

CXO REvolutionaries

Seven Questions Every CXO Must Ask About Zero Trust

An Executive's Guide to
Secure Digital Transformation

AUTHORS

Sanjit Ganguli, VP, Transformation Strategy
Nathan Howe, VP, Emerging Technology
Daniel Ballmer, Senior Transformation Analyst

SPONSORED BY:  zscaler™

Published May 2023

Second Edition

ISBN Number: 979-8-9871864-9-7

© 2023 Zscaler. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

ABOUT THE AUTHORS

Sanjit Ganguli (Zscaler VP, Transformation Strategy), Nathan Howe (Zscaler VP, Emerging Technology), and Daniel Ballmer (Zscaler Senior Transformation Analyst) bring substantial insights on zero trust with careers spanning the globe and companies including Gartner, Blackberry, Nestle, Riverbed, and Verizon. Their leadership and innovative views on cloud, security, transformation, and emerging technologies make them the authorities in zero trust strategy.

Table of Contents

INTRODUCTION		2
QUESTION 1	What is zero trust and why is it critical for secure digital transformation?	4
QUESTION 2	What are the main use cases for zero trust?	34
QUESTION 3	What are the business benefits of moving to zero trust?	52
CXO ADVICE	Alex Philips, CIO, NOV	72
QUESTION 4	How does zero trust drive success for organizations?	82
QUESTION 5	How is zero trust architecture deployed and adopted? What are some common obstacles?	99
CXO ADVICE	David Cagigal, Former CIO, State of Wisconsin	112
QUESTION 6	What are the non-technology considerations for successful adoption of a zero trust architecture?	117
CXO ADVICE	Larry Biagini, Former CIO/CTO, GE	128
QUESTION 7	What do I look for (and not look for) in a zero trust solution?	132
SUMMARY	Seven answers every CXO should know about zero trust	138
APPENDIX 1	Communicating the value of zero trust to the board of directors	145
APPENDIX 2	Evaluating the resiliency of the Zscaler Zero Trust Exchange	148

Introduction

Successful organizations are evolving through secure digital transformation. This can only be achieved by modernizing the organization's applications, networks, workforce, and security. Transformation makes business more agile and more competitive, decision-making improves as information is available more quickly, and user productivity improves while security risk goes down. Done correctly using zero trust architecture, this transformation can also decrease overall cost and complexity.

Secure digital transformation is a journey, not a single project or product. It is a change of mindset and culture. Inertia is a powerful thing, and people throughout an organization like to continue doing what they've always done. This is why executive leadership (CTOs, CIOs, CISOs, and Heads of Infrastructure) needs to drive this transformation from the top-down.

While a deep understanding of zero trust architecture is necessary for enterprise and security architects, it has become clear that CXOs also have many questions about the seemingly vague nature of zero trust and how it enables secure digital transformation. The need for a book targeted directly toward IT and security executives became clear. This book focuses on how zero trust enables secure digital transformation, the benefits of zero trust, obstacles to achieving zero trust, CXO best practices, and their journeys to achieve ideal outcomes from zero trust initiatives.

Understanding zero trust should not be limited to just those CXOs responsible for IT. Security breaches, data loss, and poor user experience do not discriminate and affect every level of an organization. Increasingly, anyone in the C-suite and the board can be involved in these discussions (or be quoted in the press following an incident), so an understanding of security posture and zero trust initiatives is critical.

This book is organized into seven broad questions and sub-questions that every CXO must ask about zero trust, including what it is, how it is beneficial, what others have done, how to deploy and operate, how to select a solution, and how to navigate obstacles. These questions are answered generally and then from a Zscaler perspective, along with commentary from actual CXOs who have transformed organizations themselves.

This is Zscaler's third publication in the “Seven” series—past publications include *Seven Elements of Highly Successful Zero Trust Architecture*, which focuses on zero trust architecture ([ZTA](#)), and *The 7 Pitfalls to Avoid When Selecting an SSE Solution*, concentrating on the security service edge ([SSE](#)). Both of these books are targeted toward enterprise and security architects.

**SECURITY BREACHES, DATA LOSS,
AND POOR USER EXPERIENCE
DO NOT DISCRIMINATE AND
AFFECT EVERY LEVEL OF AN
ORGANIZATION.**

QUESTION ONE

What is zero trust and why is it critical for secure digital transformation?

Question 1 What is zero trust and why is it critical for secure digital transformation?

Digital transformation is a heavily used term for an all-encompassing undertaking that affects the CXO role more than any other initiative. Wikipedia defines it as “the adoption of digital technology by an organization to digitize non-digital products, services, or operations. The goal for its implementation is to increase value through innovation, invention, customer experience, or efficiency.”

The COVID-19 pandemic accelerated the need for businesses to transform to stay competitive. So, while “transformation” has become a buzzword, organizations must stay competitive in a world where success is increasingly influenced by technology. Digital is the new word for “modern.”

At heart, a digital transformation is about connecting all the components of an organization: its customers, its suppliers, its employees, and its physical assets. While bringing fantastic progress, this also embeds major new risks.

Transforming digitally must be done in a secure way, and this is difficult as cyber threats increase, workers become more mobile, and apps become distributed. It means that transformation needs to happen in several ways, including transforming application, network, and security architecture to cope with the modern trends in cloud and workforce mobility. This ultimately leads to improved productivity, reduced risk, and lower cost and complexity.



Figure O1: The three pillars of secure digital transformation: application, network, and security.

Question 1 What is zero trust and why is it critical for secure digital transformation?

Specifically, the fundamental goal of network and security transformation is to address how data is secured and how information is accessed. This is where zero trust architecture comes into play.

HOW IS DIGITAL TRANSFORMATION MADE TO BE SECURE?

BY TRANSFORMING:



**DATA
SECURITY**



**INFORMATION
ACCESS**

Adequately providing data security and secure information access is challenging for organizations today. Over the last 30 years, many companies have been building “hub-and-spoke networks” where every branch is connected to the data center over a private network. They then deployed numerous and disparate security appliances or networking appliances, like routers, switches, and firewalls, to protect the data center where all the applications sat.

This model worked well when the data center was the center of gravity and employees mostly worked in an office. However, application transformation has moved most applications to the cloud, where companies are embracing software as a service (SaaS) or moving/building applications in the public cloud like Microsoft Azure or Amazon Web Services (AWS). Sensitive data is now everywhere. Additionally, employees and contractors in the post-pandemic workplace are working from everywhere. This change resulted in the architecture of hub-and-spoke networks (also called “castle-and-moat security”) jeopardizing data security and proper information access.

Question 1 What is zero trust and why is it critical for secure digital transformation?

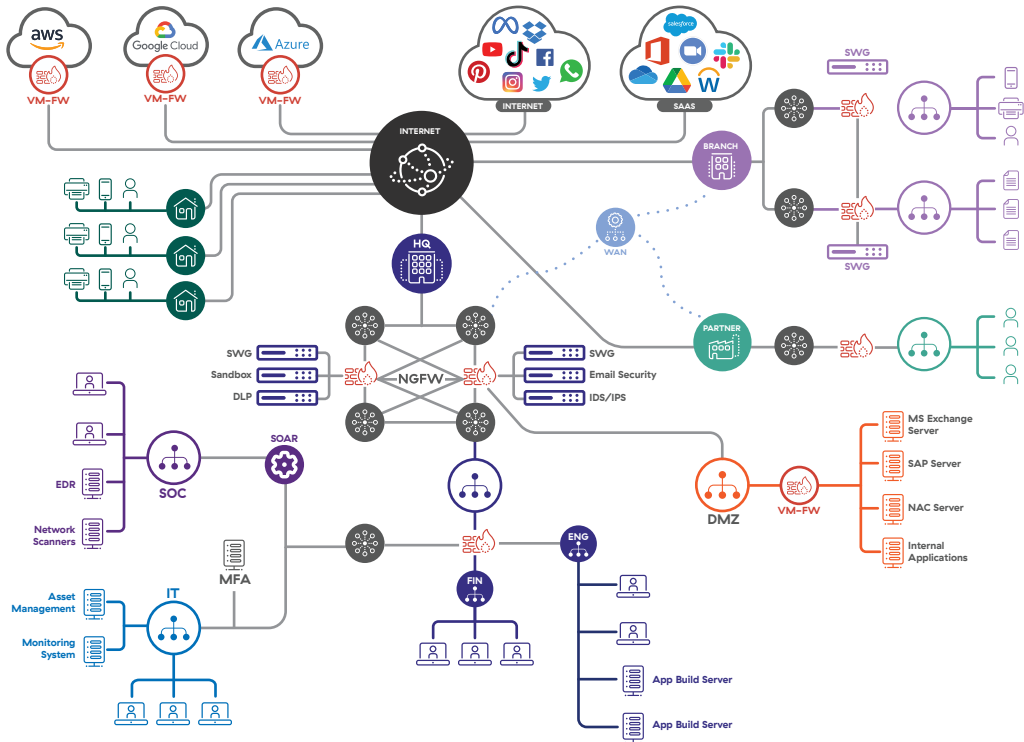


Figure O2: Traditional hub-and-spoke network and castle-and-moat security fail to adequately secure business resources.

Legacy architectures do not provide an optimal user experience because they introduce unneeded latency and complicated routing to reach applications. Users should have direct access to applications for both efficiencies of use and security, which requires a transition from a hub-and-spoke network to direct connectivity. Who likes to fly from San Francisco to New York via Houston, instead of flying direct?

When this required cloud transformation is completed, security breaks because security remains in the data center. This necessitates security transformation—a move away from the castle-and-moat model based on firewalls and VPNs. Enter zero trust architecture (ZTA), which transforms both data security and information access.

Question 1 What is zero trust and why is it critical for secure digital transformation?

The challenges caused by legacy network and security architectures are pervasive and long-standing, and require rethinking the way connectivity is granted in the modern world. This is where ZTA is leveraged—as an architecture where no user or application is

ZERO TRUST IS BASED ON LEAST-PRIVILEGED ACCESS... TRUST IS ONLY GRANTED ONCE IDENTITY AND CONTEXT ARE VERIFIED, AND POLICY CHECKS ARE ENFORCED.

trusted by default. Zero trust is based on least-privileged access, which ensures that trust is only granted once identity and context are verified, and policy checks are enforced.

The US National Institute of Standards and Technology (NIST)

defines the underlying principle of a zero trust architecture as “no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)” (NIST Publication 800-207). It’s an overhaul of the old proverb “Never trust. Always verify.”

This approach treats all network communications as hostile, where communications between users and workloads or among workloads are blocked until identity-based policies validate them. It ensures that inappropriate access and lateral movement are prevented. This validation carries across any network environment, where the network location of an entity is no longer a factor and not reliant on rigid network segmentation.

Why do I need to transform now and why can't I keep doing what I've been doing?

Let's dig a little bit deeper into why, after spending millions of dollars on network and cybersecurity, organizations still have major security risks and experience breaches. The main problem is the IP-based networking architecture designed in the late eighties created an ever expanding corporate network where users and applications were all interconnected. Companies like Cisco built great routers and switches so an enterprise could extend its data center to every branch office, warehouse, factory, etc. In this networking model, if an employee was granted access to the network, he or she could move laterally and access these data center-hosted applications. This happens because the network is routable. Users and applications occupy the same network. This represented a big breakthrough for networking and distributed computing. Unfortunately, this approach cannot adapt to the world we live in today.

As the need arose for people to work remotely, remote access virtual private networks (VPNs) extended the network to every household. Employees working from home or on the road could access the network from anywhere and move laterally to access applications. The VPN makes it appear as if the employee is in the office while sitting at home, in Moscow, or wherever they may be. If there are 50,000 users, the VPN extends the network to 50,000 households.

Couple this predicament with the embrace of the public cloud. Because users and applications must be on the same network, there is now an extension of the network to every cloud region.

Question 1 What is zero trust and why is it critical for secure digital transformation?

To mitigate some of these challenges, and since physical security appliances don't work well in cloud environments, organizations began to spin up virtual firewalls and virtual private networks (VPNs) in the cloud, deeming it cloud security. It is not. A firewall is still an IP device, even in the cloud. A VPN is still an IP device, even in the cloud. Wherever those virtual instances are spun, the corporate network gets extended to those locations. As it starts growing, it turns into a big, flat network that can and will create headaches as it enables lateral movement for users as well as for attackers.

There are four key stages, or steps, attackers take to breach organizations even after organizations have spent millions of dollars on next generation firewalls and VPNs.

**ZERO TRUST ARCHITECTURE
HELPS ELIMINATE THE
ATTACK SURFACE.
IF YOU'RE REACHABLE,
YOU'RE BREACHABLE.**

01 The bad guys find your open attack surface.

What is the attack surface? Every IP that resolves to the internet for the company is an attack surface. It may be applications. It may be the firewall and the VPN. All those systems with vulnerabilities, like servers with outdated encryption standards, can be compromised. Zero trust architecture helps eliminate the attack surface. If you're reachable, you're breachable.

02 The bad guys compromise your network.

Every compromise comes from the internet and looks for weak links, like unsuspecting users or unprotected devices, to compromise them and set up a beachhead. This beachhead is leveraged to launch further attacks. The goal should be to prevent compromise.

O3 The bad guys get on your routable network and move laterally to find high-value targets.

This is what happened with Uber and Colonial Pipeline, among many other examples, where a single machine becomes infected due to the VPN. Since it is on your corporate network, a hacker can traverse laterally across the whole, flat network and bring down every system or application. Or, they can encrypt your data and demand ransom. This is when companies try doing network microsegmentation, which is extremely difficult. It is like building a highway system of toll booths and toll roads to regulate access. A zero trust architecture, on the other hand, eliminates lateral threat movement.

O4 The bad guys steal your data and the stolen data is almost always sent to the internet.

Data is the crown jewel of any organization, and the loss of data means a loss of intellectual property, loss of trust among customers, and a blow to brand reputation. Data loss must be prevented.

In order to minimize the risk of cyber breaches, organizations should embrace zero trust architecture for protection from cyber breaches and data loss, and this architecture can't be bolted on firewalls and VPNs. However, doing nothing puts organizations at increased risk of attack, while sacrificing user experience.

Question 1 What is zero trust and why is it critical for secure digital transformation?

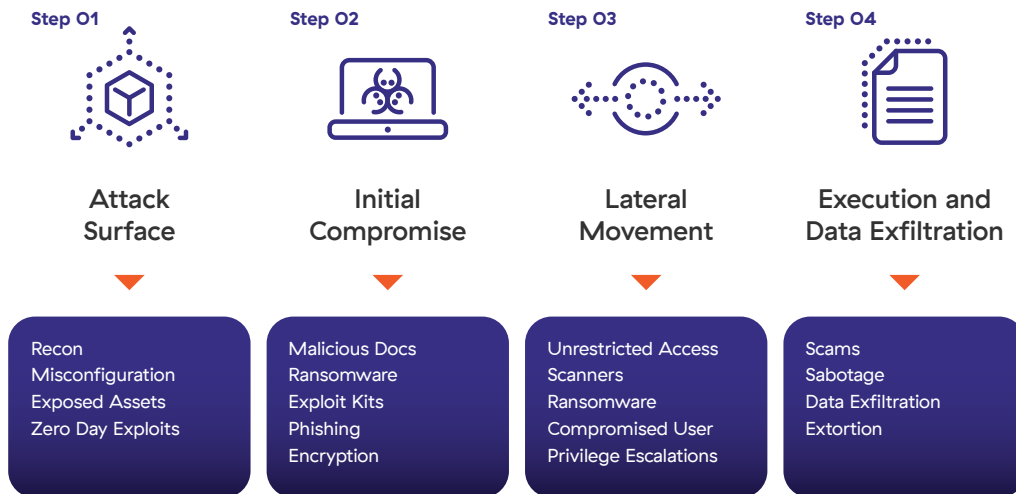


Figure 03: The four-stage attack chain used by bad actors to breach an organization.

Why switch to zero trust now?

IT leaders started doing application transformation to the cloud by lifting and shifting the applications. Then they realized that this did not give them many productivity benefits. Now they are building cloud-native applications using Platform-as-a-Service (PaaS) platforms that provide many productivity functions and tools.

Similarly, network and security transformation is in the first phase of its journey to the cloud. Customers are lifting and shifting 30-year-old routable network and firewall technology to secure their applications using the castle-and-moat architecture. This is complex, costly, and not very secure. To do security and network right for the cloud and mobile world, CXOs need to embrace a cloud-native zero trust architecture that eliminates a routable network to the cloud.

How zero trust architecture provides better cyber protection than traditional castle-and-moat security

Of the four stages of breach, stage 1 (attack surface) and stage 3 (lateral movement) are the least understood by IT and security professionals. This is because traditional network security using firewalls was never designed to tackle these issues. To illustrate, consider two analogies that describe and contrast the zero trust and firewall-based architectures.

HOW TO PREVENT LATERAL THREAT MOVEMENT ON YOUR NETWORK

The first step is NOT putting users on the network, but instead connecting them directly to applications after performing identity and context verification. How does one reach an application without being on the network? It sounds a little complicated, so the following is a simple analogy.

If a guest comes to the company headquarters and enters through the front entrance, they're going to be greeted by the receptionist who will check their ID. If the identity of the visitor is verified, they receive a badge. If they are told to go to a specific meeting room without an escort, the visitor may decide to wander around, and go to any room that is unlocked. They may go to an adjacent building since everything is interconnected, then snoop around, steal data, leave behind dangerous material, and depart unnoticed. This is not a good idea. That's why prudent companies do not allow unescorted visitors.

Question 1 What is zero trust and why is it critical for secure digital transformation?

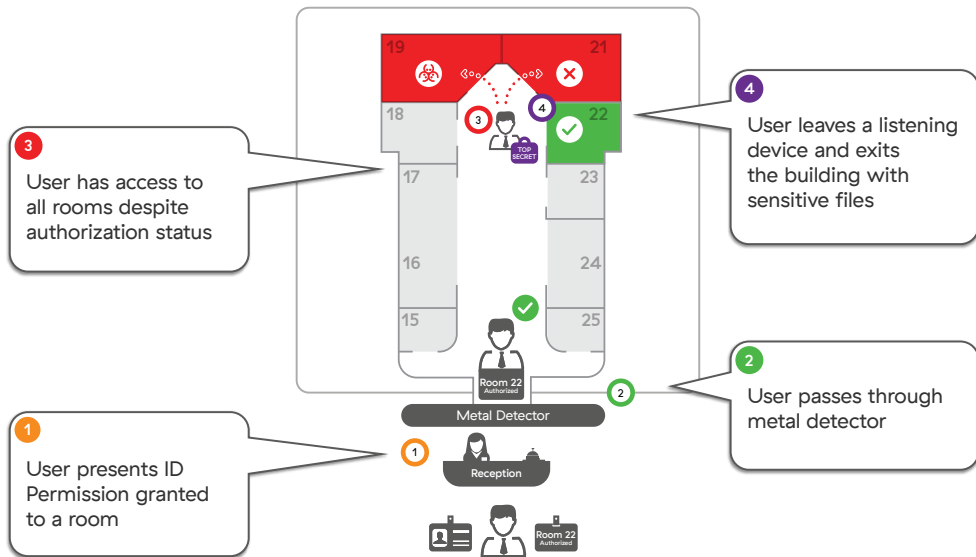


Figure O4: Legacy firewall and VPN security is similar to allowing unescorted visitors to freely wander the entire office building after checking in at reception.

Applying this analogy to lateral threat movement, once the users get on the network (either by being in the office or by using a VPN), they can traverse laterally and find hundreds and hundreds of applications and systems. How does one avoid this? The answer is zero trust architecture. To continue with the visitor analogy from above, ZTA would:

- Remove any identifying company logos and scrub its location from any internet and map sites so visitors can't even find the campus.
- Remove the tunnels that connect the buildings on campus so each building is isolated, which prevents lateral movement.
- Move the receptionist far away from the building, so outsiders can't determine which building the receptionist manages.

Question 1 What is zero trust and why is it critical for secure digital transformation?

With ZTA, visitors still stop at the receptionist, have their ID verified, and receive a badge. This time, they'll be taken to a specific room by an escort. Before the visitor enters the room, their luggage is checked for dangerous material (malware, from a security standpoint), and if all is good, the visitor is escorted directly to the specifically authorized meeting room, no loitering allowed. Once the meeting is over, the visitor is escorted out. Before the visitor exits, however, their suitcase is checked for any stolen goods; in ZTA, this translates to data loss prevention (DLP).

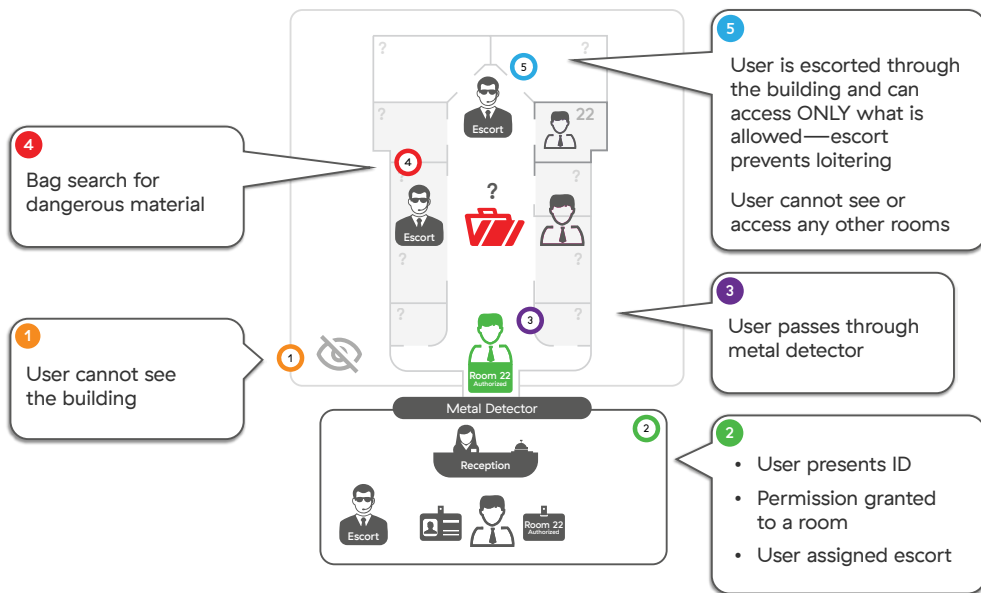


Figure O5: The ZTA model ensures the visitor can do no harm by limiting access and checking for malicious behavior.

In these examples, the first building is like the data center, where the applications are hosted. A room is like an application. The buildings represent public clouds like Azure and Amazon Web Services (AWS). ZTA, by design, acts as a switchboard that connects the user to a particular application within a particular data center or cloud (or a visitor to a meeting room, to extend the analogy).

Question 1 What is zero trust and why is it critical for secure digital transformation?

If a user needs to access a specific file share, that is all that user connects to, not the company network. The user can't move laterally to access or try to access SAP or other applications. This is how lateral movement is eliminated. It is a core principle of ZTA that traditional technology, like firewalls, are not designed to accommodate.

HOW TO PREVENT AN ATTACK SURFACE

Another tenet of zero trust is removing the attack surface, as every breach starts by discovering vulnerable users, devices, or applications.

To provide a parallel, using a traditional approach, Amy publishes her phone number in a phone book to make it easy for her friends to call her. Chris, a good friend, can find Amy's phone number, call her, and they can have a conversation. The problem is, a million other people can also find Amy's number and call her. Scam artists and spammers can take advantage of this public information. By exposing her phone number, good and bad people can call Amy.

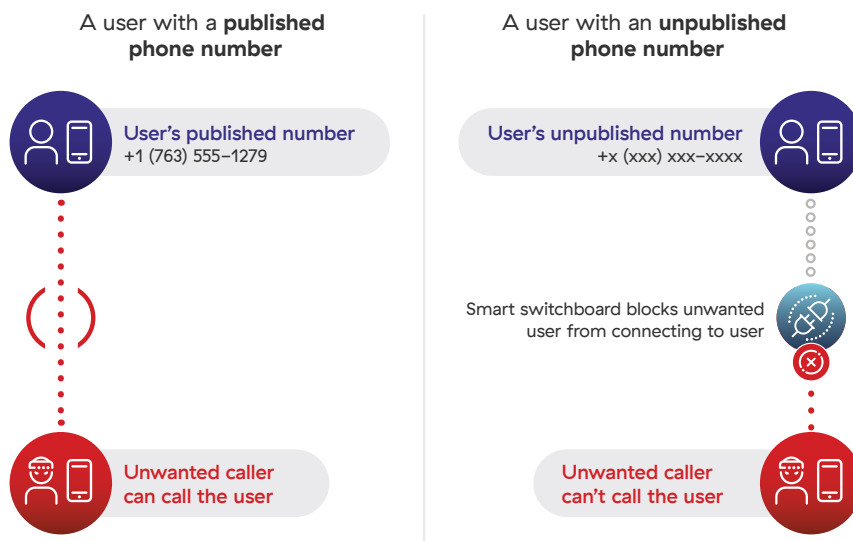


Figure O6: The ZTA model is similar to a switchboard that connects specific parties with each other, rather than publishing everyone's contact information in a public directory.

Question 1 What is zero trust and why is it critical for secure digital transformation?

This is similar to the way applications on the internet are published. Applications are published so employees can traverse the internet, discover them, use credentials to get in, and connect. But, this means bad guys can also find them. They may access apps by using stolen credentials or exploiting their vulnerabilities. They can definitely carry out distributed denial-of-service (DDoS) attacks on applications exposed to the internet. Hence, exposing apps has risks. Before zero trust architecture, we tried to mitigate this risk by creating a DMZ (demilitarized zone) with DDoS prevention solutions and firewalls—again, we built a moat around the castle. As attackers became more sophisticated, old solutions no longer worked. How does one fix this problem?

In Amy's case, she would not publish her phone number. She'd hire a smart switchboard service and provide a list of people who are allowed to connect with her. Chris calls the switchboard, and since he's authorized, the switchboard connects Chris to Amy without sharing her whereabouts or phone number. Anyone else who tries to call Amy is simply dropped because they're not authorized by her to connect.

**REMEMBER:
IF THEY CAN'T FIND
YOU, THEY CAN'T
ATTACK YOU.**

Applying these same principles is another pillar of ZTA—the user comes to a switchboard. They are validated and if allowed to access an application, they are connected. Otherwise, they simply get dropped. They don't even see where and what the applications are, and losing this visibility immediately minimizes the attack surface. Remember: if they can't find you, they can't attack you.

How does zero trust architecture work?

In the analogies described above to explain zero trust architecture, think of applications as the destination. These applications fall in two buckets:

Private Applications

Private applications are applications managed internally by the IT department. These are often hosted in a company's data centers, factories, or in IaaS/PaaS public clouds like Azure, AWS, GCP, etc.

Public Applications

Public applications are applications managed by others. These are SaaS applications hosted and secured by companies like Microsoft 365, Salesforce, ServiceNow, or Workday. This also includes destinations such as LinkedIn, BBC, Facebook, and Google Search accessed on the open internet.

Both of these application types are simply destinations. Users/devices, things (IoT/OT), and workloads need to access them. By default, they're all untrusted. The biggest difference between a zero trust architecture and traditional network security architecture is that with ZTA there's no routable network between the user and the application. How do they connect? They go through a zero trust policy engine, which acts as a switchboard for various entities (users, devices, and applications) to communicate with each other over any network.

When entity A tries to reach entity B, the connection is directed through the zero trust policy engine. The first thing that happens is that the connection is stopped.

Question 1 What is zero trust and why is it critical for secure digital transformation?



Figure 07: The zero trust architecture facilitates connections between users/devices, things, and workloads with application resources, using specified business policies.

The ZTA proxy architecture also allows an enterprise to inspect all traffic, identify and isolate threats, prevent data loss, and prevent the execution of malicious code. This proxy architecture is important because it functions as a proper ZTA ‘switchboard’ and terminates all traffic. This ensures that:

- All traffic, including encrypted traffic, can be scanned in a single pass for malware and threats
- The corporate network IP address range is no longer visible to hackers

ZTA also verifies identity using an integrated identity and access management (IAM) system. But, since an identity can be stolen, the ZTA also considers the properties of the device in use. Is it managed?

Question 1 What is zero trust and why is it critical for secure digital transformation?

Is it unmanaged? Is it BYOD? Where is its geographic location? What is the user trying to do? This context is very important. The proper policy is determined and applied based on all of these factors.

If a connection looks valid, the ZTA takes steps to measure and control risk, prevent compromise, and stop data loss. To do so, the ZTA inspects all inbound and outbound traffic for malware and outbound sensitive data.

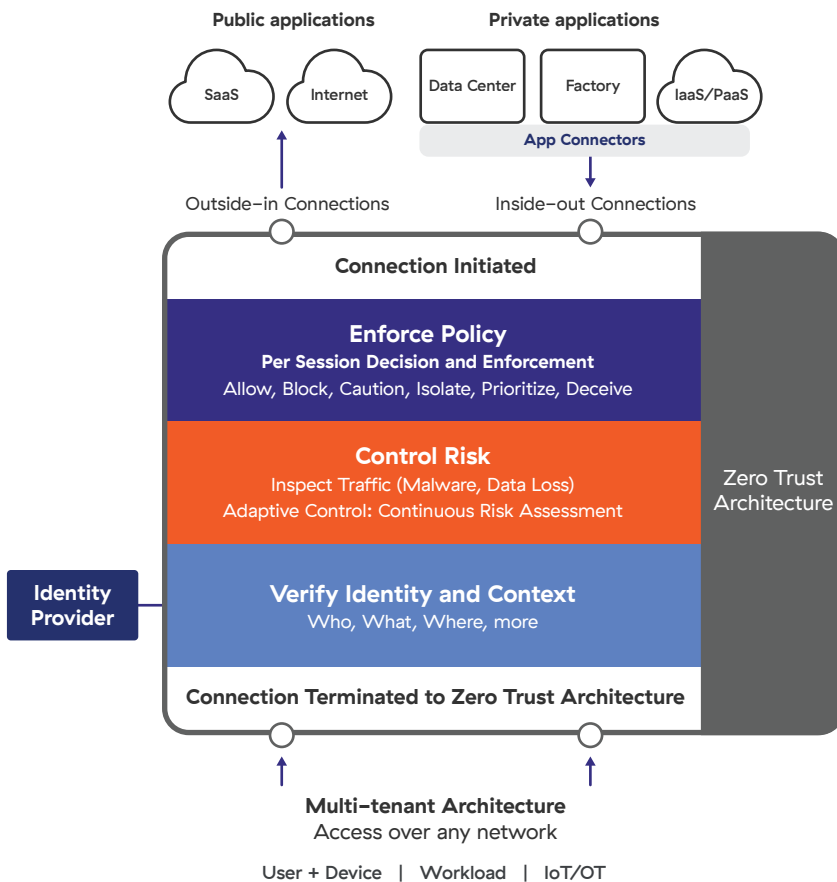


Figure O8: Zero trust architecture provides multiple layers of protection before initiating the connection.

Question 1 What is zero trust and why is it critical for secure digital transformation?

Beyond this, the ZTA leverages adaptive control, continuously assessing changes in the user's risk. If it sees anomalous behavior of traffic or the user, it can terminate any suspicious connections.

Next, the ZTA enforces policy, which is done per user-initiated session. The enforced policy could be Allow, Block, Caution, Isolate, and Stream Pixels, Prioritize, or Deceive. The ZTA grants users access only to certain applications, and prevents lateral movement.

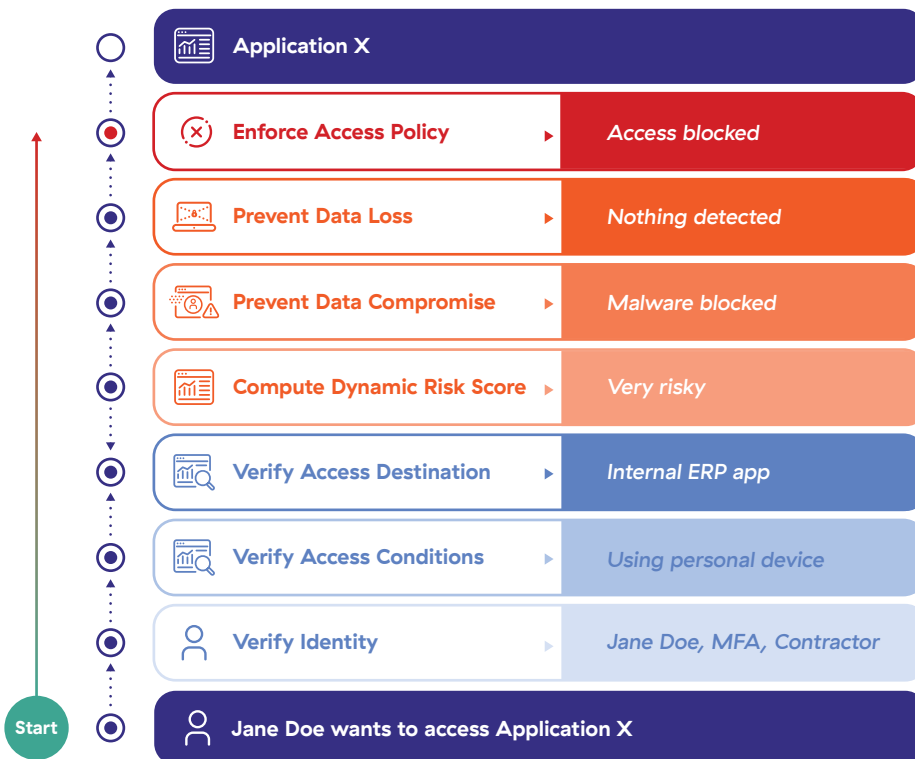


Figure O9: A sample user's journey through the steps of zero trust when connecting to an application. In this case, the user is prevented from connecting to the critical internal application, based on her identity, context, and risk.

Question 1 What is zero trust and why is it critical for secure digital transformation?

Finally, if all checks are in good standing, the ZTA takes the final step to connect the user to the authorized application. For external applications, this is a simple connection. For internal applications, the ZTA establishes an inside-out connection using a lightweight software component on the server side. This way, internal applications only resolve to the ZTA cloud and not to the internet; that's how the ZTA hides the attack surface.

How does this work in practice?

Consider the figure above where Jane Doe is requesting to access Application X. ZTA first verifies identity to learn that Jane is a contractor. Next, it looks into how Jane is connecting and sees that she is on a personal device.

The application she wishes to access is a sensitive, internal ERP application. These conditions deem her request to be “very risky,” and while there is no record of data loss, there is a history of malware downloads that had to be blocked. Based on these factors, the ZTA decides to enforce an access policy by blocking access.

Now, contrast this method with the traditional architecture of firewalls and VPNs. This is important because many legacy architectures falsely claim to be zero trust architecture. Fundamentally, a firewall is not a proxy architecture. It is categorized solely as pass-through architecture because it can only perform limited inspection and it connects users to the network. By doing this, it enables lateral threat movement. A firewall is facing the internet and basically announces, “I am here, connect with (and attack) me.”

THIS IS IMPORTANT BECAUSE MANY LEGACY ARCHITECTURES FALSELY CLAIM TO BE ZERO TRUST ARCHITECTURE. FUNDAMENTALLY, A FIREWALL IS NOT A PROXY ARCHITECTURE.

Question 1 What is zero trust and why is it critical for secure digital transformation?

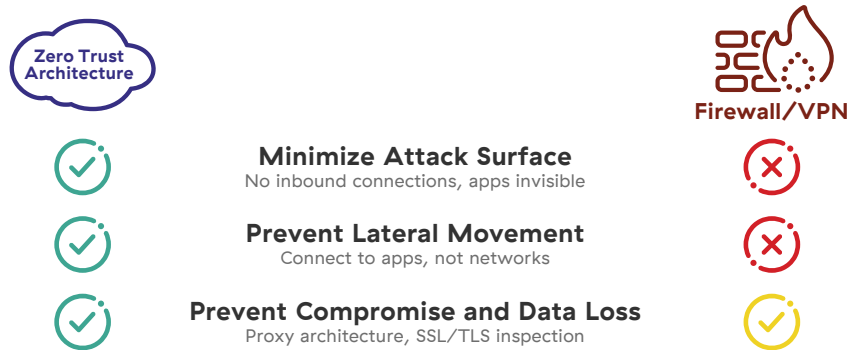


Figure 10: Traditional firewall/VPN do not provide zero trust security.

Another comparison comes to mind. An electric and a gas-powered car look very similar, but they aren't. On one hand, the electric car has a simple electric motor. In contrast, a traditional car has a very complex engine. Complexity is the enemy of security. Complexity is the enemy of reliability. The clean and simple design of the EV's engine is like ZTA.



Figure 11: Under the hood, these two cars have completely different architectures, similar to how firewall and VPN vendors claim to provide zero trust security. Under the hood, a cloud-native zero trust solution is very different.

“ The industry has invested disproportionately on the probability side of risk reduction—now we have an opportunity to reduce both the probability and the blast radius of cybersecurity incidents with zero trust architecture.”

Saša Zdjelar
SVP, Security Assurance, Salesforce

Is this just a passing fad or is it here to stay?

Zero trust has already made an enormous impact on many organizations. It proved especially valuable as the pandemic sent workers home, expanded the network, taxed VPN resources, and opened the door to new attacks. Organizations that transitioned to ZTA were able to send workers home seamlessly while avoiding the common bottlenecks and security concerns that would normally accompany such a massive workforce shift. That being said, many organizations are still in various stages of their transformation journey.

[Zscaler survey results](#) show that today, more than 90% of organizations migrating to the cloud have a zero trust security strategy in place, or plan to in the next 12 months. Respondents indicated that zero trust network access (ZTNA) is their #1 priority, based on the need to provide a secure hybrid work environment. They cite their employees' inconsistent access experiences for on-premises and cloud-based applications and data as a top reason to implement a zero trust-based hybrid work infrastructure. In addition, 68% of IT leaders also admit that cloud migration requires a rethinking of traditional security models.

Question 1 What is zero trust and why is it critical for secure digital transformation?

In the survey, the reasons to move to zero trust security were ranked by respondents in this order: (1) improve detection of advanced threats, (2) improve detection of web application attacks, and (3) broaden security to protect sensitive data.



Figure 12: Zscaler survey results on zero trust sentiment.

Gartner first published the Magic Quadrant and Critical Capabilities research on the Security Service Edge in 2022. They made the following prediction about ZTA and SSE, highlighting movement toward a consolidated SSE approach over point solutions:

“By 2025, 80% of organizations seeking to procure SSE-related security services will purchase a consolidated SSE solution, rather than stand-alone cloud access security broker, secure web gateway and ZTNA offerings, up from 15% in 2021.”¹

The data shows traditional network and security architectures are not equipped to provide adequate security and connectivity for the rapidly evolving hybrid workplace. Globally, IT and security leaders have or are actively planning to replace their legacy architectures with a zero trust solution based on an SSE platform.

¹ Gartner, “Magic Quadrant for Security Service Edge,” John Watts, Craig Lawson, Charlie Winckless, Aaron McQuaid, February 15, 2022

What is the ecosystem of technology partners required for secure digital transformation?

While discussing how ZTA reduces point products, it does not eliminate all other solutions as it is still part of an ecosystem. Zero trust vendors, in order to ensure fast, easy, and secure deployment and integration, provide integrations with ecosystem partners in the following areas:

Cloud Providers / SaaS Vendors — applications that the ZTA provides secure connectivity to, or protection of, when considering workload connectivity

Identity Management — provides user identity information from which the ZTA makes policy decisions

Endpoint Protection and Management — protection for endpoint devices that provides context for the ZTA risk calculation and access decisions

Branch Router / SD-WAN — provide branch network connectivity that works in conjunction with ZTA to create a software-defined network underlay that sends traffic to the zero trust cloud

Operations — ingests logs created by the zero trust solution for analysis and threat hunting

These integrations allow for orchestration between the ZTA and partner vendors to reduce complexity, total cost of ownership (TCO), and improve security posture.

Question 1 What is zero trust and why is it critical for secure digital transformation?

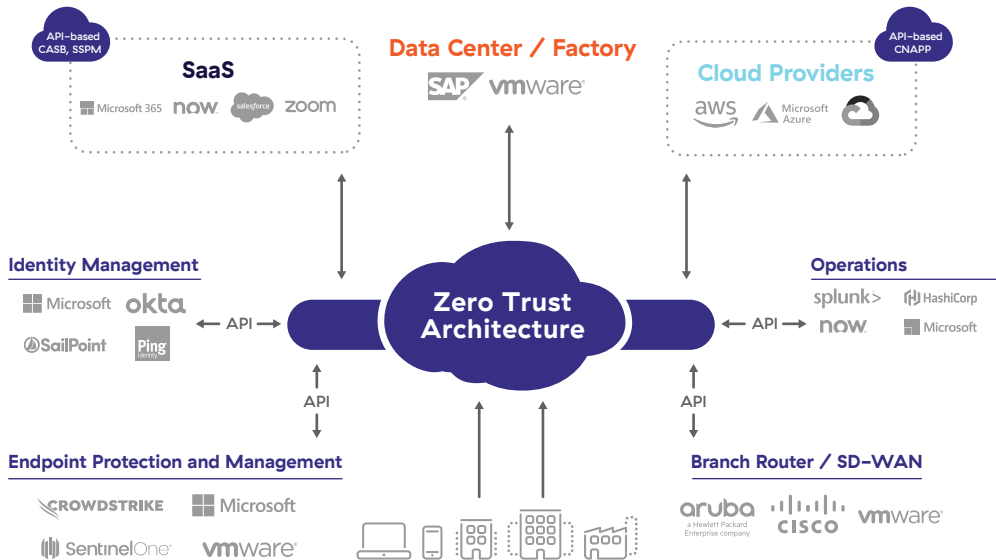


Figure 13: ZTA integrates with other ecosystem providers to offer comprehensive protection.

What is Zscaler's role in zero trust?

Given an understanding of ZTA, what does Zscaler do? Zscaler offers its own ZTA-based solution called the Zscaler Zero Trust Exchange (ZTE). It securely connects authorized users, devices, and workloads with each other, users to applications, workloads to workloads, and even IoT devices to a data lake, by using specified business policies.

What's a business policy? Unlike firewalls and network security, which work on IP addresses and access control lists, Zscaler

Question 1 What is zero trust and why is it critical for secure digital transformation?

connects users to applications. That's what makes it simple. Through this process, Zscaler eliminates many point products and reduces operational overhead.

THE ZERO TRUST EXCHANGE HAS FOUR BROAD CAPABILITIES:

01 Cyber threat protection

Cyber threat protection, holistically making sure Zscaler is protecting users, workloads, and devices from being compromised.

02 Data protection

Data protection, doing both inline and out-of-band protection and API-based securing of SaaS data, as well as securing public cloud data with sophisticated data classification, techniques, and policy engines.

03 Zero trust connectivity

Zero trust connectivity, connecting users, branches, and workloads with internal resources connected through the Zero Trust Exchange rather than a routable network. This accomplishes segmentation with zero trust without having to do network-based segmentation.

04 Optimized user experience

Optimized user experience in today's world with users working from anywhere and everywhere. A positive user experience is mandatory. Zscaler is sitting in a very meaningful place to help identify and resolve performance issues through an integrated Digital Experience Management solution.

Question 1 What is zero trust and why is it critical for secure digital transformation?

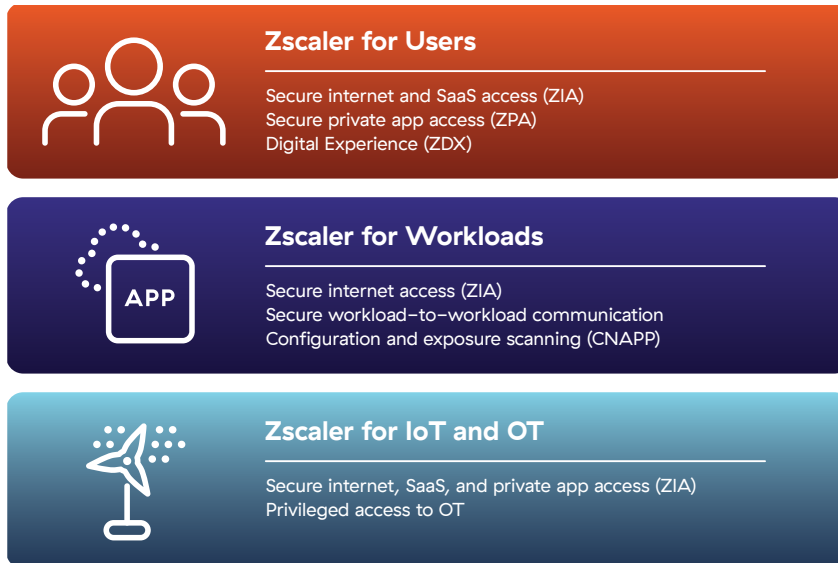


Figure 14: Zscaler core product lines.

These capabilities are offered in three platform families:

Zscaler for Users provides everything needed for a user to access any application from anywhere with a great experience. Zscaler for Users includes Zscaler Internet Access (ZIA) to allow secure access to the internet and SaaS. It also includes Zscaler Private Access (ZPA), which allows secure access to internal applications. Zscaler Digital Experience (ZDX) provides digital experience monitoring. The three modules are the primary technologies for fully protecting users.

Can Zscaler do the same thing with workloads? Workloads are very much like users since they talk to the internet and other workloads.

Zscaler for Workloads takes the same core technology engine that was built for zero trust, the Zero Trust Exchange, and applies it to workloads. Workloads talk to the internet through ZIA, not through virtual firewalls, and not through squid proxies. They communicate over a zero trust switchboard without having to use a routable

Question 1 What is zero trust and why is it critical for secure digital transformation?

network. Another important piece in this process is Zscaler Posture Control, which Gartner calls CNAPP (Cloud Native Application Protection Platform), to ensure workloads are properly configured and not overly exposed.

Zscaler applies this core technology to IoT/OT as well, with **Zscaler for IoT/OT**. These IoT/OT devices have the same lateral threat movement risk. OT systems are expensive today and are mostly accessed using remote access. VPN does not eliminate lateral movement, on-prem or in the cloud. It gives attackers the potential to do extensive harm to the environment. Zscaler brings zero trust architecture to IoT/OT.

These Zscaler products have deep integration with ecosystem partners like Microsoft, where a number of touch points (like security integrations, application integrations, and optimized connectivity) simplify the operation of ZTA.

Zscaler by the Numbers

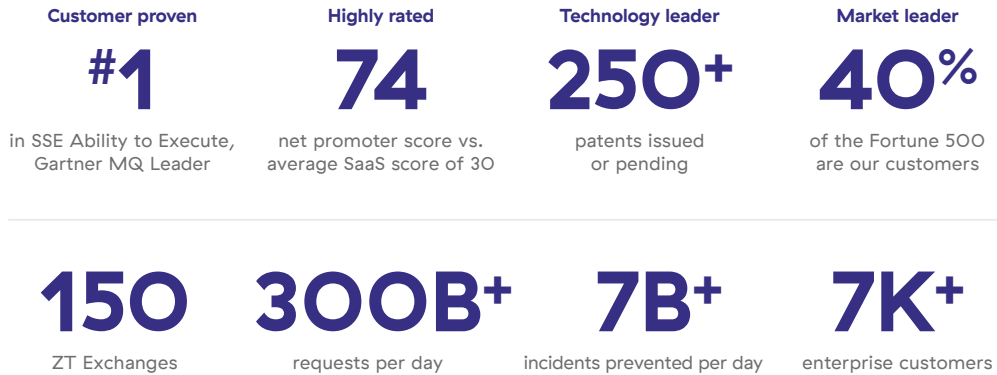


Figure 15: Zscaler is a market leader in secure digital transformation.

Question 1 What is zero trust and why is it critical for secure digital transformation?

“ I’m thrilled to see some of the largest enterprises, including Sandvik, Siemens, and GE, use Zscaler and Microsoft to deliver fast and direct access to Office 365, as well as applications running on Azure.”

Satya Nadella
CEO, Microsoft

Zscaler products have deep integration with ecosystem partners like Microsoft, where a number of touch points (like security integrations, application integrations, and optimized connectivity) simplify the operation of ZTA.

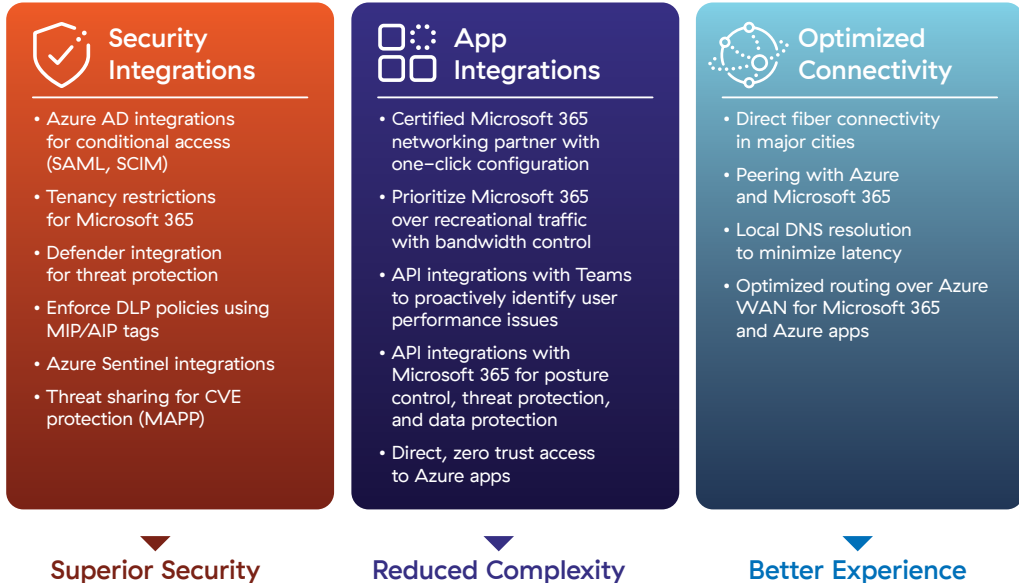


Figure 16: Zscaler provides various integration points with Microsoft to improve operations.

Is zero trust architecture a product and how does it relate to the Security Service Edge (SSE)?

Holistically, zero trust is often described as a strategy or a framework that is not a product, per se, sold by specific vendors. While this is true, in that zero trust is a way of thinking that permeates across a number of areas, not just new architecture or technology, there are practical zero trust implementations from vendors, like Zscaler, that have built their solutions with the framework at their core. The preceding section describes just that. Once deployed, zero trust technology forms the basis of providing secure access for users, things, and workloads to public or private destinations.

When considering solutions based on zero trust architecture, it is important to understand how this market is described and categorized. The most common taxonomy is called Security Service Edge or SSE (defined by Gartner), which is an umbrella description for solutions offering zero trust architecture, among other functions.

Gartner's SSE provides a framework that combines the main elements of network security—including the Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA), a Cloud Access Security Broker (CASB), and firewall as a service (FWaaS), among other components—as provided from the cloud at a location near the end user. ZTNA, in this context, relates merely to user-to-private application access. The main point is that the security stack, once hosted on-premises, moves to the cloud or the “security edge.” This affords all the benefits of cloud-hosted solutions, from the perspective of complexity, scale, maintenance, architecture, etc.

Question 1 What is zero trust and why is it critical for secure digital transformation?

How do the concepts of zero trust architecture, as described here, relate to the broader concepts of SSE? They are closely intertwined. Think of SSE as a practical implementation of zero trust architecture, along with other ecosystem components like identity, endpoint detection & response (EDR), or security information and event management (SIEM). In the remainder of this book, we will be referring both to zero trust architecture and SSE as practical methodologies for the implementation of zero trust.

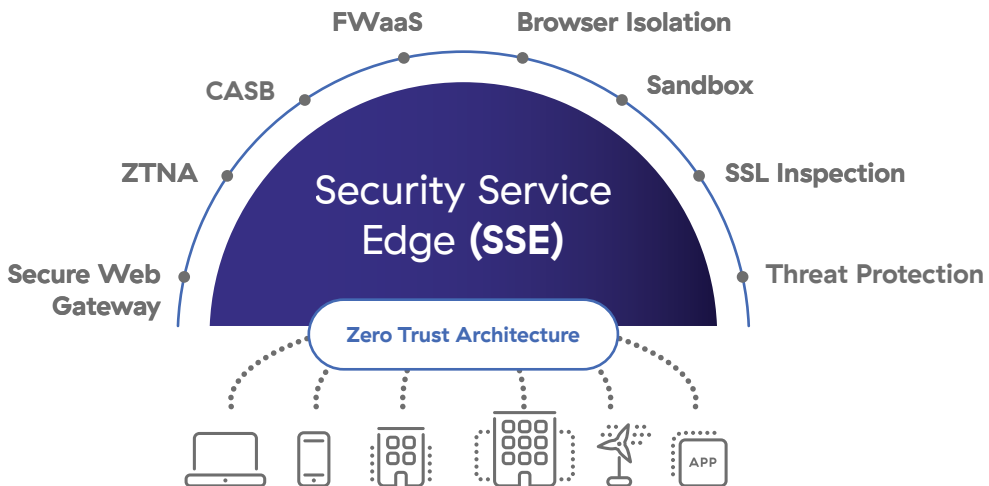


Figure 17: The components of the Security Service Edge, the basis for zero trust architecture.

SSE is part of a broader Gartner framework called SASE (Secure Access Service Edge) that encompasses both SSE and WAN Edge infrastructure, including SD-WAN. SASE is commonly delivered as a two vendor solution, leveraging robust integrations between SSE and SD-WAN architectures.

QUESTION TWO

What are the main use cases for zero trust?

Question 2 What are the main use cases for zero trust?

The adoption of zero trust is not driven by new, cool technology—but by business use cases. For most businesses, the three biggest drivers for embracing zero trust architecture are: (1) improving business productivity and agility, (2) reducing cyber risk (including potential data loss), and (3) minimizing the cost and complexity of various point products and the legacy network.

Zero trust use cases can be broken down into three distinct categories:



Figure 18: Zero trust architecture use cases include securing work from anywhere, transforming the WAN, and securing cloud migration.

Secure Work from Anywhere

The secure work from anywhere (WFA) capability provides secure and fast access to applications from any location, on any device (managed or BYOD). This is necessary to protect employees, third parties/contractors, customers, and suppliers who are using various devices from countless locations.

Question 2 What are the main use cases for zero trust?

There are several key use cases regarding secure work from anywhere:

- Secure internet access, protecting against both cyberthreat and data loss
- Zero trust application access, replacing traditional VPNs
- Secure access for BYOD as a virtual desktop replacement
- Merger and acquisition (M&A) integration
- Zero trust for IoT/OT

SECURE INTERNET AND SaaS ACCESS

Zero trust architecture protects access to the internet and SaaS applications in several ways. Initiator traffic (users, things, or workloads) is not passed directly to a destination service. First, enterprise controls are applied. These controls are applied by nodes nearest to wherever the initiator is located, thus allowing for optimized consumption of the service. Most importantly, these controls protect the initiator and the enterprise, wherever they may be.

Every single access request is checked for its identity and the context of the destination. Once connected, the content and behavior of the session is assessed through AI/ML (using decryption for encrypted traffic) to discover and block malware and prevent data loss.

The goal of this process is to ensure that the enterprise is protected against bad things “coming in” and good things “going out,” thus delivering security and granular protection for each service. Granular protection may include serving a pixelated version of the application using browser isolation. This granular policy follows the initiator, so that the same protection is provided uniformly.

Zero trust architecture not only provides superior cyber protection, but also allows the replacement of various hardware appliances, including secure web gateways, proxies, and certain firewalls.

Question 2 What are the main use cases for zero trust?

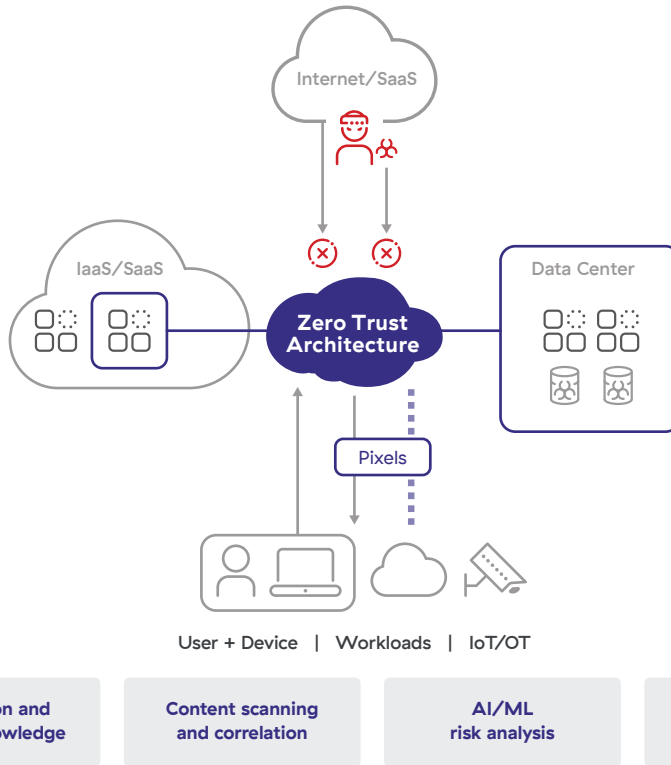


Figure 19: ZTA provides secure access to internal and external resources through a variety of means, including browser isolation/pixel-streaming.

The same controls used to protect against cyber threats are then used to protect enterprise data from being lost. The ZTA performs both inline and out-of-band data protection, allowing the inspection and control of data in motion and files at rest. Its ability to read encrypted traffic allows it to find and block sensitive data in transit, and perform other advanced DLP functions.

Inline prevention controls leverage isolation techniques to block sensitive data being downloaded to BYOD or managed devices by streaming the data as pixels. Endpoint data loss prevention goes further by protecting the data on devices from being downloaded to

Question 2 What are the main use cases for zero trust?

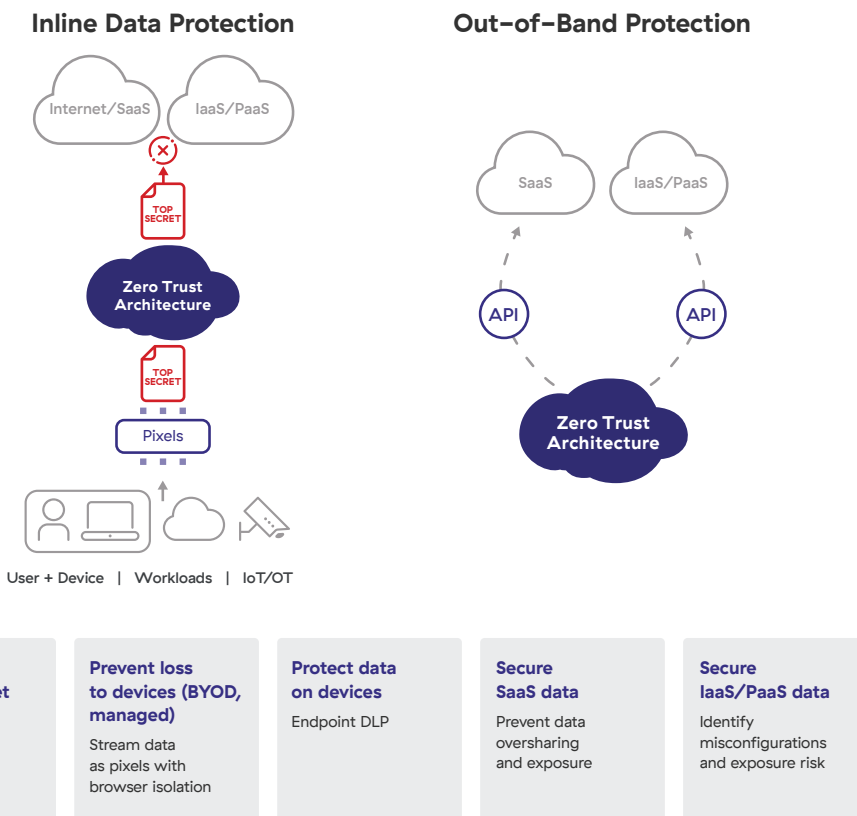


Figure 20: ZTA provides inline and out-of-band security to protect data, apps, users, devices, and workloads.

a USB drive, for example. Out-of-band data protection technology protects data living in the cloud by preventing oversharing and exposure as well as identifying misconfiguration with popular cloud platforms where sensitive data may reside.

Both of these techniques utilize advanced ways to classify data, including AI/ML, optical character recognition, and integration with Microsoft information protection standards.

SECURE PRIVATE APPLICATION ACCESS

Zero trust architecture is deployed for secure access to private apps hosted in the IaaS/PaaS cloud or in a data center.

Question 2 What are the main use cases for zero trust?

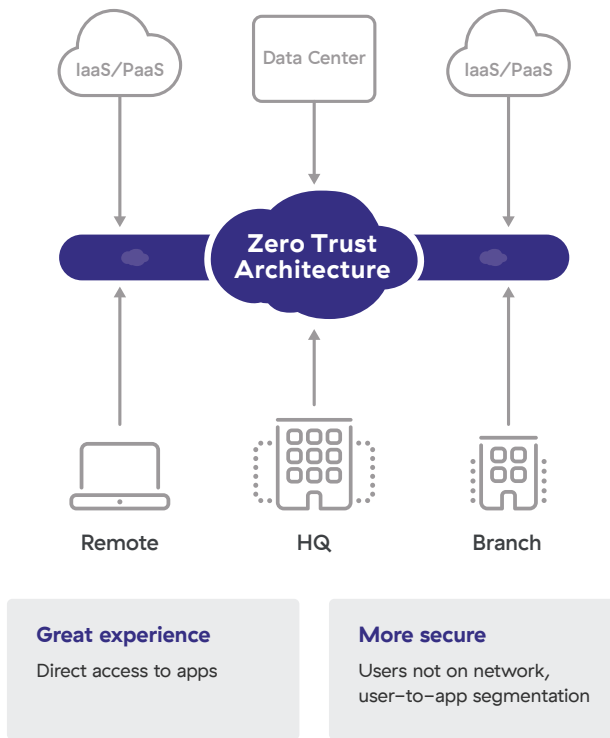


Figure 21: Zero trust application access to private applications, whether hosted in a data center or cloud, minimizes the attack surface by preventing inbound connections.

By allowing authorized initiators app-level access to destinations, it fundamentally removes the need for legacy network-based access, like VPNs.

By never exposing services to unauthorized users, IT leaders eliminate much of an organization’s attack surface (exposed destinations and services). Removing the legacy routable network greatly simplifies the technology estate and allows IT leaders to deliver services to any initiators that require access to internal resources. This can be extended to on-premises users with what is commonly known as Universal ZTNA.

This granular element of ZTA delivers the app-level segmentation that has historically been difficult to achieve at the network level,

Question 2 What are the main use cases for zero trust?

allowing the creation of three types of segmentations based on business policy:

- User-to-application segmentation
- Workload segmentation in hybrid and multicloud environments
- Identity-based microsegmentation for apps/processes

SECURE BYOD ACCESS AND VDI REPLACEMENT

Every IT leader battles with the need to allow external third parties access to their internal resources. This coupled with the rise of bring your own device (BYOD), even among employees, has left few options for uniformly secure access paths from initiators to destinations.

Whereas historically virtual desktop infrastructure (VDI) instances were the only option to secure these users, ZTA threat and data protection can be extended to BYOD using cloud browser isolation. This renders content in an air-gapped browser, and streams pixels to the user rather than loading the full HTML. For example, partners could view the contents of an inventory app but not download, copy, or print anything.

For internal employees accessing sensitive applications, a company's policy can use browser isolation for granting view-only access to untrusted devices. Virtual desktops hosted in on-prem server farms were often the only way to achieve this secure access, but browser isolation (integrated as part of ZTA hosted in the cloud) offers a powerful alternative.

M&A INTEGRATION

Many enterprise leaders deal with the demands of M&A and divestitures. Managing the complexities of the users, processes, resources, and infrastructure involved has historically been costly and challenging.

THIS GRANULAR ELEMENT OF ZTA DELIVERS THE APP-LEVEL SEGMENTATION THAT HAS HISTORICALLY BEEN DIFFICULT TO ACHIEVE AT THE NETWORK LEVEL, ALLOWING THE CREATION OF THREE TYPES OF SEGMENTATIONS BASED ON BUSINESS POLICY.

Question 2 What are the main use cases for zero trust?

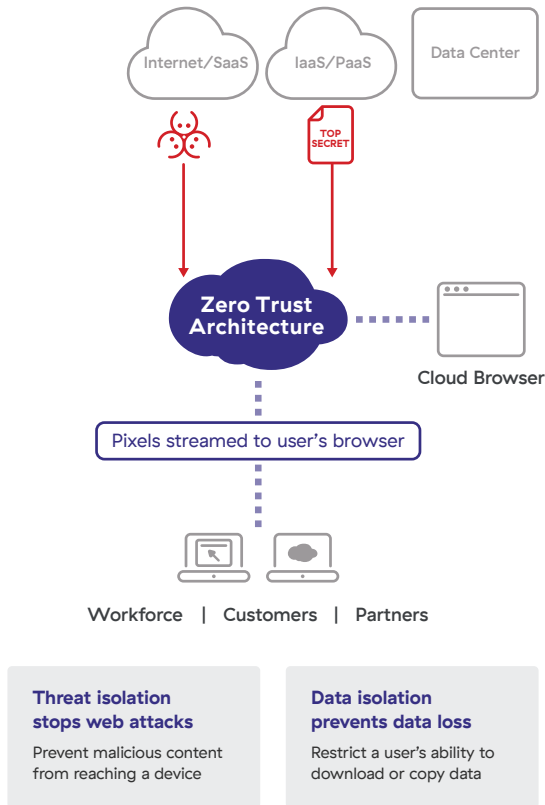


Figure 22: ZTA secures BYOD tech and eliminates VDI by using cloud browser isolation.

ZTA inherently delivers seamless integration between two entities by solving the underlying challenges of segmentation.

Zero trust architecture doesn't require two heterogeneous networks to be merged. Company A and Company B can provide standardized internet/SaaS security and secure access to apps in the data center or the public cloud by determining which users can access which destinations. Users at both companies connect to the zero trust architecture, which coordinates connections, manages access policies, and provides consistent protection.

Zero trust eliminates the need to integrate networks of two companies or the use of remote access VPN. Each entity simply needs access to the internet. As a result, the duration of the costly

Question 2 What are the main use cases for zero trust?

Transition Service Agreements (TSAs) can be vastly reduced. Meanwhile, a precise audit trail of the cross-company connections can be maintained, which provide senior executives and board members extra comfort.

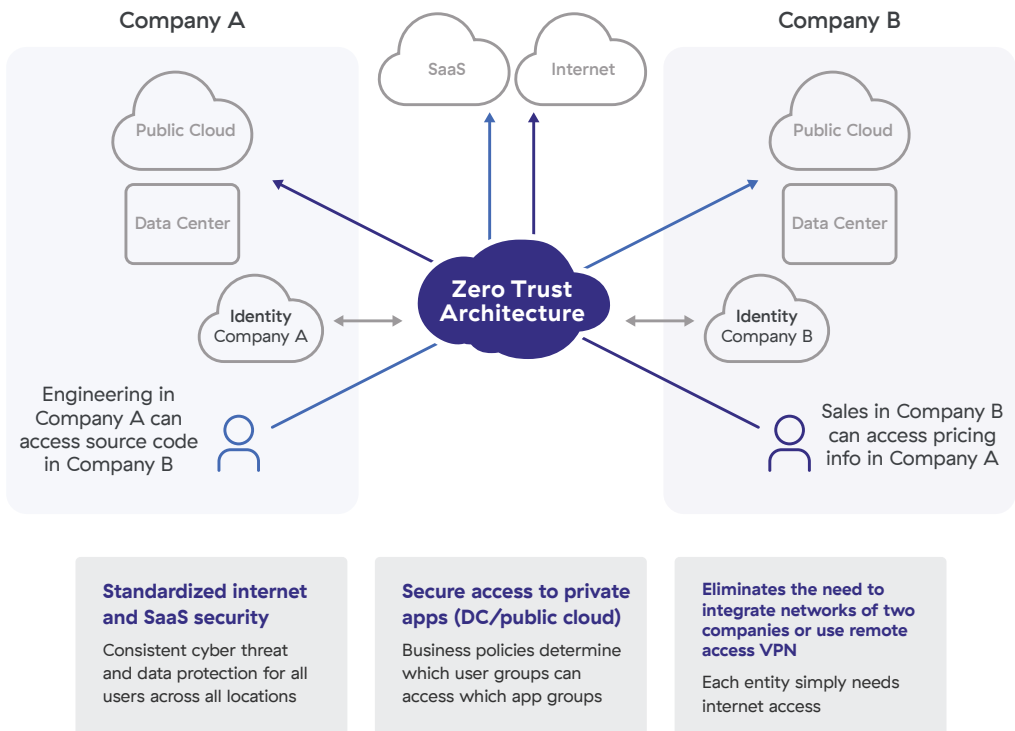


Figure 23: Zero trust enables seamless M&A integration by removing the network and introducing app-based and connection-based segmentation.

ZERO TRUST FOR IoT/OT

Secure remote access for IoT/OT systems is a service that takes a user- and application-centric approach to security. Whether a user is an employee, contractor, or third-party partner, the ZTA ensures that only authorized users have access to specific IoT/OT systems or applications. This granular segmentation eliminates the visibility of the network and prevents lateral movement.

Question 2 What are the main use cases for zero trust?

Rather than relying on physical or virtual appliances, ZTA uses lightweight, infrastructure-agnostic software like Docker containers or virtual machines, paired with browser access capabilities, to seamlessly connect all types of users to IoT/OT systems and applications, via inside-out connections.

In addition, third-party partners and users gain secure access to IoT/OT systems without needing a client agent. The zero trust cloud architecture provides policy-enforced, third-party connectivity to IoT/OT systems from any device, in any location, at any time.

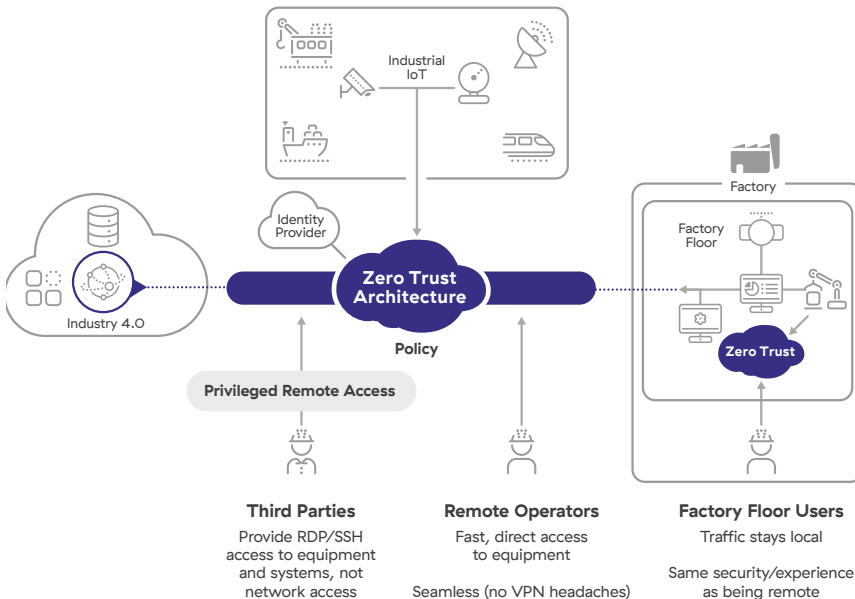


Figure 24: Zero trust for IoT/OT systems.

WAN Transformation

Wide area network (WAN) transformation is often led by the head of infrastructure and networking. WAN transformation allows organizations to convert unsecured, routable, hub-and-spoke networks to true zero trust connectivity, while also improving the user experience. Zero trust architecture (hosted as part of the Security Service Edge in POPs close to population centers) allows direct access to cloud applications via the internet, without the need for MPLS circuits back to the data center. This replaces much of the hardware-based security stack and eliminates the “hairpinning” of traffic that adds unnecessary latency.

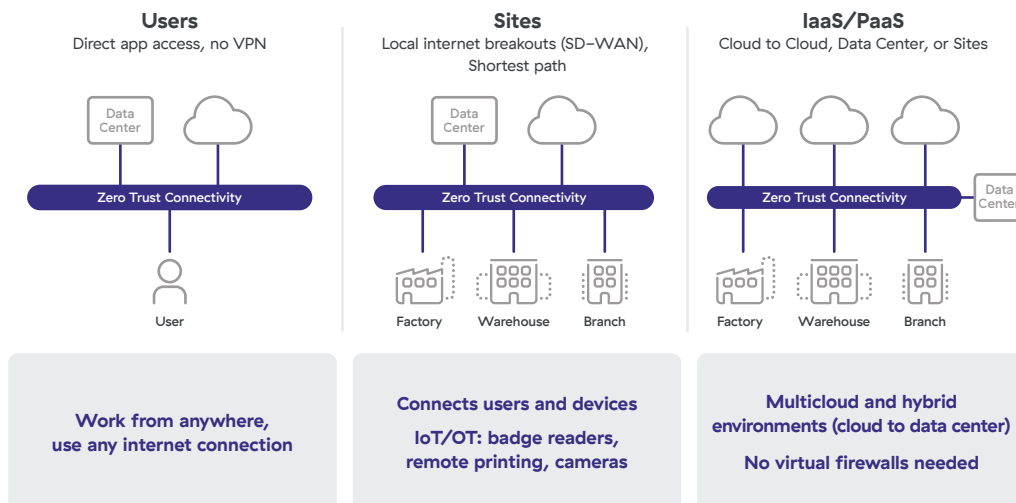


Figure 25: Zero trust enforcement nodes act as a switchboard, creating connections based on business policy. Apps are destinations, not network resources, and users and applications are never on the same network.

Question 2 What are the main use cases for zero trust?

In addition to direct application access and local internet breakouts, WAN transformation also includes zero trust software-defined wide area networks (SD-WAN) and digital experience monitoring (DEM).

ZERO TRUST SD-WAN

SD-WAN has emerged as a technology that aids in WAN transformation by bringing software-defined edge networking and path selection that reduces the reliance on extremely costly MPLS networks.

While SD-WAN and zero trust can coexist, SD-WAN is not in itself zero trust as it still relies on an underlying WAN. By definition, ZTA should be network-agnostic and not exclusively tied with any network underlay solution. In fact, many of the benefits of SD-WAN are from its “software-defined” capabilities, not the WAN, which inherently extends the corporate network and allows for lateral movement. Decision makers should carefully evaluate extending the corporate network to the branch and consider alternate approaches.

To secure connectivity for large branches or campuses, an SD-WAN solution can forward internet/SaaS traffic through the zero trust service edge to establish secure local internet breakouts. This can be accomplished through API integration, so that SD-WAN vendors automatically create tunnels to the zero trust service edge. If SD-WAN is required for path selection or centralized management, it should only be considered for large branches, campuses, or factories. In some cases, for traditional applications, some private application traffic may still need to be sent via a site-to-site VPN.

ZERO TRUST SD-WAN PROVIDES BRANCHES AND DATA CENTERS FAST AND RELIABLE ACCESS TO THE INTERNET AND PRIVATE APPLICATIONS WITH A DIRECT-TO-CLOUD ARCHITECTURE, WHICH PROVIDES HIGH SECURITY AND OPERATIONAL SIMPLICITY.

Question 2 What are the main use cases for zero trust?

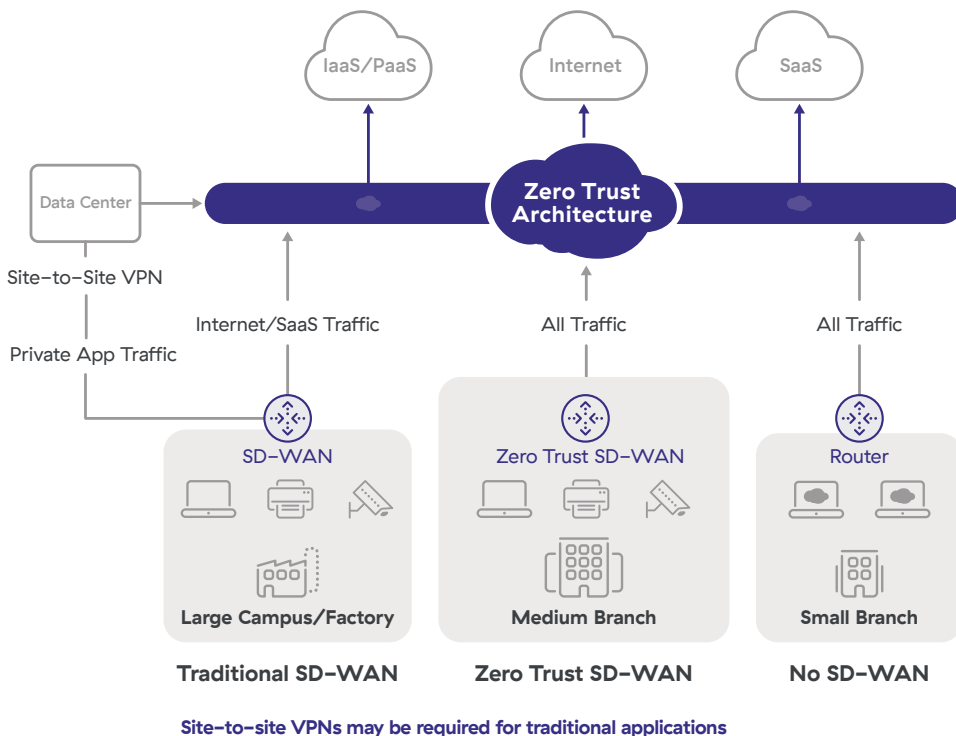


Figure 26: Zero trust SD-WAN provides secure access for users and services in branches.

There are alternatives that better conform to zero trust standards for small and medium-sized branches. For example, zero trust SD-WAN replaces traditional WAN connectivity solutions in-branch by applying zero trust principles to user, server, and IoT/OT device connectivity. Zero trust SD-WAN provides branches and data centers fast and reliable access to the internet and private applications with a direct-to-cloud architecture, offering strong security and operational simplicity. It eliminates the network attack surface by establishing direct branch-to-internet and branch-to-private app connections using a full proxy architecture.

For small branches where there are fewer users, going fully zero trust with no SD-WAN and no routable network is the preferred approach. This basically treats everyone in that small branch as a remote user. An agent installed on the user's endpoint forwards

Question 2 What are the main use cases for zero trust?

traffic to the zero trust service edge for secure connectivity to public and private applications.

DIGITAL EXPERIENCE MONITORING

Visibility is a major concern of many CXOs when transforming to ZTA, as the users have direct internet access from their location and are accessing SaaS applications. Their traffic no longer 'trombones' via a corporate data center, where monitoring it was simpler. A ZTA needs to integrate digital experience monitoring (DEM) capabilities to provide critical tools to IT operations and ensure reliability, performance, and a smooth end-user experience. In other words, DEM is necessary for IT teams to truly deliver on the “securely work from anywhere” promise.

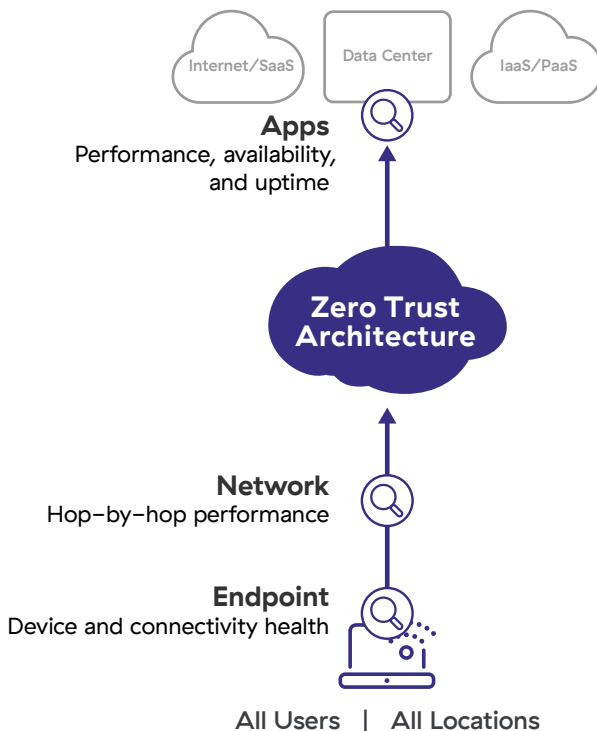
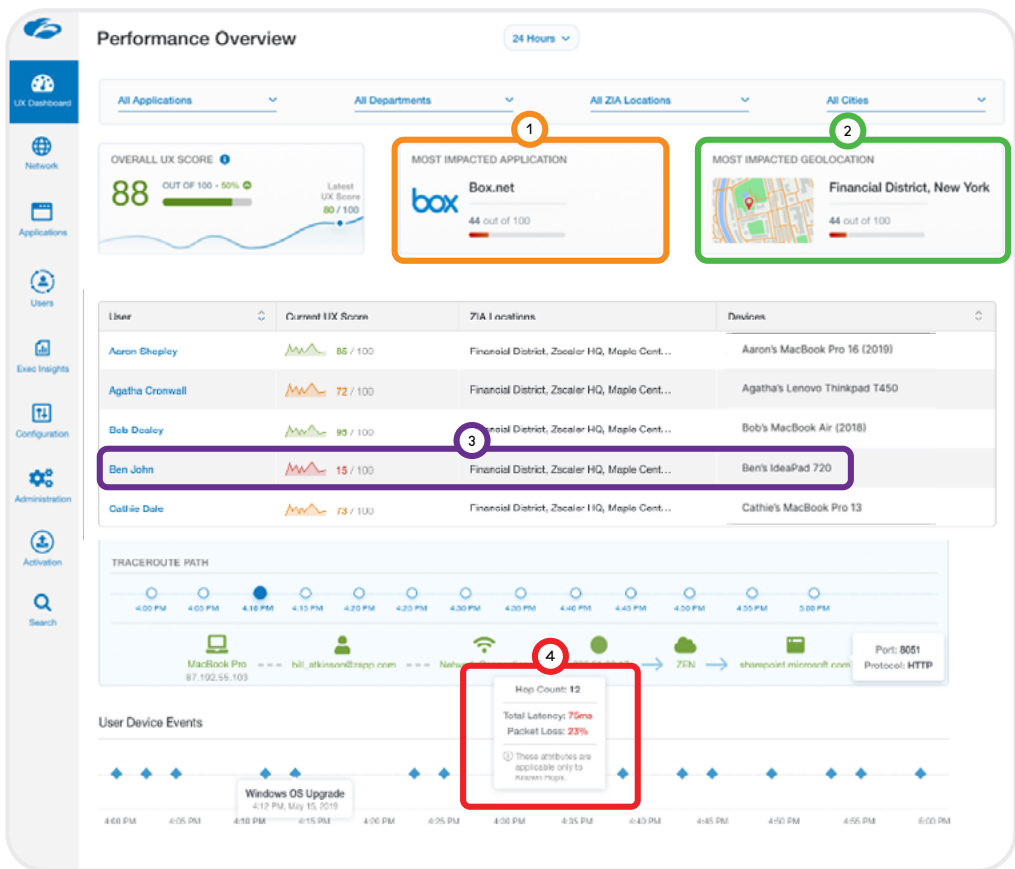


Figure 27: Visibility from the endpoint to the application is needed to troubleshoot and resolve performance issues.

Question 2 What are the main use cases for zero trust?

DEM uses telemetry data, collected from the zero trust architecture, to monitor and diagnose end-user experience and application performance issues. DEM uses machine learning (ML) to identify performance anomalies and send actionable alerts based on application, endpoint, and network analytics. This includes hop-by-hop network analysis that identifies network issues between the user endpoint and their WiFi, ISP, backbone, and the zero trust service edge; resource issues on an endpoint; or problems with the application provider.



- 1 Box app is slow
- 2 Financial District office issues
- 3 Ben has performance issues in NYC office
- 4 Packet loss between WiFi and router

Figure 28: Sample workflow of using ZTA's DEM telemetry to identify and diagnose a performance issue.

Secure Cloud Migration

As applications are migrated to the cloud or built as cloud-native, there is protection for how their workloads communicate with other workloads and the internet, and how they are entitled and configured. Providing strong posture control, secure workload configuration, and safe workload communications is an important aspect of a holistic ZTA.

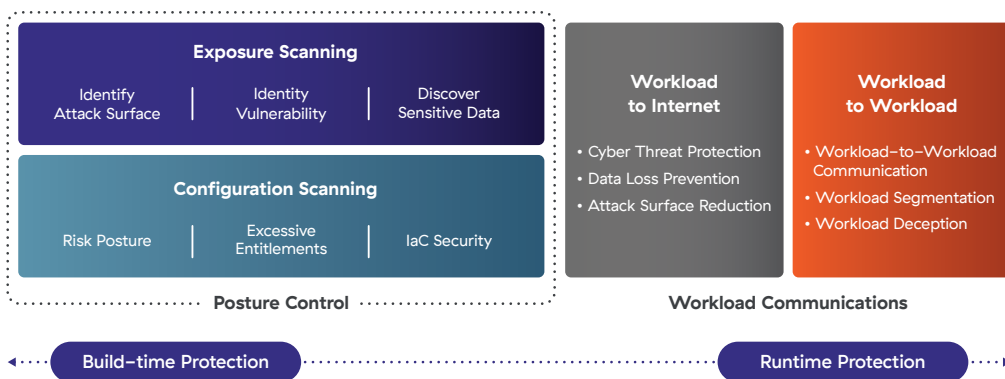


Figure 29: Secure cloud migration includes both posture control and securing workload communications.

This turns out to be particularly relevant, as there is a widespread feeling that once applications are migrated to the cloud, they are safe because the cloud providers are now taking care of their protection.

POSTURE CONTROL

Posture control for cloud applications falls into two categories: exposure scanning and configuration scanning. Exposure scanning, leveraged through API integration with common IaaS and SaaS

Question 2 What are the main use cases for zero trust?

vendors, can identify an attack surface, find identity vulnerabilities, and discover sensitive data.

Configuration scanning uses similar API integration to identify the risk posture of a cloud application, excessive entitlements, and the security of infrastructure-as-code scripts. This capability is commonly called CNAPP (Cloud Native Application Protection Platform).

CNAPP is agentless and uses ML to correlate hidden risks caused by misconfigurations, threats, and vulnerabilities across the cloud stack. Security, development, and DevOps teams should prioritize and remediate risks in cloud-native and VM-based apps as early as possible in the software development life cycle (SDLC), both at build-time and runtime. CNAPP gives professionals the visibility they need to “shift left” security practices during the SDLC, and fix small problems before they become costly disasters.

WORKLOAD COMMUNICATIONS

The preceding sections discussed private application access and cyberthreat and data protection from users accessing internal and external applications. Secure workload communication extends these same protections to workloads talking to other workloads or to the internet by using zero trust cloud connectivity. Customer-defined policies specify which workload can communicate with another regardless of region, cloud provider, or network path, in hybrid and multi-cloud environments alike.

ZTA provides a scalable, secure solution that allows cloud applications to access any internet or SaaS destination, such as third-party APIs and software updates. It inspects all transactions while applying advanced threat protection and data loss prevention controls. Workloads in one public cloud can securely communicate with any cloud, public or private, with support for communications across

ZERO TRUST SD-WAN PROVIDES BRANCHES AND DATA CENTERS FAST AND RELIABLE ACCESS TO THE INTERNET AND PRIVATE APPLICATIONS WITH A DIRECT-TO-CLOUD ARCHITECTURE, WHICH PROVIDES HIGH SECURITY AND OPERATIONAL SIMPLICITY.

Question 2 What are the main use cases for zero trust?

VPCs, zones, and regions on the same cloud. ZTA eliminates lateral movement, internet attack surface, VPNs, and the complexities of bespoke cloud routing.

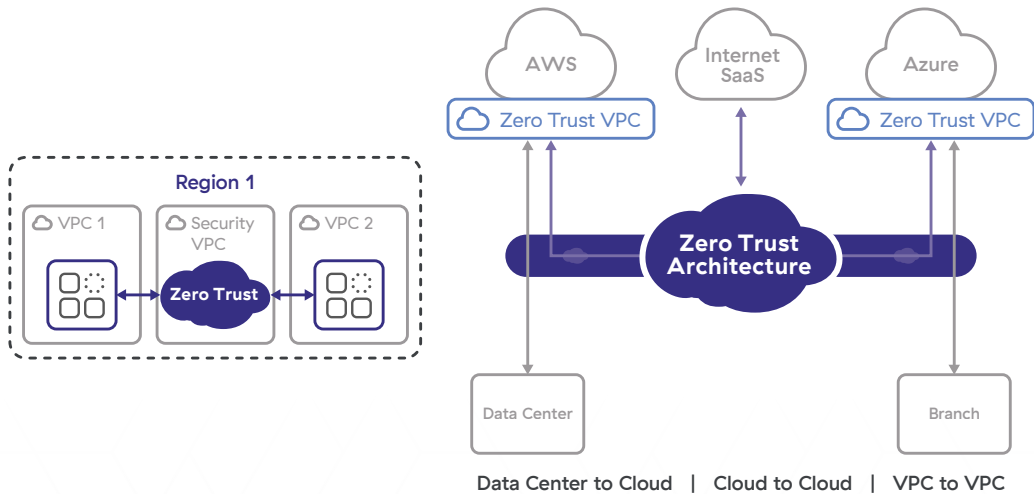


Figure 30: Zero trust connectivity for cloud workloads.

QUESTION THREE

What are the business benefits of moving to zero trust?

Question 3 What are the business benefits of moving to zero trust?

As a company moves forward with a zero trust transformation, valuable benefits can be positioned as technology-led business initiatives. These can be used to sway the organizational culture into accepting and embracing the proposed changes. Digital transformation provides a number of specific business benefits:

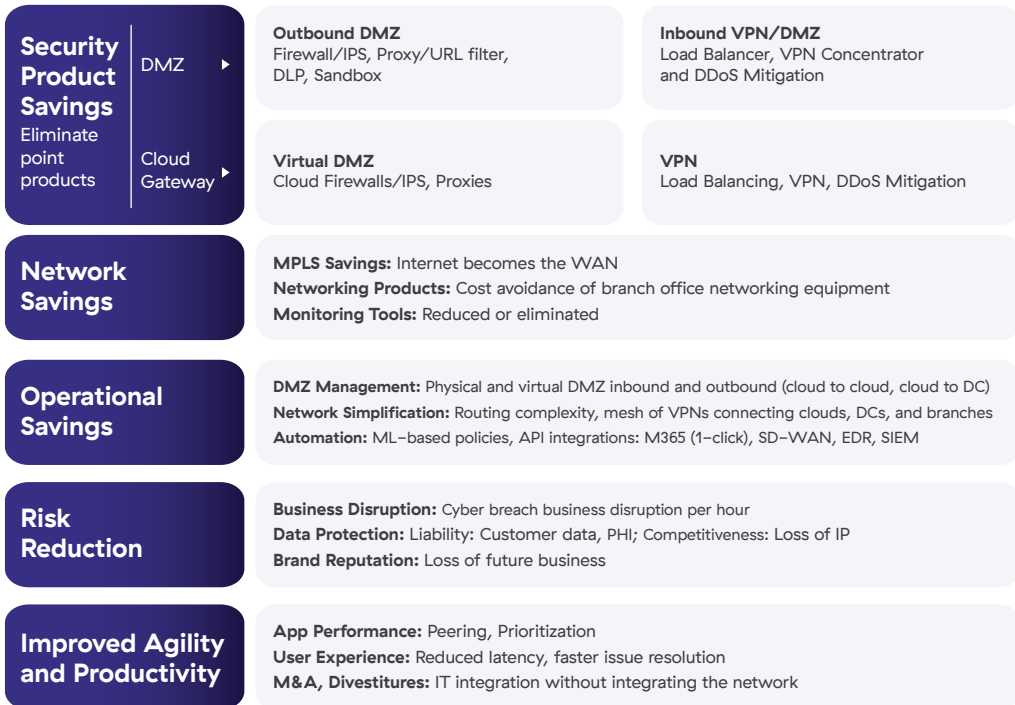


Figure 31: The business benefits of zero trust architecture.

Traditional investments made in security technologies such as firewalls and VPNs increase cost and are justified based on perceived risk reduction. Yet, any architecture that adds to the attack surface, as appliances in routable networks do, is inherently risky. Zero trust transformation done right can reduce cost, complexity, and cyber risk, all at the same time. The figure below shows typical ZTA benefits by area. This is based upon actual case studies of customers. The rest of this chapter explains each benefit area in detail.

Question 3 What are the business benefits of moving to zero trust?

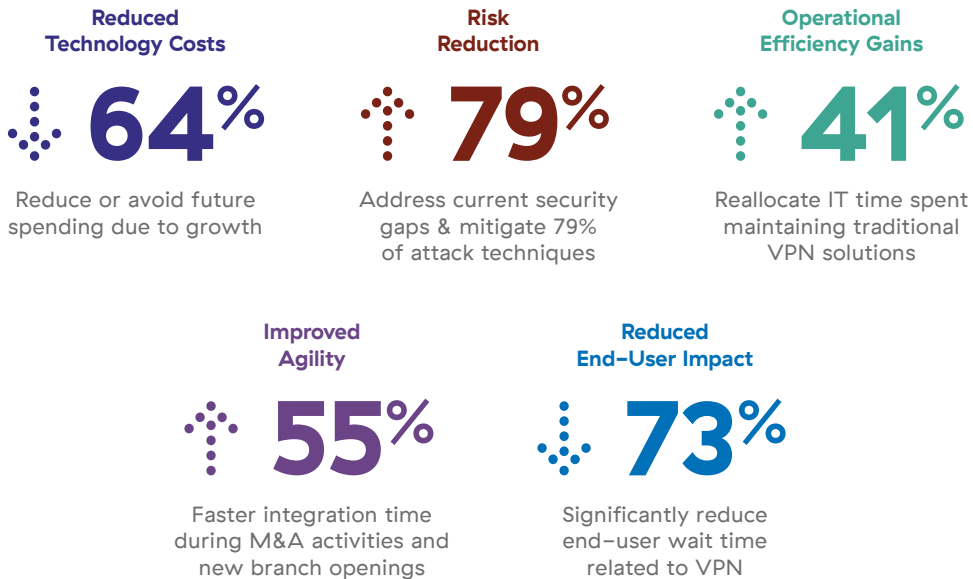


Figure 32: Resulting business benefits for a typical organization deploying a zero trust architecture.

Security Product and Network Savings

A zero trust architecture offers technology leaders a unique opportunity to deliver business functionality while ensuring cost optimization. Short-term returns manifest by removing the technical infrastructure that ZTA replaces, such as stacks of hardware once used to protect traffic to data centers, offices, or factories. Once a leader can financially demonstrate benefits to the business, it becomes infinitely easier to justify moving to ZTA.

Question 3 What are the business benefits of moving to zero trust?

When calculating transformation-related cost savings, include reduced hardware infrastructure and bandwidth cost reductions. The cost of hardware-based solutions is typically an upfront sunk cost (for the hardware itself), plus yearly maintenance and upgrade costs. Much of the hardware security equipment that sits in the data center can move to the ZTA cloud and be consumed on a subscription basis.

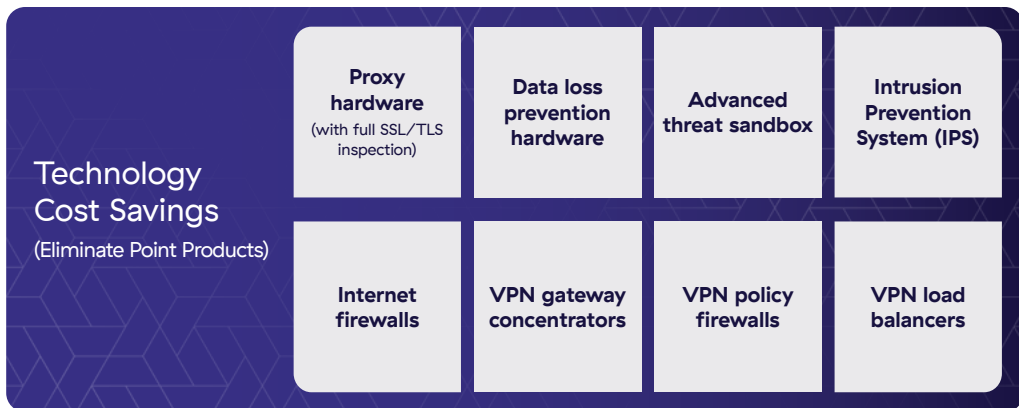


Figure 33: Zero trust architecture eliminates many point products, resulting in significant technology cost savings.

Additionally, capabilities that are hosted in the cloud can also be subsumed by the zero trust cloud, leading to vendor consolidation and subsequent cost reduction. Examples include cloud firewalls, virtual load balancers, transit gateways, VPNs, etc.

MPLS subscription costs are another candidate for savings, based on the bandwidth and service requirements of each branch location. It is likely that these costs will not go away entirely, as certain locations may still require MPLS circuits back to the data center(s), but many organizations can achieve up to 50–70% in savings.

Note that all of these cost savings won't come at once, as different use cases may take priority. Take the example of an

Question 3 What are the business benefits of moving to zero trust?

enterprise that wants to deliver ZTA for secure internet access. ZTA offers granular controlled access from any initiator to any destination, but without using a network for control. Its implementation allows an organization a chance to streamline its access control processes.

These controls, normally hosted in an outbound DMZ within a centralized network hub, contain a set of solutions to protect the enterprise traffic going to the internet, such as firewalls, IPS, proxy, and DLP. The cost of these services is not simply measured in the physical boxes, their interconnections, or even power consumption, all of which are valid costs. They also waste resources (through management expenses and support costs) by performing redundant operations. This amount is then multiplied by the total number of control hubs that an enterprise must operate across various geolocations.

THE ENTERPRISE CAN EXCHANGE MULTIPLE, REDUNDANT, CASCADING EXPENSES FOR THE SINGLE COST OF MAINTAINING A MORE SECURE AND ACCESSIBLE ZTA PLATFORM.

With a ZTA deployment, an enterprise can simply remove all of these services. The ZTA offers all of these controls concurrently, around the world. The enterprise can exchange multiple, redundant, cascading expenses for the single cost of maintaining a more secure and accessible ZTA platform.

Operational Savings (Reduced Complexity)

Delivering highly optimized business functions is invaluable to a technology leader. Zero trust architecture allows enterprise technology to move from being a bottleneck that the business will bypass to being the reason the business is competitive and able to execute at a high level.

The lack of optimized business functions comes from the complexity within many organizations' network and security infrastructure. This is caused by a number of factors:

- Point products
- Disparate policy management
- Routing complexity
- Network-based segmentation
- Limited visibility and inability to troubleshoot issues

Moving to a cloud-based zero trust architecture provides a number of operational advantages that reduce complexity.

To quantify the business benefits, compute the full-time equivalent (FTE) required to perform the same tasks on a traditional network and security architecture. Compare those numbers to the benefits above. This should be done in FTE hours saved multiplied by the typical hourly rate of an FTE, which will yield the overall cost savings. There is also the added benefit of freeing up FTE time for other projects.

Question 3 What are the business benefits of moving to zero trust?

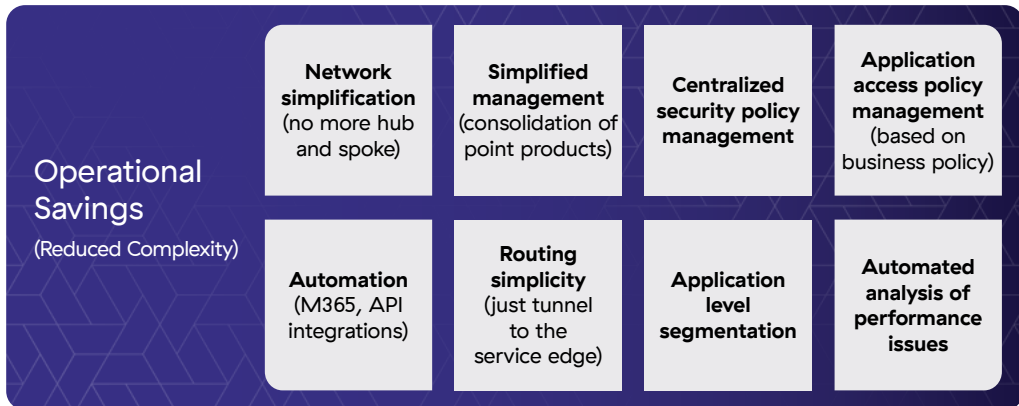


Figure 34: ZTA enables several operational efficiencies for IT.

Many operational savings are enabled by the insights and visibility provided by zero trust architecture. Zero trust gives visibility into the structure of the IT ecosystem, traffic patterns, and outliers.

For example, application access policy management can be based on the traffic flowing through the zero trust platform and understanding the access needs of the enterprise. Figure 35 depicts how zero trust can easily map the requirements for one team within an organization. Consider the following line of questioning:

Question: What part of the enterprise needs access?

Answer: The members of the account and finance teams

Question: What needs to be accessed?

Answer: SAP accounting process

Question: What controls need to be applied?

Answer: Only read access for some users. Write for others.
No download of financial information to desktop

Question 3 What are the business benefits of moving to zero trust?

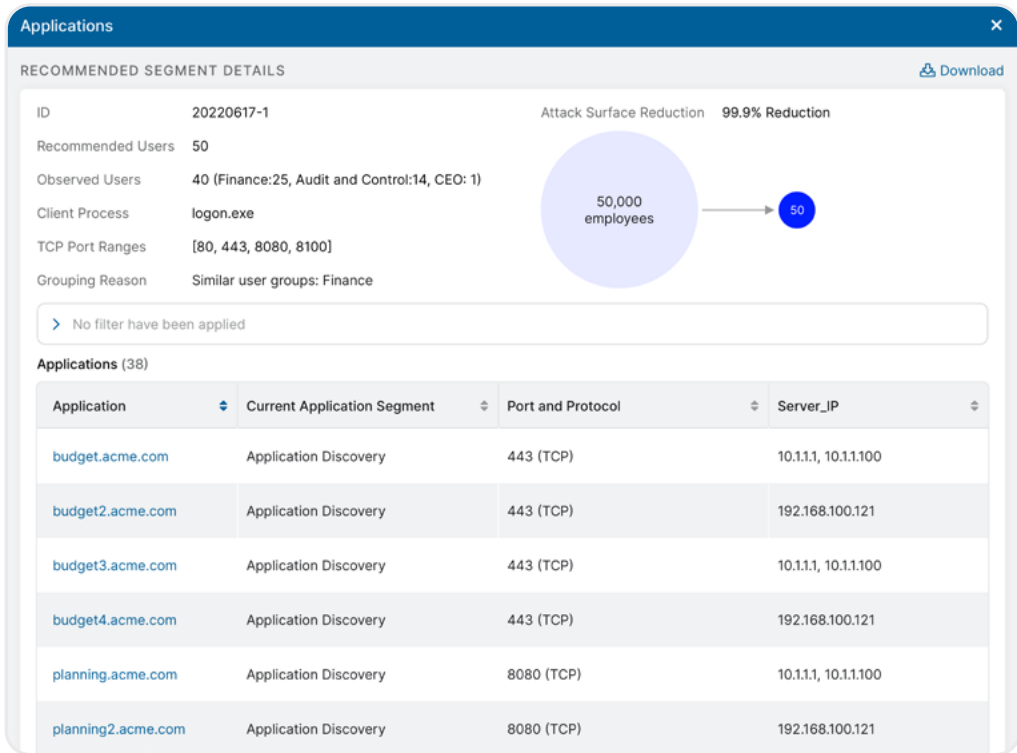


Figure 35: Zero trust provides visibility into user-to-app access requirements and makes segmentation recommendations to reduce the attack surface.

In a zero trust journey, creating this knowledge baseline is critical for the creation of application segmentation policies. Additionally, the insights provided by zero trust into data classification and cloud application usage greatly simplify the creation of security policies.

Operational efficiency also applies to end users, in that zero trust provides an “always on” and “it just works” experience. A zero trust architecture makes the decision on the best path to connect each and every session. The experience of each session is optimized and controlled dynamically at each access, ensuring the best performance for the end user.

Question 3 What are the business benefits of moving to zero trust?

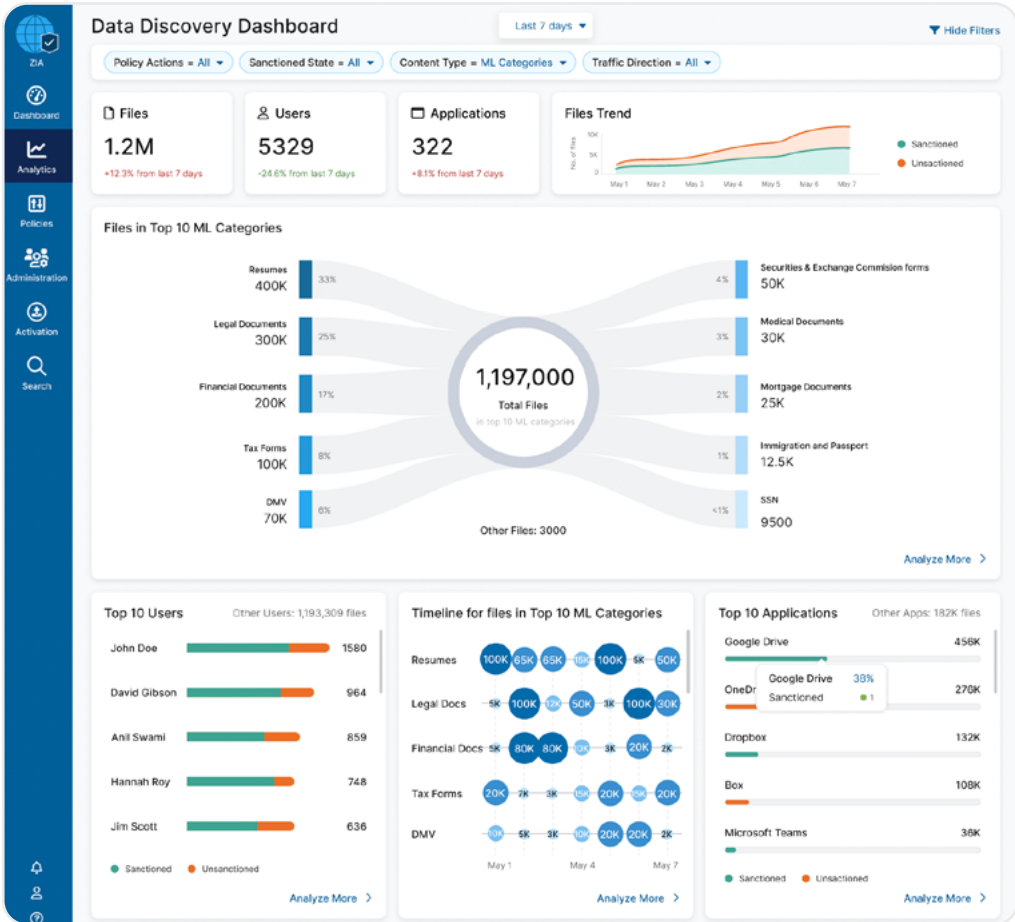


Figure 36: Zero trust increases visibility into the environment through automated data classification.

This is most evident when compared to network-based control solutions (e.g., firewalls, VPNs, and routers), which require the initiator and destination to share a routable network with the control device. This is the historic castle-and-moat design, where all services and controls are centralized. To access services (through the controls), users had to either be onsite and connected to the network, or they needed to remotely connect via VPN. This design at a network level chokes and restricts the efficiency of enterprise services.

Risk Reduction

Enterprises are particularly concerned about security breaches where intellectual property or sensitive data is lost. This fear becomes exacerbated when controls are minimized, as any employee can visit the web at high speed; anyone could upload and download content from clouds without regard for the personal or professional protection of data. With data, the drive for accessibility and functionality is often prioritized over its security. Yet, easy and open access to data can be a ticking time bomb for an enterprise.



Figure 37: Zero trust reduces many risks by improving security and preventing data loss.

Risk reduction is difficult to quantify with a single monetary figure. Suffice to say, the data protection capabilities of ZTA are immense. ZTA is able to block cyber threats, apply inline controls for data in motion and out-of-band controls for data at rest, and do so for each and every request from an enterprise. This gives organizations unprecedented visibility, and ultimately control, of the enterprise data. The power of cloud computing far exceeds the capabilities of legacy hardware and traditional data center security, which simply cannot scale.

Question 3 What are the business benefits of moving to zero trust?

Zero trust provides efficient access to an allowed application while offering the ability to view, validate, control, and protect company information. This is true regardless of the location of the assets and requestors. By being an overlay function (that being “overlaid” over any network), the beauty of ZTA is that it will work over other networks, all while ensuring the enterprise users, workloads, IoT/OT, and content are protected.

This control protects against the loss of intellectual property. The same techniques used to validate traffic and content can assess and control the loss of critical information. Businesses cannot only define the types of files or content that they do not want to lose but also leverage intelligence to ensure their critical content does not go to the internet.

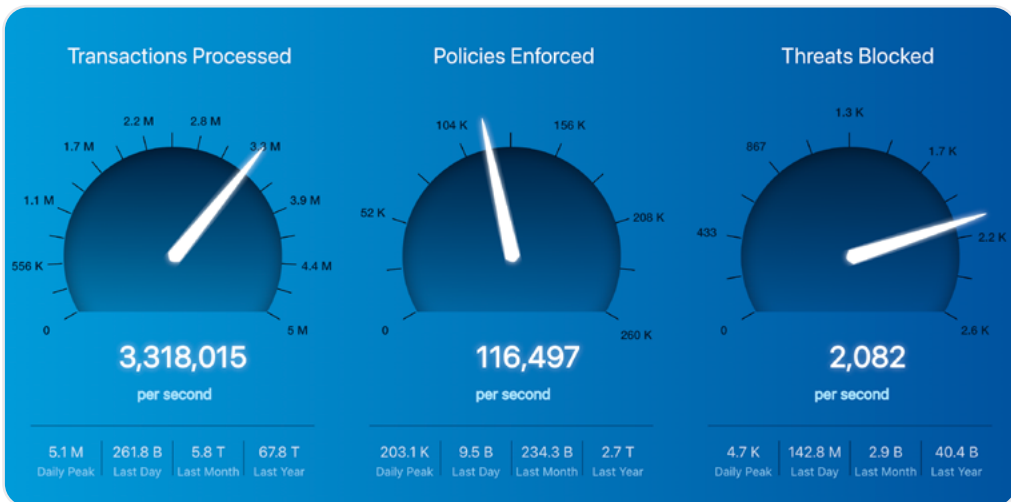


Figure 38: Zero trust architecture enforcing policies and blocking threats at scale.

Out-of-band control is important as it addresses risks that are stored “at rest” within SaaS, PaaS, IaaS, or other cloud solutions. This provides enterprises with a full view of inbound threat paths and actively identifies threats before malware is downloaded, shared, or launched.

Question 3 What are the business benefits of moving to zero trust?

It also can apply advanced threat prevention like sending thousands of files to a sandbox, or scanning encrypted traffic to prevent malware and data loss. Additionally, increased visibility into shadow IT blocks malicious content within minutes rather than days for breach prevention and a reduced risk of business disruption.

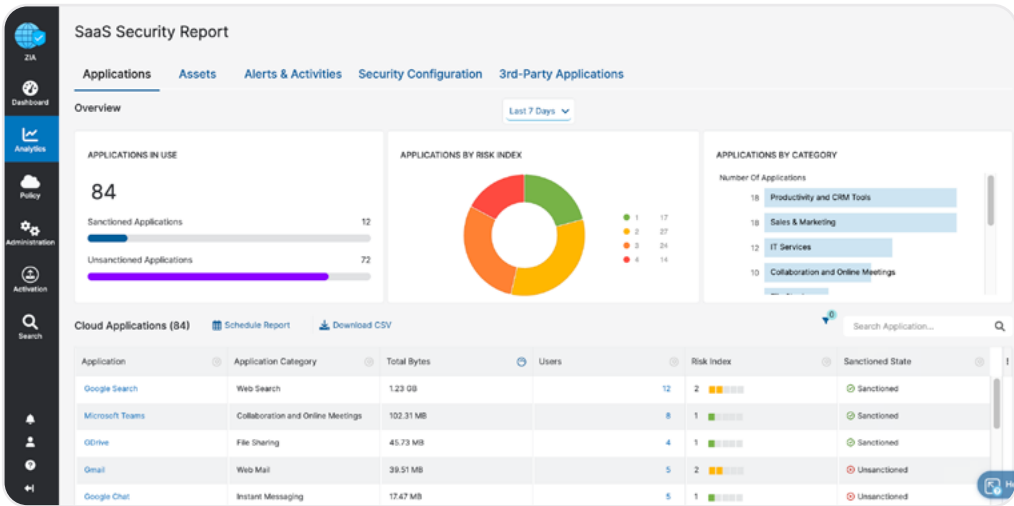


Figure 39: Zero trust architecture can identify sanctioned and unsanctioned SaaS usage.

To quantify the business benefit, consider factors like the disruption cost per hour, loss of future business, loss of competitive advantage, or customer churn. Calculate the total of a loss event with traditional security and compare it against the cost of a zero trust solution.

Improved Agility and Productivity

Looking beyond the operational efficiencies, there are the productivity gains that will benefit the workforce as well as the agility gains that will benefit the business. In terms of productivity benefits, zero trust reduces complexities and simplifies how users connect, all through a scalable and resilient cloud security platform. This architecture leads to four key gains:

- Improved application performance
- Fewer outages and maintenance windows
- Fewer VPN-related support tickets
- Faster resolution of support tickets

More important, however, is the innovation that zero trust allows due to its agile nature. Deploying zero trust allows for faster branch deployment, quicker M&A integration, or adoption of next-generation business-enabling technology, for example.

To demonstrate, consider a global company's point-of-sale (PoS) operation across thousands of stores.

Before ZTA, the global retailer had to configure systems on a per-store basis to enable POS devices for several reasons:

Question 3 What are the business benefits of moving to zero trust?

- The security team mandated, rightfully, that all financial transaction data must exist, run, and communicate on a dedicated “secure network.”
Note: Store networks would vary depending on the store type. Some may have cameras, doors, guest WiFi networks, etc. But the PoS network and protection was mandatory
- This network required connectivity, which was deployed with an SD-WAN service for both internet and MPLS connectivity. In addition, a firewall function was needed to isolate the PoS service from the rest of the network.
- There was no global/unified protection for internet consumption.
- Lead time, architecture, infrastructure installation, management, etc., not to mention the supply chain restrictions, put lots of store deployments at the whim of providers.



Figure 40: Zero trust fosters innovation by increasing business agility.

The company, convinced by the integrity and efficiency of zero trust over any network, rebuilt their store solutions with ZTA. Gone was the complex infrastructure. This was replaced by Android-, iOS-, and Windows-based PoS solutions, all of which had 4G, 5G, and WiFi connectivity directly built in. While the network functions become “direct,” ensuring PoS transactions happen across the

Question 3 What are the business benefits of moving to zero trust?

dedicated network wasn't possible. That is, until the security team realized that zero trust ensured each PoS transaction would not only pass over its own unique and encrypted session but could also steer that PoS exactly to where it needed to go.

Once security observed the greatly improved security function, protection of the data, and the enablement of the business, they signed off on the new store PoS system.

When properly executed, a zero trust journey will lower the end cost impact on a business. This cost benefit will not only deliver improved efficiencies and optimizations but will drive innovation for future projects. All this, while also delivering protection to the enterprise's users, data, and intellectual property.

END-USER IMPACT

While zero trust improves the operational efficiency of IT, as discussed above, there are numerous gains for employees as well. By providing seamless access to private applications without the need for insecure VPN connections, many hours of unproductive time can be eliminated.

Taking the case of VPN usage, any employee working remotely would spend several minutes of their day logging into their VPN client.

While this may seem insignificant for an individual, collectively this delay results in many, many thousands of lost hours of work (see Figures 41 and 42). Zero trust makes application connectivity seamless.

**WHEN PROPERLY EXECUTED,
A ZERO TRUST JOURNEY
WILL LOWER THE END COST
IMPACT TO A BUSINESS.
THIS COST BENEFIT WILL
NOT ONLY DELIVER ON
IMPROVED EFFICIENCIES
AND OPTIMIZATIONS, BUT
WILL DRIVE INNOVATION
FOR FUTURE PROJECTS.**

Question 3 What are the business benefits of moving to zero trust?

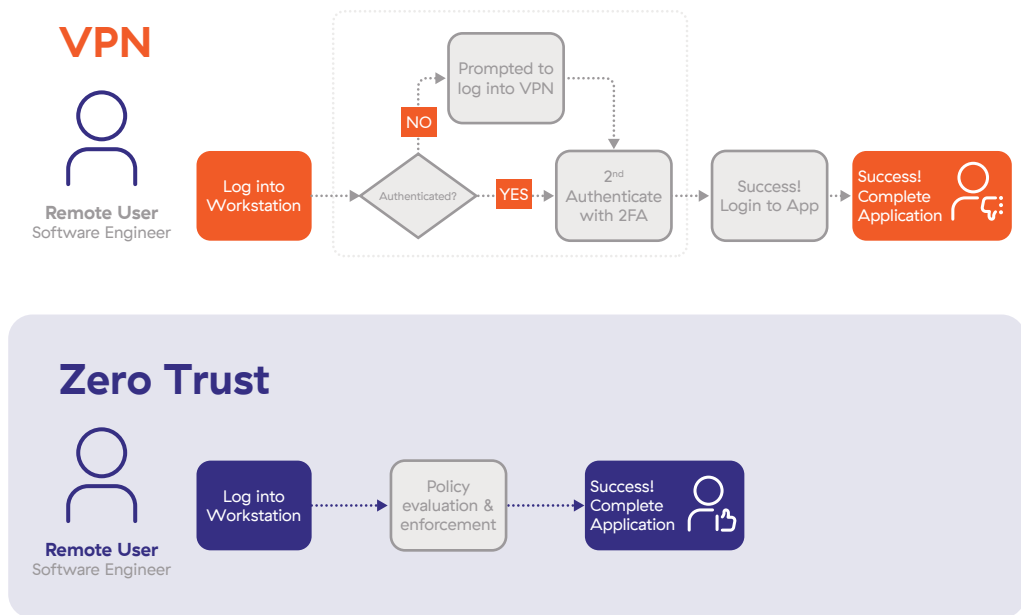


Figure 41: Zero trust reduces the inefficiencies end users experience when using VPNs.



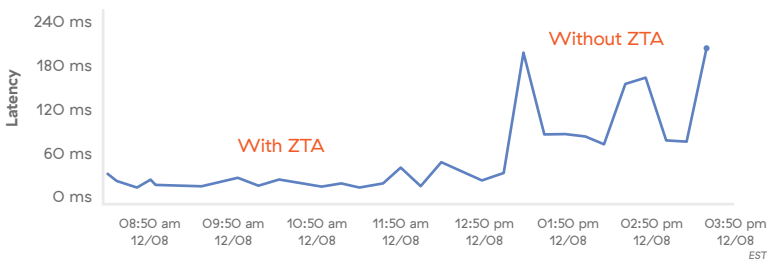
Assumes 23K remote users experiencing six minutes of unproductivity per working day. 50% improvement from Zscaler.

Figure 42: VPNs lead to high labor expenses.

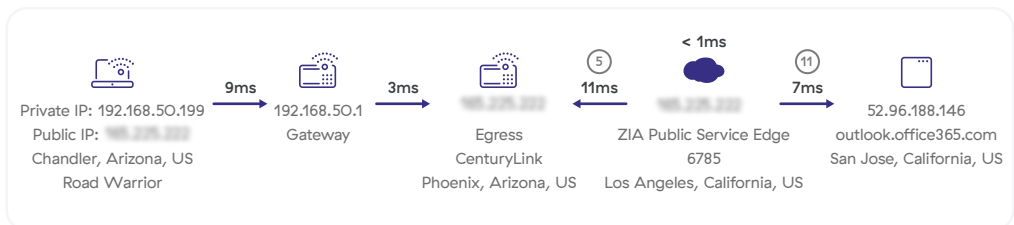
For third parties like contractors and customers, gaining access to private applications also presents difficulties, since installing VPN agents on unmanaged devices is a challenge and there are risks associated with exposing these applications on the public internet. With zero trust, secure access can be granted to these third parties without the risks of exposure.

Question 3 What are the business benefits of moving to zero trust?

Also consider the improvement in response times for employees accessing applications. Traditional routing would often hairpin internet-bound traffic from a remote location or branch office through the data center to send it through the security stack. ZTA provides local internet breakouts for branches, eliminating the “hairpin” with a direct path (through the distributed ZTA cloud) to the application, cutting the response time significantly. For the remote worker, the elimination of VPNs also allows a more direct path to the application, again over the distributed ZTA cloud.



With ZTA, total latency is 40ms



Without ZTA, total latency is 183ms

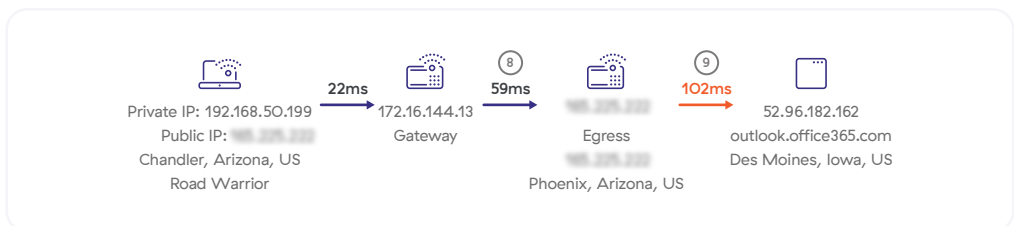


Figure 43: Comparison of end-to-end latency with and without ZTA for a remote worker. Without ZTA, excess latency is incurred by hairpinning traffic to the data center where the VPN concentrator is hosted.

Quantifying the Zscaler Business Benefits

An example of business benefits for typical organizations is shown below, based on the Zero Trust Exchange:

Verified customer benefits

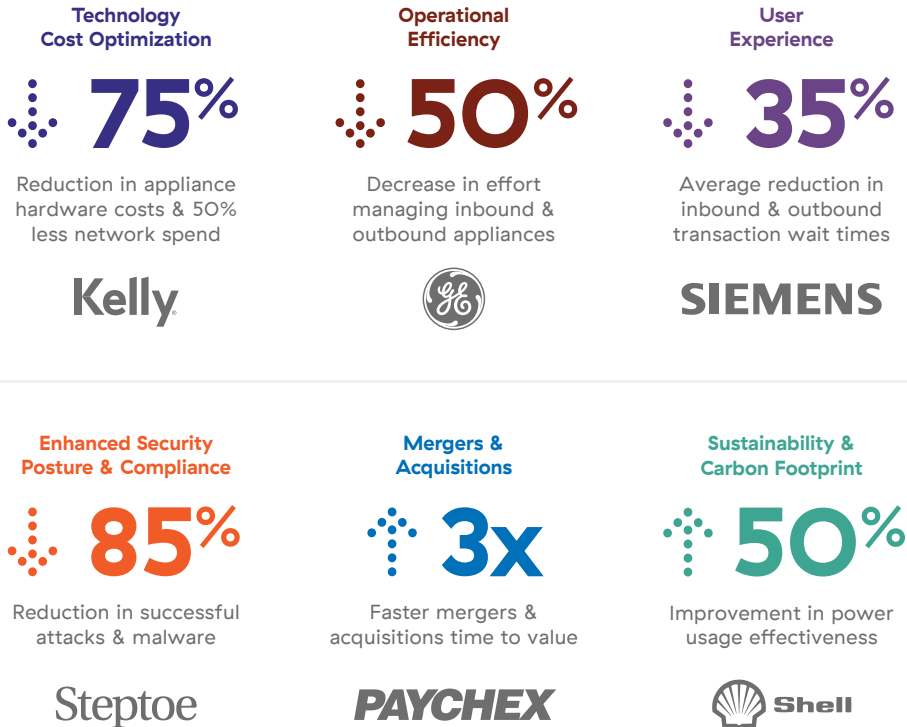


Figure 44: Verified business benefits for a number of organizations who are all using the Zscaler platform.

Question 3 What are the business benefits of moving to zero trust?

Realized benefits of Siemens with Zscaler

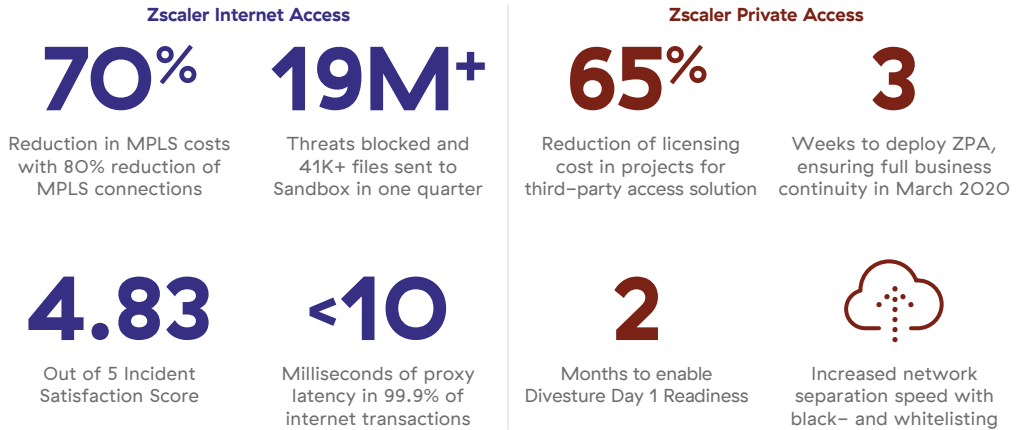


Figure 45: Proven Zscaler business benefits for Siemens.

Question 3 What are the business benefits of moving to zero trust?



There are several [factors in going zero trust]! Obviously, the primary goal is improved security, but many other benefits flow from this including:

- Simplified network architecture with policy enforcement for every connection.
- Better user experience by allowing users to more directly connect to the resource they need (e.g., avoiding hairpinning through a data center to get to Microsoft 365) and giving them a consistent experience independent of where they are connecting from. You are "always" connected securely.
- Financial benefits by simplifying network design and eliminating network equipment and its associated upkeep and support.

The security benefits are many, but include reduction or elimination of your internet attack surface, and the elimination of lateral movement by only connecting to the resources you are authorized to use.”

Greg Simpson

Former Chief Technology Officer, Synchrony

Alex Philips
CIO, NOV Inc.

How I drove secure digital transformation

Alex Philips is the Chief Information Officer of NOV Inc. In this position, Alex is responsible for overseeing all aspects of Information Technologies, Systems, Applications, and Security to further NOV's strategic goals. Alex joined Phoenix Energy Services, now a part of NOV, in 1997 as an IT Network Administrator. During Alex's 25-year tenure at NOV, he has served in various roles including IT Infrastructure Manager, ERP Director, and Chief Information Security Officer. Alex was promoted to Chief Information Officer in July 2015.

As the CIO of NOV, my job is to make sure that IT infrastructure and security enable our business to power the people who power the world. By this, I mean our 27,000 employees across 60 countries working with thousands of partners, suppliers, and customers. They all require secure, reliable technology anytime, anywhere, on almost any device—the same reliability we expect when accessing electricity and water. Over the last several years, I led a secure digital transformation that made NOV more agile and adaptable to challenges thrown our way.

A TRANSFORMATION TO CLOUD AND ZERO TRUST

Like many enterprises, we had a legacy IT environment that included data centers, hundreds of branch offices, factories, and OT systems, connected via a hub-and-spoke network. We used a castle-and-moat security model with ever-expanding layers of security appliances to address each new threat vector. We relied on multiple VPN technologies for remote access. It was expensive and not flexible enough to support our increasingly mobile and dynamic business.

I needed to reduce cost, improve security, and make life easier for both our users and IT administrators. I needed our systems to work all the time, aka gain resiliency. It had to be a win across all these goals, so we set out two main priorities.

First, be “cloud smart” and take advantage where it can help. I had heard way too many horror stories of “cloud first” mass migrations causing extreme cost overruns and business-crippling outages. We had to be smart and figure out where the cloud could add value and drive out cost. Our approach had to be evergreen, not replacing one legacy tech debt with new tech debt.

Second, transform our networks and security thinking. Focus on the internet first. Our global MPLS network was excessively expensive, and our old security appliances needed a multimillion-dollar upgrade. The majority of our internet traffic was encrypted, which we were unable to see. The bad guys were hiding in that traffic and compromising our users, then moving laterally to access high value targets.

Next, move toward zero trust. We wanted to follow the maxim “never trust, always verify,” which we later learned was called a zero trust architecture. This meant enforcing access policies based on multiple contexts—user's role, location, device posture, and the applications they are permitted to access.

**THE BAD GUYS WERE HIDING
IN THAT TRAFFIC AND
COMPROMISING OUR USERS,
THEN MOVING Laterally TO
ACCESS HIGH VALUE TARGETS.**

As we say in Texas, “We might need a new horse.” Sometimes your old horse can't adapt and you need a new one. Sure, you love and find comfort in the old steed, but it can't take you where you need to go next. Our existing technology vendors and channel partners proposed we buy more of what they were already selling us. “Don't change,” they said. “Double down with what got you into this predicament.” Maybe they could help us win with a couple of goals, but not all of them. We would need to explore new horizons.

OUR PHASED TRANSFORMATION JOURNEY

A successful digital transformation is a journey that doesn't happen all at once. Progress came in increments with each experience influencing successive phases:

Phase 1

Collaboration solution

During phase one, we adopted Microsoft Office 365. Collaboration and sharing of large datasets was painful and we had outgrown our email system. We began rapidly migrating hundreds of terabytes of emails, files, SharePoint data, etc. This delivered immediate productivity value and business flexibility, even with our legacy network and security appliances still in place.

Phase 2

Secure access to internet and SaaS from anywhere

Phase two had **three steps**. First, we enabled secure access to the internet and SaaS applications through the Zscaler Zero Trust Exchange. This was deployed on our existing legacy MPLS global network in 60 days for the entire company, simultaneously, while phase one was executing. It immediately gave us resiliency and increased our security posture.

Step 1: Global ZTA rollout

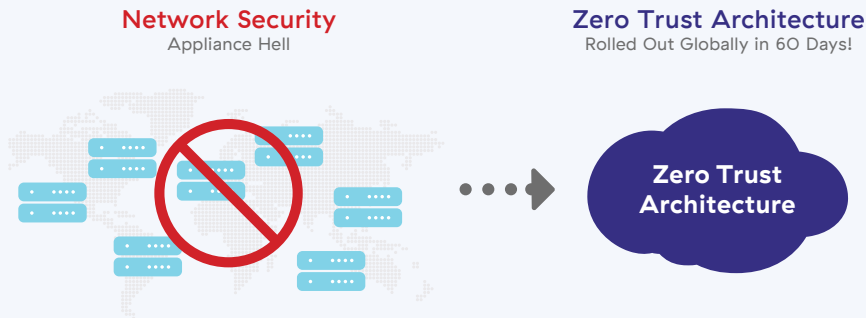


Figure 46: Eliminating hardware by moving to zero trust can save significant costs while reducing data traffic on overburdened corporate data centers.

The next step of phase two was to eliminate our MPLS networks and provide local internet breakouts. This resulted in millions of dollars in savings, faster connections, and enabled direct access to SaaS applications such as Office 365 by eliminating traffic through a centralized hub.

Step 2: Local internet breakouts

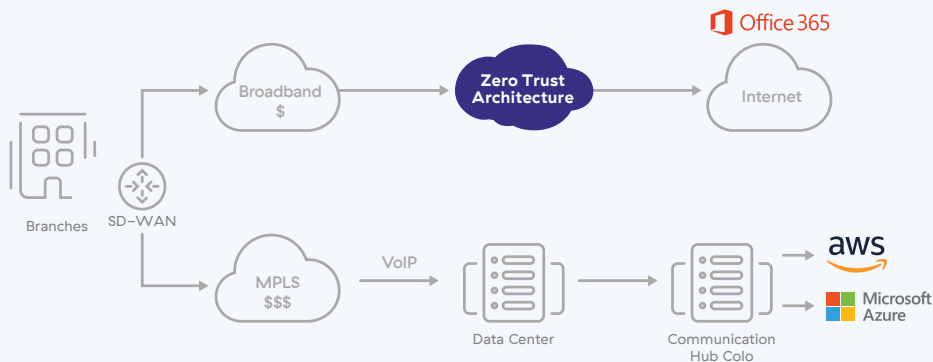
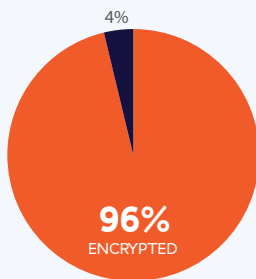


Figure 47: Improving performance by eliminating MPLS and using local breakouts can bring costs down by 4x while delivering a 10-20x faster user experience.

The final step involved turning on TLS inspection capabilities to detect and block threats hidden in encrypted traffic. This significantly improved our risk posture.

Step 3: TLS inspection required to block threats hidden in encrypted traffic

Traffic volume by protocol



■ Encrypted Traffic ■ Unencrypted Traffic

Quarterly advanced threats blocked in TLS traffic

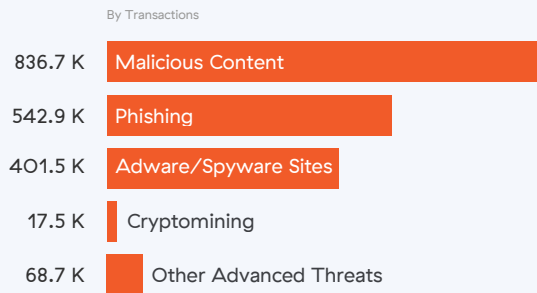


Figure 48: Given the high percentage of encrypted traffic, enabling TLS inspection reveals hidden threats, and allows for them to be blocked.

Reduced computer reimaging after moving to zero trust

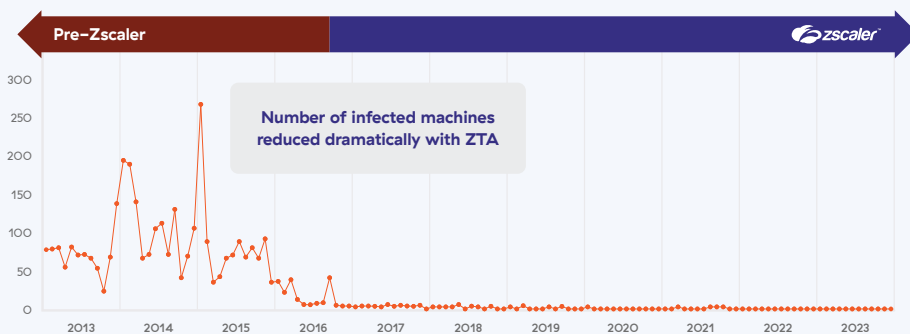


Figure 49: Moving to zero trust significantly reduced the number of computer wipes and reimaging required due to a reduction in malware infections.

Phase 3

VPN replacement with zero trust security

In phase three we replaced multiple remote access VPN solutions and provided fast and secure zero trust network access (ZTNA) to private apps using Zscaler Private Access. This allowed NOV employees and our third-party contractors access to 7,500 NOV applications in multiple data centers and public cloud regions directly over the internet. We did this a few years before the COVID-19 lockdown, so we were fully prepared to support our users' need to work from home without any interruption.

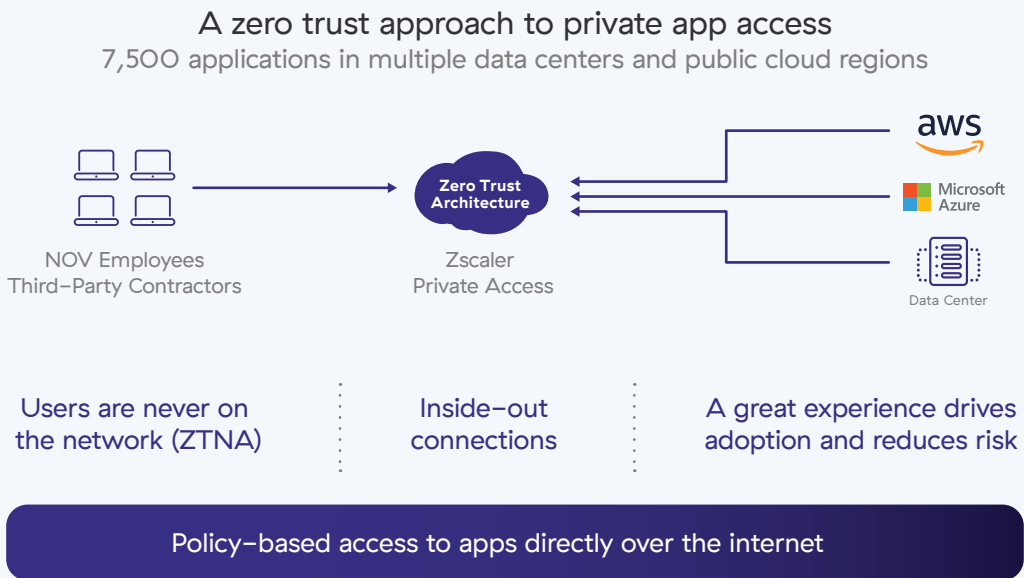


Figure 50: Users are able to securely access apps over the internet from anywhere through ZTA.

Thanks to our cloud transformation journey,
we were ready for WFH

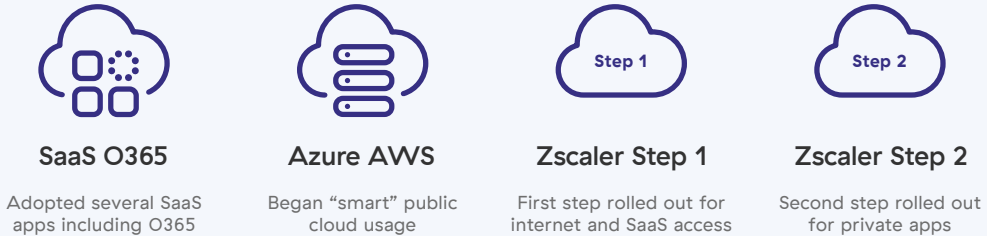


Figure 51: Cloud transformation enabled WFH, with Zscaler rolled out for secure access to internet/SaaS and private apps.

Phase 4

Move private apps to the cloud and consolidate data centers

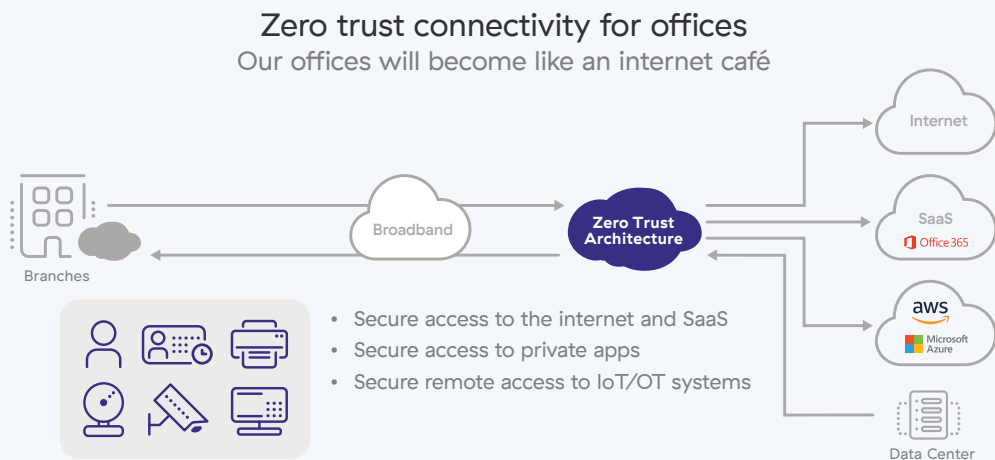
Phase four required two steps. First, we moved our critical customer-facing applications into AWS. Then we moved our many regional data centers, which lacked the scale needed to operate efficiently, to Azure.

Phase 5

Zero trust connectivity for offices

This upcoming phase of our transformation will be the most exciting. Its genesis arose from a question collectively asked by all of our users working remotely from home. If we all can work fine remotely in a zero trust manner, why can't we do that when at our facilities? Do we even need the network? How can we provide ZTNA to devices without identity such as printers, barcode scanner guns,

time clocks, IoT, and OT systems? Legacy networks are a security risk due to a lack of identity and we are going to replace it with zero trust access! With zero trust connectivity, our offices will become like an internet café, and we will no longer extend our corporate network to every office. This step is critical for eliminating lateral threat movement.



**Don't extend the network to every office.
Eliminate lateral threat movement.**

Figure 52: The final phase of zero trust secures work from anywhere connectivity, on any device, and brings the café computing experience to offices.

Many of these phases are complete and some are still ongoing due to contractual commitments. Phase five is just getting started. The journey hasn't always been a straight line, but I can proudly say that we are overachieving our goals.

Here are some of the lessons I learned from our transformation journey:

- Moving from legacy networks and security to zero trust is an architectural change. As it requires cultural and mindset changes, we identified forward-thinking leaders early on in our journey who helped us drive this initiative.
- Choose an integrated platform that not only secures users but also workloads and IoT/OT systems.
- Select a partner who has a highly reliable security cloud. Zscaler's more than 10 years of operational experience in managing the largest security cloud has delivered us high-performance service without interruptions to our business.
- Don't boil the ocean—just get started. Look for quick, small wins that are easily achieved to drive organizational acceptance of this journey

Our secure digital transformation has made NOV business a lot more agile. It has saved millions of dollars, improved user productivity, and reduced our cyber risk.

QUESTION FOUR

How does zero trust drive success for organizations?

Question 4 How does zero trust drive success for organizations?

Now that the basics of zero trust architecture and its accompanying benefits are understood, how can organizations successfully adopt the framework? Many organizations have a multilayer security stack that represents years of reactive security thinking. Security leaders know it is far easier to justify buying new technology than attempting to replace existing solutions. Finding a security offering that addresses a specific risk gives stakeholders a quick and easy way to solve one problem. Making the case for doing security a new way, to address several problems, is a heavier lift.

One foreseeable objection is that the current system works well enough, so why make any changes? Other organization members, for example, those currently tasked with operating and maintaining the current security stack, have a vested interest in the status quo. It is also possible that the CIO or CISO is not entirely sure which aspects of the security posture are providing the most value. Inheriting

years worth of security solutions that are layered on top of each other can be similar to assessing a large Jenga® tower. Which pieces can safely be removed without the entire structure collapsing?

In this section, we will examine organizations that successfully overcame several technical, cultural, and financial obstacles in their zero trust journey. While no two organizations are exactly alike, many share similar challenges when migrating from traditional security postures to a zero trust framework. Understanding how others navigated their way to a zero trust environment can help you successfully guide your organization's transformation journey.

INHERITING YEARS WORTH OF SECURITY SOLUTIONS THAT ARE LAYERED ON TOP OF EACH OTHER CAN BE SIMILAR TO ASSESSING A LARGE JENGA® TOWER.

Coca-Cola Consolidated

Liberating remote employees from network performance and productivity bottlenecks



Organization	Coca-Cola Consolidated
Industry	Food processing
Employees	16,000+

ORGANIZATION DETAILS

Coca-Cola Consolidated, founded in 1902, is the largest bottler of Coca-Cola products in the US. It produces and distributes more than 300 Coca-Cola products to over 66 million consumers. The company has more than 100 locations spread over 14 states and the District of Columbia. They employ over 16,000 people at manufacturing facilities, corporate headquarters, and sales and distribution centers. As a major food processor with global reach, Coca-Cola Consolidated needed reliable, secure, and transparent connectivity. Speaking on post-pandemic challenges, Darrell Thompson, CIO at the company, said, “Our culture at Coke Consolidated has always been a brick-and-mortar operation. We’re in facilities, we’re working together, we’re collaborating, we’re producing, selling, and distributing Coca-Cola. Now that we’re in this remote work environment, it’s a little bit harder to see the work happening.”



[Zero trust architecture] was easy to deploy behind the scenes and didn't interfere with the way [our employees] worked.. I can't tell you the last time I rolled out something that really gave us so much capability without much pain."

Rory Regan

**Director of Infrastructure of Information Technology Services,
Coca-Cola Consolidated**

PAIN POINTS

The performance of Office 365 took a major hit during the pandemic when thousands of users began working from home and connecting via VPN.

Microsoft Teams and other latency-sensitive applications for internal communications suffered service degradation from increased latency caused by traffic 'tromboning.'

Relying on VPN to accommodate remote workers resulted in increased infrastructure costs and a negative user experience.

SOLUTION

Adopt a zero trust provider that uses client connectors to communicate between users and apps on a per connection basis.

Peel Microsoft traffic away from other traffic to ensure quick routing and strong performance.

The organization uses a platform that displays usage metrics to ensure productivity remains on track.

Question 4 How does zero trust drive success for organizations?

BENEFITS

Coca-Cola Consolidated opted to use zero trust connectors to broker employee traffic directly to applications on a per-connection basis. This approach allowed the Microsoft 365 traffic to be isolated and optimized. The ability to segment traffic by user or application applied to other internal and external applications used by the company as well. Once users were individually connecting to specific resources through the zero trust connector, the overhead related to backhauling VPN traffic was eliminated and performance improved.

Another benefit to secure, per-connection, zero trust segmentation is the transparency it gives to operations. It becomes easy to identify which resources are accessed, by whom, and how often because these details are at the core of network functionality. Zero trust architecture can inspect encrypted traffic, which denies attackers a popular attack vector for exploiting organizations. Embracing a zero trust cloud architecture let Coca-Cola Consolidated securely support its remote workforce without suffering productivity issues or exposing themselves to massive risks.

[Read the full success story](#)

**EMBRACING A ZERO TRUST
CLOUD ARCHITECTURE LET
COCA-COLA CONSOLIDATED
SECURELY SUPPORT THEIR
REMOTE WORKFORCE
WITHOUT SUFFERING
PRODUCTIVITY ISSUES OR
EXPOSING THEMSELVES TO
MASSIVE RISKS.**

Sandvik Group

Staying competitive while advancing the world through engineering



Organization	Sandvik Group
Industry	Industrial engineering
Employees	37,000+

ORGANIZATION DETAILS

The Sandvik Group, headquartered in Stockholm, Sweden, was founded in 1862. It holds more than 6,000 patents related to industrial tools, advanced stainless steel, alloys, and mining/construction equipment. As a global leader in mining, rock processing, and machining technology, the company sees nearly 20,000 users accessing its applications at any given time. These users include vendors, consultants, contractors, and its 37,000 employees deployed to 600 sites located across 140 countries.



Prior to the pandemic, VPN technology was increasingly insufficient for supplying secure connections that encouraged productivity. When the pandemic required sending most of our workforce remote almost overnight, we needed to modernize immediately.”

Michael Alvmarken

**Service Manager for Cybersecurity and Technology,
Sandvik**

PAIN POINTS

The organization experienced productivity issues due to its immense workforce relying on VPN for connectivity.

Users, frustrated with VPN-related access barriers, were discovering and using unauthorized shortcuts to circumvent the problem.

Connectivity and latency problems were exacerbated during the COVID-19 pandemic when the business transitioned to a work-from-anywhere (WFA) model.

SOLUTION

Sandvik adopted a zero trust platform that connects users to individual apps through a client connector, resolving connectivity problems and improving access speeds.

Sandvik IT teams use the platform to exercise granular control over access to company resources worldwide. Strong IAM measures improve security and reduce the risk of unauthorized access to company resources.

App-based segmentation limits the potential damage threat actors or malicious users with valid credentials can cause.

Question 4 How does zero trust drive success for organizations?

BENEFITS

By using per-app authentication, Sandvik eliminates the risk of lateral movement in their environment. Their attack surface is greatly reduced, as business applications and other resources are secured behind a zero trust cloud and rendered invisible to public browsing. This arrangement works seamlessly with Sandvik's WFA policy, providing reliable and secure connections to their users and contractors around the globe. Michael Alvmarken, Service Manager for Cybersecurity and Technology at Sandvik, says, "We received comments like 'Wow, we don't have to log into the VPN!?! That's amazing.' Users repeatedly called our new approach lightning-fast."

[Read the full success story](#)

THIS ARRANGEMENT WORKS SEAMLESSLY WITH SANDVIK'S WFA POLICY, PROVIDING RELIABLE AND SECURE CONNECTIONS TO THEIR USERS AND CONTRACTORS AROUND THE GLOBE.

Carlsberg Group

Serving up security perimeters around people, not networks



Organization	Carlsberg Group
Industry	Beverages
Employees	40,000+

ORGANIZATION DETAILS

Headquartered in Copenhagen, Denmark, the Carlsberg Group was founded in 1847. It has since grown to own 140 brands that it distributes to 150 markets around the globe. The company employs over 40,000 people worldwide and has expanded its portfolio to include ciders, soft drinks, and bottled water. Carlsberg also had a longstanding relationship with Microsoft and needed to ensure that any steps toward digital transformation included compatibility with Office 365. The company created a bold initiative titled Sail '22 to guide its business transformation.



Our network consisted of a hub-and-spoke architecture, MPLS with central internet breakouts, and centralized security controls. Our employees had to suffer through a poor user experience.”

Jonathan Sheldrake
Director of Global Network Services,
Carlsberg Group

PAIN POINTS

Traditional hub-and-spoke network architecture and using MPLS resulted in employees having a generally poor user experience, particularly with Skype and Office 365.

Administrators lacked visibility into key aspects of the environment.

Too many applications in the environment caused a strain on IT resources.

The CIO required that any upgrades had to be performed without causing downtime.

SOLUTION

The selected zero trust provider easily integrated with Office 365 and allowed the IT team to stop maintaining ACLs, IP addresses, and DNS addresses.

The organization adopted app-level segmentation with visibility into encrypted traffic.

Assets migrated to the cloud.

Applications were consolidated in the environment and a significant number of on-prem servers were retired.

Question 4 How does zero trust drive success for organizations?

BENEFITS

After migrating to a cloud-based zero trust platform, Carlsberg went from processing 70% of traffic on its internal network to processing 70% over the internet. They reduced their application usage from 873 apps to 350 and their on-prem servers from 1,300 to 700. Carlsberg reduced its vendor partnerships to less than 20 while increasing its network bandwidth from 600 Mbit to 6 Gbit (MPLS to broadband). Most importantly, the Office 365 connections, which account for 45% of all traffic, are fast and secure. Granular access control and improved visibility have improved several aspects of Carlsberg's business operations. Jonathan Sheldrake, Director of Global Network Services for the Carlsberg Group, said, "Skype, SharePoint, OneDrive—all the things the business needs on the internet—get prioritized, and we have no more congestion. This is a big thing for us." Carlsberg is planning to expand its IT transformation to another 80 sites located in Asia.

GRANULAR ACCESS CONTROL AND IMPROVED VISIBILITY HAVE IMPROVED SEVERAL ASPECTS OF CARLSBERG'S BUSINESS OPERATIONS.

[Read the full success story](#)

Cache Creek Casino Resort

Holistic zero trust approach that makes adding and adapting functionality in the future a sure bet



Organization Cache Creek
Casino Resort

Industry Recreation

Employees 2,000+

ORGANIZATION DETAILS

Cache Creek Casino Resort, founded in 1985, has grown to become a major destination in Northern California. The company runs thousands of slot machines, hundreds of gaming tables, ten restaurants, an event center, golf course, and a four diamond-rated hotel. Cache Creek Casino Resort employs roughly 2,000 people and regularly works with contractors to keep operations running.

“ We desperately needed better remote access but I wanted to leapfrog traditional VPNs and their security and useability issues to provide a modern remote access experience that mimics being on-premises.”

Stephen Bailey
VP of Information Technology,
Cache Creek Casino Resort

PAIN POINTS

A recent cyberattack highlighted the urgent need for upgrading security.

Business required infrastructure to accommodate remote work due to the COVID-19 pandemic.

Security-hardened laptops employees used for work had serious performance issues when connected to the corporate network.

SOLUTION

Cache Creek explored a number of zero trust vendors, including those favoring substantial customization and extensive use of multifactor authentication (MFA).

The business adopted an SSE solution that routes traffic through zero trust enforcement nodes after conducting a successful proof of concept.

The company concealed infrastructure behind a zero trust cloud.

The organization updated laptops and other IoT devices to use a zero trust internet access broker, which improved performance and connectivity for remote workers.

Question 4 How does zero trust drive success for organizations?

BENEFITS

Cache Creek describes the single sign-on remote user experience as “seamless.” Their zero trust provider was able to integrate with the company’s pre-existing identity access management (IAM) to accommodate a smooth user transition. Once their zero trust solution for applications was in place, adding the additional internet access security took less than a day. Within three months, their zero trust provider inspected 1.7 TB of data, prevented 345,000 policy violations, and blocked 629 threats.

The ability to easily work from anywhere (WFA) has also improved the work environment for employees and allowed the company to broaden recruitment practices. Cache Creek

Casino Resort is 30 minutes from the nearest population center, making the commute longer than an hour for most employees. The company’s WFA capabilities have led to understaffed departments seeing 60% increases in hiring, and the ability to acquire talent from other states.

[Read the full success story](#)

THE ABILITY TO EASILY WORK FROM ANYWHERE (WFA) HAS ALSO IMPROVED THE WORK ENVIRONMENT FOR EMPLOYEES AND ALLOWED THE COMPANY TO BROADEN RECRUITMENT PRACTICES.

US Federal Government Civilian Agency

Journey from legacy network security to seamless and secure cloud was no accident



Organization	US Federal Government Civilian Agency
Industry	Government
Employees	500+

ORGANIZATION DETAILS

This US Federal Government agency is responsible for investigating significant travel accidents worldwide, developing factual records, and formulating safety recommendations. Investigators are deployed to a number of geographical environments and require reliable, secure, high-performance connections to apps when performing incident responses. The agency was directed to adopt cloud technologies in accordance with the Office of Management and Budget's (OMB) Cloud Smart strategy. By evaluating vendors authorized by the Federal Risk and Authorization Management Program (FedRAMP®), the agency found a reputable zero trust provider.



We faced multiple challenges with accessing both cloud-based applications and those in the data center. Users experienced latency and connection issues and our legacy solution also had inherent security insufficiencies. We needed a new solution that delivered a seamless and secure path to the cloud.”

CIO for the Agency

PAIN POINTS

The organization had been using a complex system of legacy network security and frustrating access processes.

Accessing applications in the cloud and in agency data centers proved challenging.

Users often experienced latency and connection issues while trying to perform assigned duties.

SOLUTION

The agency selected a well-known zero trust platform to assist with their digital transformation.

They adopted a client-to-app connection model that utilizes a security service edge (SSE) framework and resolves latency and connectivity issues.

They also implemented an advanced cloud sandbox capable of AI-powered analysis to add an additional layer of data protection.

Question 4 How does zero trust drive success for organizations?

BENEFITS

By transitioning to a ZTA, the agency was able to retire a considerable amount of its legacy infrastructure. A representative from the agency, speaking on the benefits of retiring firewalls and dismantling VPN, says, “In both cases, eliminating appliances reduces the exposure of our applications to the internet. As a result, we’ve improved security, reduced taxpayer costs, and significantly enhanced user experiences.”

BY TRANSITIONING TO A ZTA, THE AGENCY WAS ABLE TO RETIRE A CONSIDERABLE AMOUNT OF ITS LEGACY INFRASTRUCTURE.

Where field agents once had questionable connectivity, they can now reliably collaborate via online video. Improved connectivity in urban and rural areas has enhanced job performance and alleviated user frustration. The zero trust platform uses AI-powered analysis across its global ecosystem,

quickly identifying threats worldwide and offering protection to all of its customers simultaneously. The rigorous but non-intrusive IAM measures ensure unknown actors, or those posing as known users, are unable to access the environment.

[Read the full success story](#)

How is zero trust architecture deployed and adopted? What are some common obstacles?

Question 5 How is zero trust architecture deployed and adopted? What are some common obstacles?

A PHASED JOURNEY TO ZERO TRUST

Implementing a zero trust architecture (ZTA) should not be a daunting experience. Yes, it does challenge the status quo of existing infrastructure and IT functions. Yet, the journey should not be so large and all-encompassing that it stops your organization like a deer in headlights.

Ask any enterprise undergoing its zero trust journey where to start and the answer will be, "Start somewhere, anywhere, but just start." Each transition to ZTA must be tailored to the specific enterprise, and success measured by its delivery on critical use cases (see Question 2).

The pandemic's separation of users from the network is a perfect instance of delivering a zero trust outcome with large gains but minimal impact. The result of this separation is a prime example of how ZTA satisfies urgent use cases (e.g., end users having the same experience and protections on and off the network). Older network-based solutions require the users to change their behavior when off-net versus on-net.

Older network solutions are anchored in a vulnerable topography and unable to adapt gracefully to remote and mobile work. True adoption of ZTA means that initiators are moved off the network, but have an identical user experience whether in or out of the office.

A phased journey to zero trust

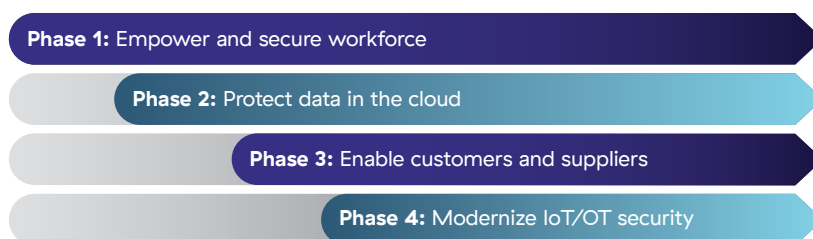


Figure 53: The four phases of the zero trust journey.

Adopting zero trust architecture is a journey and should be broken into manageable phases that demonstrate incremental business value. For many organizations, it has helped to break this transformation process into four distinct phases:

Phase 1

Empower and secure the workforce

Focus on the employees and how they are accessing public and private applications. This is often where the greatest risks lie, and where ZTA can have the most immediate impact. Digital experience management tools are a key technology for providing visibility into how things are operating in the environment. Route internet bound traffic through the security service edge, so that cyber threats are stopped and data loss is prevented. Private application traffic also traverses the service edge for zero trust protection, to eliminate the attack surface, and prevent lateral movement.

Phase 2

Protect data in the cloud

Once employee traffic is secured, it is time to secure the data that lives in the cloud. The growth of SaaS applications like Microsoft 365 and Google Workspace has made it imperative for organizations to ensure that only sanctioned data with the correct entitlements lives in the cloud. This phase should also address and regulate shadow applications, like an unofficial Box.com account, which may host sensitive data.

Question 5 How is zero trust architecture deployed and adopted? What are some common obstacles?

Phase 3

Enable customers and suppliers

While the initial focus is on employees, phase three extends zero trust protection to customers and suppliers who may also need to access internal resources. Since these users are coming from unmanaged devices, ZTA requires them to be redirected to the security service edge, where their access can be vetted. Based upon a number of factors, their connection requests may be allowed, blocked, or isolated (by sharing a pixel-streamed version of the application).

Phase 4

Modernize IoT/OT security

The final step along the zero trust journey is protecting IoT/OT resources. This entails providing zero trust access to these endpoints for employees and third parties without using a VPN. These systems should also be removed from public view, making them invisible to attackers by removing the attack surface.

A zero trust journey can be achieved in a multitude of ways. To demonstrate the possibilities, here are a few practical examples of how to start today and receive direct business benefit.

Protect Strategic Core Business Functions

ZTA is anchored in only allowing a verified entity access to a verified destination. As such, one of the simplest deployment scenarios for zero trust architecture is by first enabling granular access control for a specific set of individuals.

In this case, imagine a set of executives who need access to highly restricted and classified applications. The deployment is very simple:

- O1** Define which users (initiators) need access
- O2** Identify trusted devices (in this case, it was mobile iOS devices running a specific MDM with certificate validation in place)
- O3** Define which application (destination) is to be accessed
- O4** Configure the zero trust controls via application segmentation policy
- O5** Deploy to the user devices
- O6** Enable access

Question 5 How is zero trust architecture deployed and adopted? What are some common obstacles?

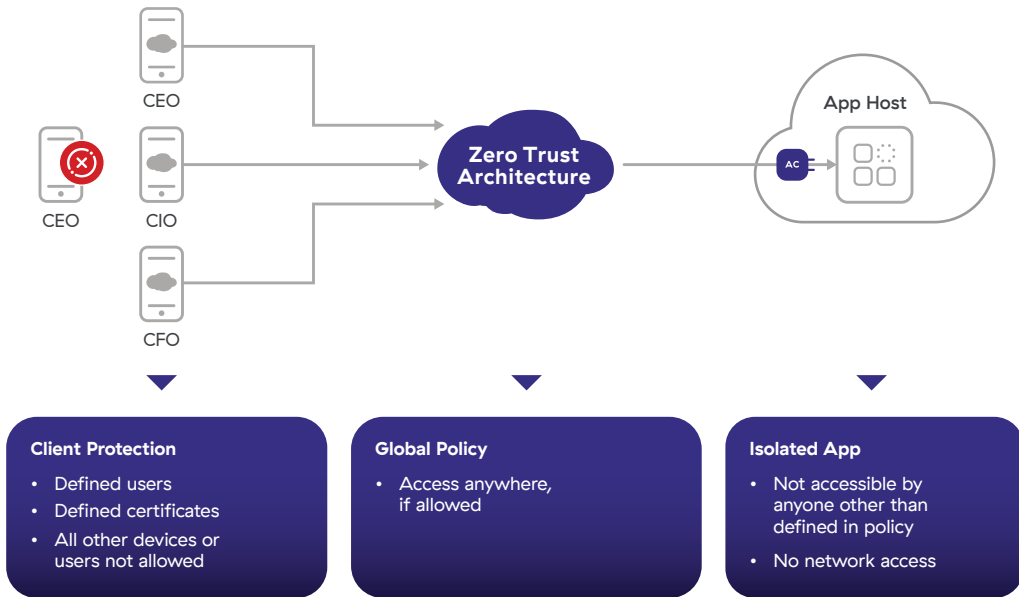


Figure 54: Zero trust protects core strategic business functions by enforcing security measures throughout the connection chain. Here, the CEO can access the application through a managed device, but not an unmanaged device.

The power here is that a simple access policy to a destination application reduces the attack surface of that application immensely. In fact, by leveraging a ZTA for specific uses, one can deploy this exact scenario over any network, regardless of how hostile that network may be.

Connecting over any network, including cellular or WiFi, means that the executives do not need to worry about the phone's underlying connection: it just works. This simplicity will drive consumption and use of various services, rather than creating technological challenges.

This network-agnostic versatility has also been used to deploy zero trust architecture within breached ecosystems, allowing business to continue while IT remediates compromised platforms.

Question 5 How is zero trust architecture deployed and adopted? What are some common obstacles?

There are several business benefits of ZTA:

Operational: The organization experiences speedy, resilient, and granular enablement of access to specific business applications.

Risk Reduction: Access is only granted to users/devices whose posture value is allowed, ensuring no access for non-compliant requests. The attack surface is greatly reduced and lateral movement is eliminated.

Agility: Securely deliver access over any network while protecting the assets and intellectual property of the business.

Simplify Mergers and Acquisitions

Mergers and acquisitions ask a lot of IT teams. In a short period, an untrusted and complex technological ecosystem must be connected to an enterprise's trusted environment. Often, the technological challenges compel both parties to blindly allow access. They enable business functionality by sacrificing security.

On that note, consider an architecture that allows granular access at the application or user level. With ZTA, vetted and verified identities are allowed access to specific resources on a per-connection basis. This approach is a godsend to an M&A team. Not only does ZTA alter the design of a merger and acquisition process, but it actually enables greater speed (approximately 50% faster) to deliver on the integration.

Question 5 How is zero trust architecture deployed and adopted? What are some common obstacles?

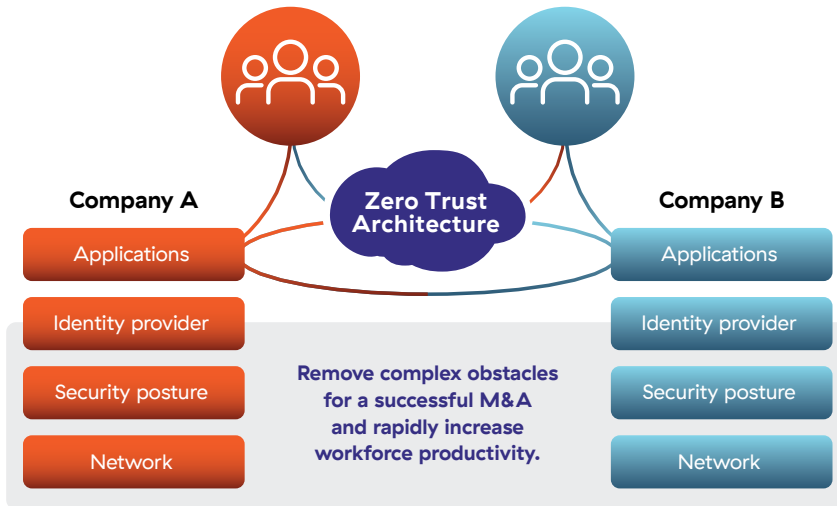


Figure 55: Zero trust removes major obstacles in M&A integration.

The complexity of merging networks is greatly reduced when users no longer authenticate to a network, but instead to specific applications. Connecting at a network level often requires resolution of duplicate IP addresses—either through re-addressing or dual-NAT (network address translation). Both are time-consuming activities. This 'lost time' is an opportunity cost that reduces the business value of the actual M&A activity.

When acquiring a new enterprise, zero trust architecture deployment and enablement are simple:

- 01** Deploy client software or set up clientless access
- 02** Integrate an identity platform into the zero trust architecture
- 03** Configure the controls of who gets access to what—this can be broad at first until more granular controls are understood
- 04** Deploy the application paths (via software-based application connectors)
- 05** Enable access

Question 5 How is zero trust architecture deployed and adopted? What are some common obstacles?

This enables authorized users to access whatever they need without ever connecting separate networks or businesses.

ZTA speeds up and secures the integration process. Symmetrically, it can also deliver the same value in the case of a disposal reducing costly Transition Service Agreements (TSAs) while providing precise cross companies connection and audit trails.

ZTA provides specific benefits to mergers and acquisitions:

Operational: There are no duplicate IP addresses, policies, hardware, configurations, or networks—they simply interconnect.

Risk Reduction: The company has full control of who gets access to what and ensures data classification and controls can be followed.

Agility: Achieve a high-speed, business-focused acquisition process, removing the overhead and challenge of consolidating separate environments.

Protect the Enterprise

Deployment, management, and control of access for a global workforce is a challenge every organization faces. Initiators, not just users, need protection when accessing internet services. This was most evident during the Solarwinds security issues of 2021. During this attack, the initial breach came via a trusted application path, the SolarWinds service. If the internet traffic generated by a server, IoT, or OT workload was not controlled, attackers were able to impact more than the SolarWinds solution.

Question 5 How is zero trust architecture deployed and adopted? What are some common obstacles?

True zero trust deployment means granular controls, even for workloads. There should never be a reason for servers to call an unsanctioned destination. To that point, ZTA deploys granular internet controls to any and all users, IoT/OT solutions, and workloads.

A ZTA deployment to protect the enterprise is simple:

- 01** Define categories of access initiators—they could be as basic as Users, Locations, Sites, etc.
- 02** Set up connections from these initiators to the zero trust solutions
- 03** For users, roll out the client software
- 04** For workloads, forward the network traffic to the zero trust platform
- 05** Build access policy, initially at a wide level and then define specifics as needed
- 06** Enable access
- 07** Observe and fine-tune access policy

There are several business benefits:

Operational: Visibility over the entirety of the enterprise landscape, access requirements, not just over users. This allows for optimization, control enhancements, and ultimately enables the best access requirements.

Risk Reduction: Deliver protected services to all initiators ensuring that “bad things” are blocked, and verified actors enjoy a secure experience.

Agility: Knowing which assets exist and what they request will allow an enterprise to build “fit for purpose” controls in the future. This enables enterprises to adapt new solutions to protect themselves “out of the box.”

Common Obstacles

Given all the benefits associated with zero trust architecture, there still exist several obstacles that can either slow down or derail the journey. Three potential obstacles that a technology leader may face are outlined below, with suggestions on how to turn these obstacles into enablers.

COMPLEXITY CAN HINDER THE JOURNEY

Issue: As a technology leader, complexity or technical debt is part of day-to-day operations. Servicing this technical debt and addressing complexity can stop an innovative transformation in its tracks. It is important to leverage complexity as a catalyst for substantial change, using the prospect of ZTA to shine a spotlight on all things legacy.

Solution: Divide and conquer by picking the areas of business where zero trust can have the maximum benefit. For example, focus on enabling access to internal applications for third-party partners. Start with moving them from full network access to zero trust access. This will yield two benefits by providing visibility into

- who is connecting and from which firm and
- where they are connecting to.

This simple exercise will deliver great access protection, as the third parties aren't on the business network. It also provides two areas of immediate improvement: the ability to apply controls to different third parties based on role, company, etc., and allowing access only to known and authorized apps.

Question 5 How is zero trust architecture deployed and adopted? What are some common obstacles?

The end result is a zero trust, hygienic foundation of access for third parties. Plus, being able to inventory users and workloads allows for iterative improvements, such as focusing on workloads the third parties are accessing and preventing access from these apps to additional services.

FRAGILITY OF THE BUSINESS

Issue: Change can often induce fear, especially in a business environment. Moreso, when talking about the IT services that underlie the fragile ecosystem of key core business functions. When handling fundamental business functions that require absolute stability, anything new must be incremental and not disruptive.

Solution: Deliver enablement. Zero trust architecture still delivers services but in a more resilient way. This factor is key to businesses adopting the architecture. Through ZTA, businesses achieve better enablement. Through proper planning, a business can facilitate its entire workforce with a new way of working in days. To demonstrate this appropriately, IT leaders need to showcase the multiple, valuable incentives of zero trust architecture. Good examples of high-level value outcomes are:

- Visibility of connections between initiators and destinations
- Intellectual property protection as well as highlighting areas where corporate secrets are vulnerable
- Reduced infrastructure costs by removing superfluous equipment, licenses, etc.
- Accelerated business deployments—not relying on hardware removes the need for lead times, deployments, etc.
- One architecture that addresses many use cases eliminates the headache of building and maintaining piecemeal solutions

Question 5 How is zero trust architecture deployed and adopted? What are some common obstacles?

LEGACY SYSTEMS HOLD BACK INNOVATION

Issue: Enterprises attempting to deliver innovative solutions are often held back by their legacy platforms. Thus, they are forced to split their technology stack over two (or more) areas, one for innovation and the other for “keeping the lights on.” This division breeds challenges with administration and requires different sets of knowledge and services to address. It also asks enterprises to work in a hybrid manner, with various solutions for each set of ecosystems it manages.

Solution: Empower innovation. A zero trust architecture allows an enterprise to execute anywhere, regardless of worker or application location. It allows any initiator to connect to a destination, regardless of the technical scenarios of either (e.g., cloud-based, on-premises, etc.). With ZTA, an enterprise only needs to consider what will be an initiator and what will be a destination. Networks no longer matter. In many cases, destination workloads will also be initiators. A true ZTA allows these types of flows to be securely built and enabled.

WITH ZTA, AN ENTERPRISE ONLY NEEDS TO CONSIDER WHAT WILL BE AN INITIATOR AND WHAT WILL BE A DESTINATION.

David Cagigal

Former CIO, State of Wisconsin

The cyber safety of our infrastructure plays a critical role in the health of our democracy

David is a seasoned executive with over 25 years of experience in information technology visioning, strategic planning, and management. He is experienced in converging business strategies with ever-changing and innovative information technologies. He also identifies and implements the appropriate change management processes and risk-mitigating strategies for each unique culture. David Cagigal was appointed Wisconsin's CIO in late 2012 after several decades in the private sector, including stints at the oil giant Amoco, appliance manufacturer Maytag, and midwestern power utility Alliant Energy. During his tenure as the CIO of Wisconsin, he oversaw the process of consolidating all the data centers into one facility that serviced 50 agencies.

I was appointed the CIO for the state of Wisconsin in November 2012. This position also allowed me to serve as Division Administrator for the Division of Enterprise Technology (DET). DET manages IT assets for the state of Wisconsin and provides several technologies to agencies including computer services, voice-data-video telecommunications, and print and mail services. While state CIO, one of my accomplishments was collaborating with more than 30 other state agency CIOs to consolidate our data centers into a single enterprise.

I also worked extensively with the Wisconsin National Guard, National Governors Association (NGA), and the Department of Homeland Security to protect 16 Critical Infrastructure/Key Resource Sectors. In 2013, following the multi-agency data center consolidations, I implemented the Zscaler Internet Access solution to improve Wisconsin's security posture. There are two things my decades of experience in the public and private sectors have taught me about successfully implementing digital transformation:

- The processes for continuously managing access must be as robust and reliable as those that grant or remove access.
- Communication is the difference between success and failure, and leaders must provide clear, consistent, and concise messaging throughout the life of a project.

CONTINUOUS ACCESS MANAGEMENT

Access management must happen across an employee's tenure, not just the endpoints. To illustrate the first point, consider the process of hiring a new employee. They are assigned a PC. This workstation is connected to the domain, configured properly for official duties, patched up, and ready to go. Likewise, the user account is properly provisioned with all the permissions necessary

for the employee to complete their work. This onboarding process is generally optimized, as IT teams have repeated the steps hundreds or thousands of times. The same is true of offboarding. The PC is removed from the domain, the user account is terminated, and all access permissions are revoked. Unfortunately, onboarding and out processing are the only two times users and devices are likely to have their permissions properly configured.

Access rights tend to become bloated the longer a person stays at an organization. As people assume new positions and roles they accrue additional access and permissions. What about the old access users no longer need? These rights are often forgotten.

Over time, this repeated process inevitably leads to an accumulation of excess access rights. My first piece of advice is to have a continuous process in place to remove unneeded access before it leads to far greater problems.

CONSISTENT, PERSISTENT MESSAGING OVER TIME

My second recommendation, maintaining consistent communication, is particularly important for leaders and drivers of change. I advise executives to communicate their message seven times in seven different ways. The messaging must be persistent and communicated through multiple venues such as PowerPoint, voicemail, text, email, etc. Throughout the transformation journey, leaders must be clear about why changes occur and keep employees updated on the current progress. Frequently repeating the transformation plan and goals will help combat several key points:

**UNFORTUNATELY,
ONBOARDING AND OUT
PROCESSING ARE THE ONLY
TWO TIMES USERS AND
DEVICES ARE LIKELY TO
HAVE THEIR PERMISSIONS
PROPERLY CONFIGURED.**

- Confusion over key terms such as “zero trust” and ambiguity over expected outcomes
- Message distortion that naturally occurs as directives pass through multiple layers of management
- Loss of focus that occurs as people leave the project and new members come aboard

For example, change leadership often starts at the governor's or CEO's office. The executive issues a mandate for change and sets goals for the organization. The order could be as brief as “you will adopt zero trust principles,” or “you will adopt a zero trust philosophy in protecting our assets.” Yet even simple messages can become mangled when projects drag on. Without continually specifying what zero trust ultimately looks like, or how the framework will be applied to business-critical resources, the end result could be disastrous. This is especially true when messaging is passed throughout the organization in a piecemeal fashion.

Likewise, many workplaces are organized in a hierarchy. There may be multiple layers of management between those directing changes and those performing the work on the ground. Messaging must remain consistent as it passes through each layer of management. This can be achieved by forming an oversight committee that regularly meets to ensure all stakeholders are on the same page.

While CIO for Wisconsin, I met every Monday with the deputies of major cabinets to reiterate the message and the mission. For four solid years, each deputy returned to their home offices bearing an identical message about what we were doing, how, and why. Keeping everyone informed of the plan and working toward the same goal was critical for our success.

STAY FOCUSED FOR SUCCESS

Organizational change happens at the employee level, but it requires strong change leaders to guide the effort. Changing technological processes and practices in a large organization is a daunting task, and requires a multitude of skills to accomplish. However, in my experience, keeping a close eye on access permissions and providing consistent messaging are two key ingredients to achieving success.

QUESTION SIX

**What are the
non-technology
considerations
for successful
adoption of a zero
trust architecture?**

Question 6 What are the non-technology considerations for successful adoption of a zero trust architecture?

Digital transformation occurs not only in technology but also in a number of non-technology areas. These include changes in culture and mindset, organizational structure, processes, and skill sets. While often not prioritized while undergoing secure digital transformation, these areas all play a critical role in its success.

If done correctly, non-technology transformations can have lasting positive effects on how the organization functions. They may improve an organization's abilities to cater to business requirements, become agile, and break down silos. However, these changes do not happen overnight. They rely on the fortitude of dedicated CXOs exercising effective top-down leadership.

Culture and Mindset

Culture and mindset are areas that are hard to define, measure, and influence, but are crucial to the adoption of zero trust technology. Persuading the business culture and mindset to embrace zero trust greatly affects the success of its deployment and operation. Organizations trapped in a legacy mindset may find pockets of resistance to change. Within every IT department, there are people who love their network, have faith in their firewalls, and believe there's nothing wrong with VPNs.

Companies selling traditional solutions have no interest in disrupting the market because they can simply create another point product to address the next problem. Another product equals another sale, including fees for upgrades and maintenance—and the cycle is perpetuated.

Question 6 What are the non-technology considerations for successful adoption of a zero trust architecture?

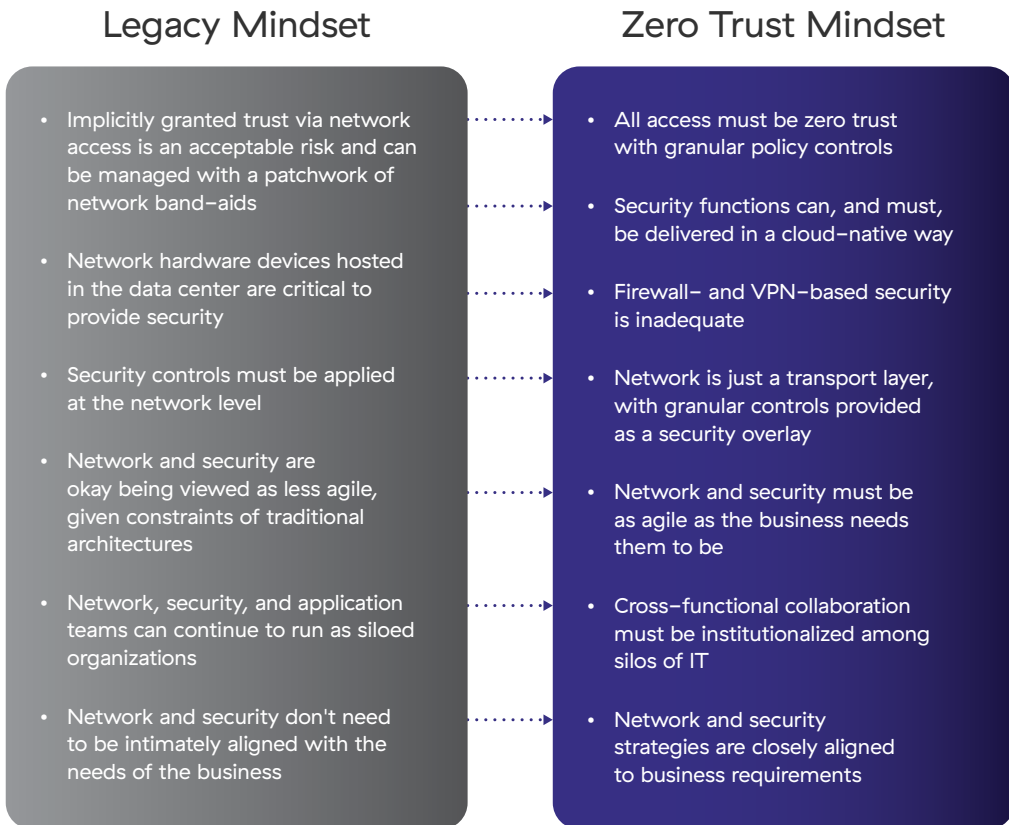


Figure 56: Zero trust transformation requires a rethinking of long-held beliefs.

Many companies have invested so much in point security and networking products that it's not easy for them to try something new, even if the benefits are measurable and significant. Zero trust represents a departure from long-standing norms, and a journey into unfamiliar territory.

When trying to change culture and mindset, it can be useful to use the analogy of embracing cloud-hosted applications. This usually begins with a lift-and-shift approach (moving data center apps into the public cloud), and ultimately ends with building cloud-native applications and adopting SaaS. This process was daunting at first, but it is now mainstream.

Question 6 What are the non-technology considerations for successful adoption of a zero trust architecture?

A similar shift in mindset is needed when transforming network and security. That which can be implemented in the cloud must be, for both operational and scale benefits. That which can remove the inherent security risks in legacy architectures, a pillar of zero trust, must be embraced as well.

While changing business culture and mindset is difficult, CXOs are leaders by nature and have the benefit of implementing a top-down approach. For example, changing KPIs and incentive structures may nudge their teams toward accepting a new way of thinking.

Organizational Structure

Traditionally, organizational structures within IT tend to be siloed in nature and aligned along functional responsibilities (e.g., network, security, and application). Daily operations among these groups are not particularly aligned:

- The network team's remit is to provide fast and reliable connectivity to resources.
- The security team's function is to provide security and controlled access to the same resources.
- The application team's goal is to ensure employees' application usage is optimal for the business.

While each of these goals sometimes seems at odds with one other, the ultimate goal of all of these parties is the same:

Question 6 What are the non–technology considerations for successful adoption of a zero trust architecture?

ensuring employees have fast, reliable, and secure use of business resources. Zero trust architecture is a key enabler of this unified goal.

Zero trust optimizes the efforts of various IT teams by allowing them to work together. A few examples of cross–functional collaboration include zero trust connectivity and application access policies:

- While security often takes the lead in operating ZTA, network and security must work together on the architecture. Zero trust control is provided via a security cloud. Therefore, network teams working closely with security are critical to ensure the connectivity of users, branches, things, or workloads to the service edge.
- Additionally, the ownership of the hardware–based security stack that typically fell to the network infrastructure team now becomes a joint effort when migrated into a cloud–based ZTA. Configuration of the service edge now falls to both network and security.
- User access policy is set from a user–to–app perspective and is no longer at the network level. This means application teams working closely with security are responsible for setting the granular access policy that ZTA allows.

ZERO TRUST OPTIMIZES THE EFFORTS OF VARIOUS IT TEAMS BY ALLOWING THEM TO WORK TOGETHER.

CXOs can consider creating zero trust team structures (that have representatives across teams), and realigned KPIs or incentive structures. All of these techniques can encourage cross–functional collaboration.

In addition, their personal leadership will be essential to overcome the challenges of a siloed legacy.

Question 6 What are the non-technology considerations for successful adoption of a zero trust architecture?

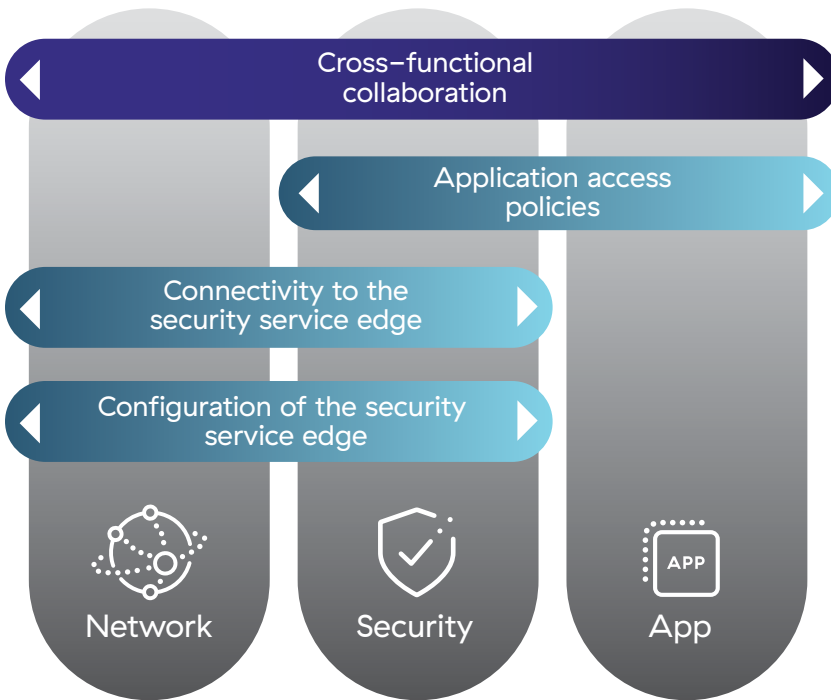


Figure 57: Zero trust transformation requires cross-functional collaboration between traditionally siloed disciplines.

Processes

Moving to zero trust architecture can greatly simplify cumbersome manual processes. As with any transformation, adopting zero trust technology requires processes to be rethought to ensure both the deployment and operationalization of zero trust technology take advantage of the desired security and network benefits.

Question 6 What are the non-technology considerations for successful adoption of a zero trust architecture?

Under a ZTA, there are far fewer disparate systems to manage. This leads to reduced complexity, including the following:

- Being able to segment apps by simple identity-based rules, not by manually intensive network-based configurations
- Leveraging a cloud-based intelligence engine to simplify updating threat intelligence or data classification rules
- Visibility into app access and usage leading to insights that can improve workflows and processes

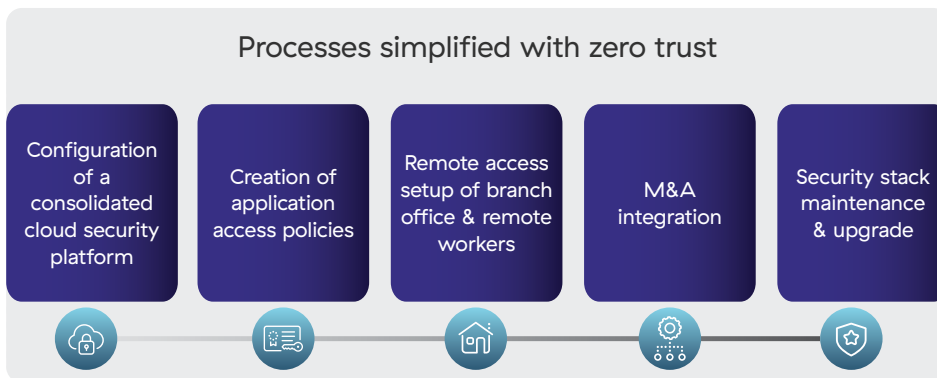


Figure 58: Zero trust simplifies several critical business processes.

There are five areas where a ZTA can simplify existing processes:

01 Configuration of a consolidated cloud security platform

ZTA removes much of the configuration required by network-level controls. Network layer segmentation rules, done through VLANs and ACLs, are now done at the user-to-app level through logical policies (only Department X can access Application Y). Other configurations are greatly simplified. For example, DLP, firewalls, SWGs, etc., performed on hardware-

Question 6 What are the non-technology considerations for successful adoption of a zero trust architecture?

based appliances procured from a variety of vendors (each with its own UI), are now centrally consolidated on a cloud security platform. A single UI from a single vendor yields significant advantages by removing the many processes required to maintain individual security point solutions.

02 Creation of application access policies

Zero trust eliminates many network layer processes while introducing the initial setting and upkeep of granular application segmentation policies. These policies govern which users can access specific resources. Shifting from network level to app-based requires some investigative work. Processes must be initiated to discover who needs to connect to what so that proper policies can be set. There will also need to be procedures to change these policies if they are too stringent or lenient, or when user requests come in.

Zero trust solutions simplify this process by revealing application flows and making policy recommendations. This process extends to understanding identity (as defined by the IdP), user context, and user risk. These factors will influence the type of access granted to a connection (e.g., allow, isolate, warn and allow, etc.).

03 Remote access setup of branch office and remote workers

Processing the configuration of a branch or remote worker also changes in a zero trust architecture. A single agent sitting on the end user's device facilitates all secure connectivity (through the zero trust cloud). Any network-layer configuration, other than basic routing, goes away, as does the need for branch office firewalls or other security stacks. Under certain

Question 6 What are the non-technology considerations for successful adoption of a zero trust architecture?

configurations, there may be a need to configure a GRE or IPSec tunnel to forward traffic to the zero trust edge, but all other functions are handled by the security cloud.

Setting up remote workers is also greatly simplified. The same always-on agent secures access for remote and mobile users (based on user-to-app policy). The agent intelligently forwards internal and external traffic through the appropriate controls. This eliminates the complex processes needed to deploy, maintain, and write configurations for VPNs.

O4 M&A integration

The IT process that accompanies a merger and acquisition (or divestiture) can be daunting, given the complexities of integrating disparate network stacks, with its unique addressing and laden with technical debt. A ZTA greatly simplifies M&A integration, since the network is abstracted— all integration happens at the application level. This allows users to access applications without ever having to integrate at the network layer.

O5 Security stack maintenance and upgrade

Processes to maintain and upgrade a hardware-based security stack can be cumbersome and expensive, especially given recent supply chain issues. A cloud-based zero trust provider can replicate the same security stack functions, infrastructure maintenance, and upgrades. Just the configuration and underlying network connectivity to the security cloud is required by the organization.

Skill Sets

While moving to zero trust architecture can greatly simplify the many manual tasks that IT personnel have to manage, it does require that such personnel have a different skill set from traditional network and security engineers, architects, etc. Essentially, network and security personnel are being asked to convert to a zero trust way of thinking, which will upend many of the skills they may have spent years or decades mastering.

The number of required vendor-specific skills diminishes as tasks are consolidated on a zero trust platform. Network and security personnel will need to refocus their training on the operational skills needed for a smaller set of ecosystem vendors.



As a result, some of the certifications championed by hardware-based vendors become less meaningful. In their place, professionals can pursue zero trust certifications offered by industry organizations, like the Cloud Security Alliance (CSA), or security vendors, like [Zscaler's Zero Trust Certified Architect program](#).

Question 6 What are the non-technology considerations for successful adoption of a zero trust architecture?

Sanjit Ganguli

Zero trust architect

sganguli@gmail.com +12 34 56789012 linkedin.com/sganguli



“Sanjit was key in developing our industry-first zero trust architecture. Without Sanjit, we would have been left vulnerable to cyber threats.”

-CISO, ALPCORP

SKILLS:

- Understands zero trust concepts and how they apply to enterprise security architectures
- Ability to customize zero trust controls that apply to secure design and architecture methodologies
- Ability to write and maintain technical documentation, including reference architectures and implementation plans for zero trust transformation
- Understands security requirements, security assessments, and security recommendations using industry standards as reference models, including an understanding of NIST 800-207
- Ability to work cross-silo, across network, security, and application teams, meaning having a focus area with functional knowledge of adjoining areas

EXPERIENCE:

ALPCORP | 2018-2022
Zero trust architect

- Delivered industry-leading zero trust architecture
- Oversaw seamless security during the merger of multiple companies
- Oversaw the digital transformation of remote workers during Covid-19

Figure 59: Sample CV of an ideal hire to architect a move to zero trust.

“ For IT, [zero trust means] more holistic insights and scope on the health of accessing data and information, spread over many fewer services. [There is now] less complexity, and faster ability to help the business and business users. Post-migration, there will be less services, processes, and complexity involved in the IT portfolio.”

Craig Clay
Former Lead Connectivity Architect

Larry Biagini

Former CIO/CTO, GE

Zero trust is a journey and not a single project

Larry Biagini is a retired CTO and CIO from GE who has made instituting zero trust practices at global enterprises his mission. Larry's focus during his executive career was contemporizing infrastructure, employee services, and deploying cloud technology to enable the secure usage of those services by employees, customers, and partners. He held various high-level positions in information technology, often bearing responsibility for all aspects of risk, governance, and security. Larry's career has spanned 35 years in technology, covering manufacturing, logistics, and financial systems. Industrial verticals include healthcare, media, aviation, and energy.

A successful digital transformation cannot be achieved while using antiquated networking concepts, tiptoeing toward change, and avoiding risk. Thinking about enterprise security in terms of hub-and-spoke architecture and VPNs is taking a long journey down a dead-end path. There is only one network, the internet, and it is beyond the control of any business organization. In fact, maintaining secure access to cloud services via the internet is key to many organizations' survival. Legacy networks and the technologies that support them are simply incapable of providing the level of secure cloud access modern businesses need.

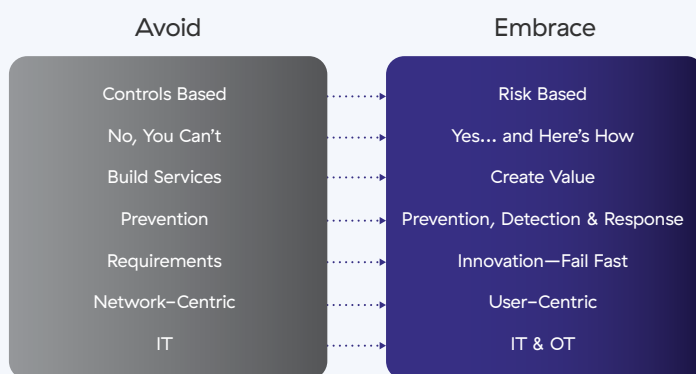
Consider the stark differences between yesterday's enterprise control framework and one facilitating secure cloud/mobile transactions today:

Control Framework	Data Center Model	Cloud Model
Users on company network	Yes	No
Device under IT control	Yes	No
Corporate network controlled by IT	Yes	No
Apps in DC	Yes	No
Data in DC	Yes	No

The differences between these two models should be evident to IT professionals, yet explaining them to other executives and the board can be tricky. Unfortunately, many security leaders are overly technical when having conversations on why their organization must digitally transform. They rely on doom-and-gloom scenarios and hypothetical attack costs to persuade their audience. Instead, IT

leaders should ensure their message focuses on adding business value and highlights the immediate benefits of doing things a new way.

Here are some key ways IT leaders can reframe conversations on digital transformation to achieve better results:



Successful CIOs, CTOs, and CISOs of tomorrow will approach technology problems much differently than those who currently think in terms of traditional networks. **Specifically, forward-looking CIOs/CTOs will**

- focus on growth and move fast—speed is the new currency
- move from being an IT shop to acting as a digital enabler
- be honest with the board about technology debt
- address the legacy environment head-on
- embrace the cloud, but thoughtfully, for relevant applications
- realize the internet is the new corporate network
- transform traditional hub-and-spoke networks to a direct-to-cloud architecture

Likewise, successful CISOs will

- stop talking to the board in terms of security, but instead focus on risk
- create a risk assessment and risk appetite that provides the business a means to make decisions
- separate critical resources from the consumers of those assets (don't put users and servers on the same network)
- get identity right — invest in identity and access management
- realize securing the traditional network is no longer relevant and focus on providing trusted users access to authorized applications, irrespective of the network

Business and technology are not slowing down. Today's executives face a simple choice: climb aboard the train to a cloud-based, zero trust world or be crushed by it. Technology leaders should be thinking, speaking, and acting in terms of business risk, not security. No combination of products can address the fundamental vulnerabilities endemic to the traditional network. Adding more security layers on top of an insecure foundation is pointless—those scrambling to protect everything wind up protecting nothing.

It is time to retire the network in favor of app-based and identity-based connectivity. To accomplish this, an organization must know the identity of people, devices, machines, and APIs. Once an organization can securely connect a trusted user to an authorized resource, the network layer (and all of its vulnerabilities) becomes largely irrelevant.

TODAY'S EXECUTIVES FACE A SIMPLE CHOICE: CLIMB ABOARD THE TRAIN TO A CLOUD-BASED, ZERO TRUST WORLD OR BE CRUSHED BY IT.

What do I look for (and not look for) in a zero trust solution?

Question 7 What do I look for (and not look for) in a zero trust solution?

Zero trust architecture is part of a transformation journey that involves both technology and non-technology factors. The technology aspect of the zero trust journey requires the careful selection of a solution that accomplishes the goals of network and security transformation.

When selecting a solution to embrace a zero trust architecture, there are several pitfalls to avoid.

Pitfalls to avoid when choosing a zero trust solution



Figure 60: Avoid these seven pitfalls when selecting a zero trust solution.

Instead, organizations should focus on vendors who excel in seven key areas of successful digital transformation. Each of these seven factors is described in its own section below.

Fully Address the Specific Needs of the Enterprise

A successful zero trust solution scales for business needs today and, more importantly, for its future goals. Scalability is not simply the mechanism to build out, but to address enterprise needs without sacrificing the function, stability, and protection of the business. The zero trust solution should

- provide evidence and transparency of its global cloud deployment
- have documented and validated SLAs for its zero trust services
- have a history of deploying several customer organizations of relevant size and complexity
- deliver all critical functions to all sites without backhauling or hairpinning traffic
- provide inline and out-of-band protection
- offer solutions designed for operational and functional resilience

Core Zero Trust Tenants

Protecting an enterprise and its users must be approached in a way that delivers access on a need-to-know, least-privileged basis. It is imperative to separate the jargon and marketing hype of “zero trust” from the core functionality that defines the term. To this end, a true zero trust foundation should

- protect all enterprise services by validating the identity of the entities before allowing conditional access; everything else must be blocked

Question 7 What do I look for (and not look for) in a zero trust solution?

- check various contexts such as device posture, user risk, etc.
- connect users to specific applications, not the network
- be network-agnostic and eliminate routable networks
- eliminate the attack surface for internal application

Cloud-Native Infrastructure

Recent industry reports indicate that 85% of cyberattacks come through encrypted channels. This makes the ability to inspect encrypted traffic critical for organizations. Inspecting this traffic at scale, with minimal latency, requires leveraging the power of the cloud. Only zero trust solutions with properly optimized cloud-native architecture can deliver

- inspection of all traffic at production scale with minimal impact on performance, based on a proxy architecture
- a single memory scan architecture for decryption at scale
- the experience to guide customers through the steps and challenges of performing SSL/TLS inspection

Flexible, Diverse, and Scalable

Flexible, diverse, and scalable zero trust deployment options provide organizations all the benefits of zero trust, regardless of geographic location. In other words, security must extend to every user, app, and resource no matter where they are. Look for vendors offering solutions that

- can be managed from a central control plane with corporate policies applied evenly and dynamically across all users/devices or IoT/OT communications

Question 7 What do I look for (and not look for) in a zero trust solution?

- extend the same protections to managed and unmanaged/ BYOD devices, facilitating third-party access for contractors and remote employees without increasing the attack surface
- provide workload-to-workload security that affords DevOps and CloudOps engineers the same zero trust protections for their applications when accessing other workloads, other clouds, or the internet

Optimal End-User Experience

The success of any transformation, be it digital, network, or security, is driven by the end-user experience. The ultimate goal of any zero trust project is to improve end-user experience while reducing threat exposure and increasing security. Therefore, look for

- a zero trust solution that optimizes the user experience and uses a proactive approach to measure and diagnose problems
- a zero trust solution that collects metrics from applications, endpoints, and network layers to find anomalies and provide root cause analysis
- A zero trust vendor who provides minimal hops between their cloud and popular destinations like Microsoft 365 to minimize latency

Strong Ecosystem Integrations

Vendors that cobble together a zero trust solution portfolio through acquisitions tend to fall behind in product innovation and often lack interoperability with third parties. Look for zero trust vendors that integrate with leading ecosystem players (like CSPs, SD-WAN, IAM, SOAR/ SIEM, EDR, etc.), future-proof their technology, and reduce technical debt. Zero trust vendors who offer rich, API-based, third-party integrations provide operational efficiencies by allowing organizations to orchestrate best-of-breed solutions and avoid vendor lock-in.

Easy to Pilot and Deploy

Performing a pilot will determine whether a zero trust solution is easy to deploy, performs well in the production environment, and achieves business objectives. Look for

- zero trust vendors that can demonstrate a low TCO, a single unified agent, access to a global set of service edges, and a centralized and easy-to-use UI, indicating that maintaining the solution will be straightforward and cost-efficient
- zero trust architecture and design that makes it easy to add on features with minimal additional deployment requirements (like adding more agents or VMs), allowing organizations to take a phased approach to zero trust knowing that moving between phases will not require heavy lifts
- zero trust vendors with a positive track record of being customer-focused, and demonstrate this quality during the pilot

Uninterrupted Business Continuity

One reservation often voiced about cloud migration is concern about resiliency of the cloud. Businesses may be reluctant to trust their data to third parties, and worried that events like cloud outages will disrupt their operations. When selecting a zero trust cloud provider, it is important to consider who ultimately controls the infrastructure, their trustworthiness, and their record for providing consistent service.

Additionally, catastrophic natural events (hurricanes, earthquakes, etc.) or human-driven disruptions (wars, insurrections, espionage, etc.) can threaten regional cloud connectivity and availability. For this reason, it is highly recommended that organizations adopting cloud security ask providers about the resiliency and distributed nature of their architecture. A service cannot guarantee secure access to business resources if it does not have a plan to limit the impact of outages.

Seven Answers Every CXO Should Know About Zero Trust

In summary, let's take a look at the seven questions every CXO needs to ask about zero trust and the key points in answering each of them.

QUESTION 1

What is zero trust and why is it critical for secure digital transformation?

Cybersecurity must evolve to accommodate new technology and an increasingly distributed, remote, and mobile workforce. Securing employees using any device, working from anywhere, and accessing resources in data centers or the cloud requires a modern security framework. Traditional network topologies and concepts do not work in a world where countless external actors, resources, and unmanaged devices regularly interact with business infrastructure.

Modern security requires removing the network from view and brokering a validated and enforced connection between participants—this is the basis of zero trust. When transactions only occur on a trusted, per-connection basis, the attack surface is minimized and potential damage from compromise is extremely limited. Additionally, using a cloud-based ZTA improves connection speeds, provides better visibility into operations, and saves businesses revenue by replacing outdated assets and processes.

QUESTION 2 What are the main use cases for zero trust?

Zero trust is a security architecture that is designed to protect businesses from cyber risks, improve productivity and agility, and minimize the cost and complexity of various security products. It has three main use cases: secure work from anywhere, WAN transformation, and secure cloud migration.

For secure work from anywhere, zero trust architecture provides secure and fast access to applications from any location and device, protecting employees, contractors, customers, and suppliers. It protects against cyber threats and data loss can replace traditional VPNs, and provide secure access for managed and unmanaged devices.

For WAN transformation, ZTA converts unsecured, routable, hub-and-spoke networks to true zero trust connectivity based on network overlays, while also improving the user experience by eliminating latency-inducing hairpinning. This WAN transformation works across different offices and branches, using connectivity mechanisms like zero trust SD-WAN.

For secure cloud migration, zero trust architecture ensures that workloads securely communicate with other workloads and the internet, and ensures that those workloads are securely entitled and configured. A holistic ZTA environment can provide strong posture control, secure workload configuration, and safe workload communications.

QUESTION 3 **What are the business benefits of moving to zero trust?**

There are several business benefits to adopting zero trust architecture (ZTA), including technology cost savings, reduced risk, operational savings, and improved agility and productivity.

- Technology cost savings can be achieved by consolidating vendor subscriptions and reducing the need for hardware infrastructure and bandwidth costs.
- Risk reduction can be achieved by protecting against data breaches and insider threats, as well as improving compliance with regulatory requirements.
- Operational savings can be achieved by streamlining processes, improving productivity, and reducing maintenance and support costs.
- Improved agility and productivity can be achieved by enabling remote work, streamlined M&A integration, and allowing for innovative solutions. This includes improved end-user experiences by not requiring users to log into VPNs.

QUESTION 4

How does zero trust drive success for organizations?

Five case studies from various organizations highlighted how each used zero trust to drive success.

- Embracing a zero trust cloud architecture let Coca-Cola Consolidated securely support their remote workforce without suffering productivity issues or exposing themselves to massive risks.
- Sandvik found that ZTA worked seamlessly with their WFA policy, providing reliable and secure connections to their users and contractors around the globe.
- Carlsberg Group achieved granular access control that improved visibility, enhancing several aspects of Carlsberg's business operations.
- Cache Creek Casino Resort found that, within three months, their zero trust provider inspected 1.7 TB of data, prevented 345,000 policy violations, and blocked 629 threats. The ability to easily work from anywhere has also improved the work environment for employees and allowed the company to broaden recruitment practices.
- A US Federal civilian agency was able to retire a considerable amount of its legacy infrastructure by transitioning to a ZTA. Their improved connectivity in urban and rural areas has enhanced job performance and alleviated user frustration.

QUESTION 5 **How is zero trust architecture deployed and adopted? What are some common obstacles?**

Implementing a zero trust architecture is a journey, so it is important to break the journey into manageable phases in order to show incremental business value. The journey can be divided into four phases:

- Empowering and securing the workforce — protect strategic core business functions by allowing only verified entities access to verified and allowed destinations
- Protecting data in the cloud — protect data at rest by using ZTA to monitor and control access to data repositories
- Enabling customers, contractors and suppliers — secure remote access of non-employees (not on managed devices) by redirecting this traffic through the zero trust architecture
- Modernizing IoT/OT security — protect critical infrastructure by isolating and protecting sensitive systems from external threats

QUESTION 6 **What are the non-technology considerations for the successful adoption of a zero trust architecture?**

Adopting zero trust architecture requires a transformation in both technology and non-technology areas:

- Culture, mindset, and communications
- Organizational structure
- Processes
- Skill sets

These changes can be difficult to implement, particularly due to hardened cultural and mindset issues that may exist within the organization.

To successfully shift towards a zero trust culture and mindset, CXO leaders should adopt a top-down approach and consider changing KPIs and incentive structures. In addition, organizational structure and processes must be aligned with the zero trust philosophy, and the necessary skills must be developed within the organization. Finally, it is important to establish strong communication and collaboration among various teams and functions within the organization to ensure a successful transition to zero trust.

QUESTION 7 **What do I look for (and not look for) in a zero trust solution?**

A zero trust solution is an important part of a network and security transformation journey. When selecting a zero trust solution, it is important to consider the vendor's ability to address the specific needs of the enterprise, provide a true zero trust foundation, have a cloud-native infrastructure, offer flexible, diverse, and scalable deployment options, and optimize the end-user experience. It is also important to ensure the vendor has a global and diverse cloud deployment, documented and validated SLAs for their zero trust services, has deployed for customers of a similar size and complexity as the enterprise, and is designed for operational and functional resilience.

Communicating the value of zero trust to the board of directors

The benefits of secure digital transformation (and zero trust) resonate with a board of directors, but only if communicated correctly. Technology CXOs are in a unique position to educate board members on cybersecurity-related business risks and recommend solutions. Effective cybersecurity messaging must take into account the structure of the board, and frame conversations in ways that are relevant to member's individual roles.

To assist in oversight, boards establish standing committees, several of which have risk management responsibilities, which includes cybersecurity. Types and roles of committees vary across organizations. Generally, there are a few specific committees where technology CXOs can discuss zero trust and gain further organizational support:

- **Audit Committee** — A majority of boards have some form of an Audit Committee oversight group. This committee has general oversight on organizational reporting, controls, and compliance. CXOs should discuss how zero trust practices provide better cyber risk management, data protection, and governance over cyber risks and controls with this group. Be sure to cite specific financial benefits when explaining initiatives.
- **Risk Committee** — More boards are now standing up a separate Risk Committee or having it serve as a sub-group to the Audit Committee. This committee, with general oversight on enterprise risk management and policies, is an important group to meet regularly as a technology CXO.

Appendix 1 How do I communicate the value of zero trust to my board of directors?

Discussions should focus on how leveraging zero trust decreases risk exposure and attack vulnerability, reducing the impact of an incident. Also emphasize that zero trust offers superior visibility of enterprise-wide cyber risk tolerances and controls.

- **General board members and other committees** — There are several benefits to zero trust that can be effectively cited in general board-level or committee-based conversations. It is important to frame these conversations in terms of financial, operational, and reputational impact to the company. For example, zero trust reduces the security spend on assets, streamlines remediation processes, and increases oversight over the environment. Board members concerned with regulatory fines may be particularly interested in the data loss prevention (DLP) and encrypted traffic inspection capabilities of zero trust.

It is important for board members to understand their organization's cybersecurity strategy. They need to be able to answer the following questions:

- What are the technology and organizational costs of its current cyber risk solution?
- What is the risk of exposure for the organization?
- Is data streamed through a centralized point of governance and oversight or are current processes and technologies spreading data and users activity out across disparate systems?
- Is there a culture of cyber awareness and transparency across the organization?

When answering these questions for the board, emphasize the ability of ZTA to mitigate these cyber risks, minimize cyber incidents,

and aid in governance and oversight. Highlight the inability of traditional architectures to do the same. Zero trust mitigates the security gap created between legacy processes and technologies and the adoption of new technologies.

Ask board members to recommend that their executive leaders conduct and share a complete assessment of known cyber risk gaps. This assessment should model the spread of risk, and show worst-case scenarios with the probability of occurrence. This exercise will be key in crafting a risk-cost-benefit analysis.

When completing these assessments, factor in the attack surface minimization and lateral movement prevention that zero trust architectures offer. Present this zero trust cyber risk analysis data in terms of financial, economic, customer, and operational impact terminology, not just in technical terms (see discussion in Question 3).

Also, communicate what assets and processes are of highest value and highest risk to focus the whole organization on addressing priority cybersecurity issues. By framing messaging in terms of organizational risk, financial exposure, and impact on employees and customers, CXOs empower the board to make sound security decisions.

Evaluating the resiliency of the Zscaler Zero Trust Exchange

Questions about resiliency are commonly raised when shifting to a cloud-hosted zero trust architecture. This is true of any cloud migration, where control of the infrastructure is passed to a third party, in this case Zscaler. When considering resiliency, it is important to look at four specific areas of the cloud infrastructure: capacity, availability, performance, and security.

When evaluating Zscaler's Zero Trust Exchange, consider:

Capacity of the Zscaler cloud:

- Globally distributed data centers, with ample processing capacity at each
- Redundant data center network that provides high bandwidth

Availability of the Zscaler cloud:

- Automatic failover from one geographically proximal data to another proximal data center
- Ability to control routing in the event of network routing issues

Performance of the Zscaler cloud:

- Internet exchange peering
- Carrier-neutral data centers

Appendix 2 How do I evaluate the resiliency of the Zscaler Zero Trust Exchange?

- Hardware suitable for low latency SSL/TLS decryption

Security of the Zscaler cloud:

- Internal zero trust access, multi-factor authentication, including physical tokens and ephemeral keys

Beyond architectural design that provides resiliency, equally resilient operational processes must also be present. Zscaler has the experience of operating an inline security cloud—the world’s largest—for over 12 years of service and counting. This includes:

- specialized testing and simulations for agility and reliability
- limited risk exposure based on purpose deployment infrastructure
- rolling deployments with strict backward/forward compatibility
- dedicated Trust Portal for customer communications
- well-defined customer escalation processes
- proactive detection and auto-remediation with 24/7 NOC/SOC
- predictive monitoring with ML and external probing

Finally, the cloud must be able to handle all failure scenarios including data center outages / connectivity issues, hot clusters / connectivity issues, and black swan catastrophic failures. In each case, the Zero Trust Exchange provides dynamic / automatic failover and disaster recovery mechanisms to minimize the impact of these rare events.

For More Information

Congratulations on becoming well-armed with the knowledge necessary to drive a successful digital transformation. The need, benefits, and process for migrating to the cloud and implementing zero trust security are well established. The obstacles, challenges, and objections for doing so are known and navigable. All that remains is to put this newfound knowledge into action.

The following resources are available for additional assistance:



CXO REvolutionaries

Created for CXOs by CXOs. Learn from IT leaders bringing a new wave of cloud- and mobile-first technology to major enterprises globally. The website publishes the latest insights by digital transformation pioneers and thought leaders.



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.



The 7 Pitfalls to Avoid When Selecting an SSE Solution eBook

Tips for building SSE on a foundation of zero trust.



Zero Trust Webinars



Run an Attack Surface Report for Your Domain