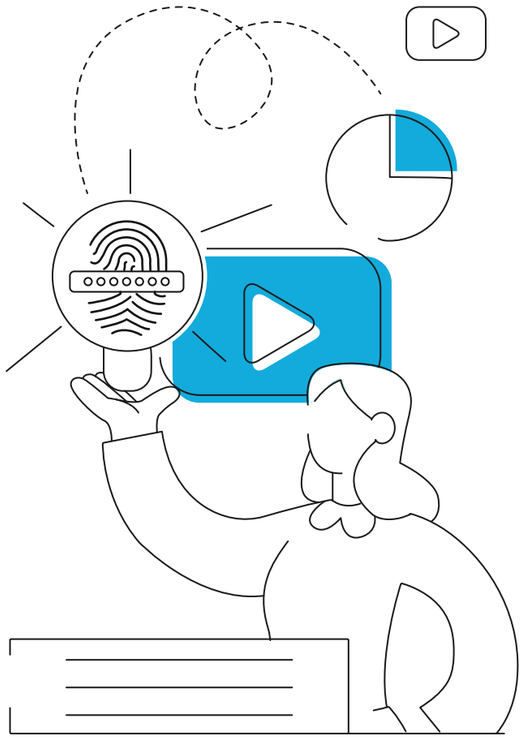
The policy engine feeds the full range of inputs to a trust algorithm, which leads to an access decision. Signals that can show suspicious activity are processed at the automation and orchestration layer (as per the CISA framework). The architecture makes possible fully automated, dynamic, context-based, least-privilege access to services and data; and interoperability with continuous monitoring and centralized visibility.[5]

While zero trust is a major step forward in cybersecurity, it is more than just that. It is a model for governance that shapes ownership of the overall vision, transformation program and outcomes. It sets business-aligned security policy and allocates responsibility to stakeholders. It also determines if a particular implementation results in a successful transformation in operations.

In the conversion to zero trust, the new environment has to be designed with metrics in place to demonstrate success and effectively manage efficiency and costs.

Examples of how these metrics could demonstrate value:

- A reduction in insurance costs, where an insurer recognizes reduced risk of cyber-attack by moving to zero trust
- Improved user experience, proven via employee surveys and metrics from Zscaler Digital Experience (ZDX)
- Fewer security incidents by eliminating exposed internet attack surface, lowering operating expenses
- Reduced cost of migration to cloud services using a consistent approach
- Reduced networking costs by swapping expensive
- routing links (e.g., MLPS) for Zscaler via internet
- Reduced total cost of ownership for security through tooling consolidation.



[5]Cybersecurity and Infrastructure Security Agency, "*Zero Trust Maturity Model, Version 2.0*", April 2023, p.9

Damage limitation through micro segmentation

A major vulnerability of the hard shell/soft interior model has been the freedom an attacker has had to do as much damage as they wanted once they managed to break through the hard shell around an organization's network. Zero trust's micro segmentation capability reduces the affected area of an attack.

Common practice has been that each application has had either an associated certificate, or username with a password, which it can use to access other applications and data. Credentials can be found on the dark web, for example, through a leak to a GitHub repository, or in a carelessly saved text file, or through capture and replay. This enables attackers to masquerade as an application, or other workload. Once in the soft center, they often have the freedom to attack at will.

In the zero-trust model, access may still be possible, but a signal that the user is accessing from an unusual place, or that an application is accessing certain unusual data, will trigger an alert and begin an interrogation process with contextual questions to identify a potential compromise, and subsequently block it. We also implement the principle of least privilege, by which users and applications are only allowed access to the services and data that they need to fulfil their function. For example, rather than controlling which servers can talk to other servers, we control which specific applications on those servers can talk to other applications.

Simplification for mergers and acquisitions

In a merger or acquisition situation, organizations need to consolidate their networks and security tooling, which might describe an edge router, a firewall, a VPN — hardware for Internet connectivity. Each party will bring their own wide area network (WAN) and related network security tooling in data centers and a merger/acquisition has strict deadlines to adhere to for change of control requirements, requiring integration under pressure.

During integration, a cloud-delivered zero trust network access service such as Zscaler, a leader Protecting legacy systems in zero trust solutions, allows users to access applications without requiring extensive network changes or delivering connectivity via a remote access service like a VPN. It consolidates technology sets from different businesses by providing the same set of capabilities in one package. Enterprises can publish their business applications to a central exchange, from where users can request access regardless of which business entity they are from. This brings considerable simplification and acceleration to mergers.

Protecting legacy systems

There has been a monumental shift to cloud-based systems, but aging IT infrastructure persists and requires protection. Shifting to zero trust brings cost savings through safe retirement of legacy security technology but change can be difficult to implement in legacy environments. With zero trust, security is achieved by ring-fencing legacy systems, putting controls around the boundary, and blocking access unless a request for access passes all checks. Similarly, a user will not be able to exit the legacy environment without passing context-based zero trust checks.

Zero trust for a global pharma group

A large pharmaceutical group with more than 150 locations globally and over 20,000 users brought Capgemini in to deliver zero trust as part of a larger infrastructure re-design.

The infrastructure was complex due to multiple system architectures after a series of mergers and acquisitions. It was also expensive to maintain with numerous gateway devices, software agents, identity sources and security policies.

The goals for the program were:

- Improve the user experience with corporate applications and service access in a hybrid environment, which would also bring productivity benefits
- Reduce the visible attack surface of critical business services and applications
- Initiate a 'least privilege' policy for users, meaning limiting user access to the specific data, resources, and applications needed for a task
- Meet users' expectation of "anytime, anywhere, any device" (ATAWAD).

The client set two strategic objectives. Firstly, to achieve a return on investment for capital expenditure (CAPEX) and operational expenditure (OPEX) while the zero-trust journey was underway. Secondly, to enable the group to progress future mergers and acquisitions regardless of identity sources and network constraints.

Capgemini executed a customer transformation program to adapt a modern digital landscape to one where the Internet became the corporate network. This included creating a corporate zero trust roadmap and identifying relevant future use cases to define the architecture accordingly.

Using an end-to-end process, the project achieved significant user experience enhancement. This was achieved with a single zero trust Zscaler Private Access software agent and streamlined global technical infrastructure for internal applications access, simplifying ongoing management. The transformation also led to OPEX and CAPEX optimization via a dynamic cloud-based security services consumption model.

Capgemini's end-to-end methodology for zero trust implementation

Capgemini's approach to delivering zero trust for clients begins with analysis of an organization's culture, goals, and business strategy. It is vital that security architectures and solutions align with and support the greater business goals.

We review the current security capabilities of the organization with respect to zero trust, in alignment with the industry standard maturity model developed by the US security agency CISA.

We help our clients with all elements of zero trust, from governance, operating models, and principles, through architecture and design, all the way through to implementation (technology and process) and managed services once in operation.

Our teams can either work with you, to enable knowledge sharing; or for you, to transform your security approach and implement secure zero trust environments, embed new governance structures, and manage operational services. We build, configure, and integrate new technology solutions and operate these services from secure locations across the globe. This enables us to provide modern, dynamic, and context-based access control and full security monitoring and incident response, 24x7.

Contact

Lee Newcombe
Cybersecurity Director
lee.newcombe@capgemini.com

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the future you want | www.capgemini.com

GIS_042024_SC