zscaler™

EBOOK

The Three Keys To Transformation Through Zero Trust: **Platform, People, and Process**

The path to zero trust

Digital transformation has fundamentally changed the way modern businesses operate. Your **employees are on the internet now more than they are on the corporate network,** accessing applications and data from everywhere. Sensitive business data has become more distributed, residing outside the corporate perimeter in SaaS applications, such as Microsoft 365, and private applications in AWS, Azure, and Google Cloud Platform.

The process of digital transformation improves business agility and information flow, but dramatically expands the attack surface and exposes your business to new threats. Traditional security architectures, which focused on protecting the network, are no longer effective in this new reality. Protecting your business and retaining the benefits of **digital transformation requires migrating to a zero trust security model delivered through the cloud,** closer to where your users and business assets are now centered.

What is zero trust anyway?

The concept of zero trust has been around for more than a decade, yet there's been a lot of confusion about what the term actually means. It is not simply a single technology.

Zero trust is a holistic approach to securing modern organizations, based on least-privileged access and the principle that **no user or application should be inherently trusted.** It begins with the assumption that everything is hostile, and **only establishes trust based upon the user identity and context,** with policy serving as the gatekeeper every step of the way.

Zero trust in practice

Zero trust tackles today's most difficult challenges encompassing security, networking, and enabling the modern workplace:

SECURITY

Prevent cyberthreats:

Zero trust delivers cyberthreat protection—not just for users, but for cloud workloads, for servers, as well as for SaaS applications.

Prevent data loss:

Zero trust provides a holistic approach to ensuring data can't be leaked or lost, either accidentally or intentionally by users, or from cloud workloads.

NETWORKING

Simplify user and branch connectivity:

Zero trust enables organizations to transform legacy hub-and-spoke networks, enabling branch offices and remote users to securely connect to any destination directly over the internet, regardless of where the user connects.

Secure cloud connectivity:

Rather than extending traditional site-to-site VPNs to the cloud, which carries the risk of lateral movement, zero trust enables workloads to securely connect to other workloads.

ENABLING THE MODERN WORKPLACE

Secure work-from-anywhere:

A true zero trust solution should enable your employees to safely and seamlessly work from anywhere, without having to worry about the network or whether or not they need to turn on a VPN.

Optimize user experiences:

By ensuring you understand the experience of every employee for every application, zero trust enables organizations to consistently deliver a great user experience.

Planning for zero trust success

As the internet becomes your new corporate network, zero trust provides the path to **fast, seamless, and secure access** across your entire business ecosystem.

But implementing a zero trust security model isn't just a function of IT—it impacts all areas of your business, and beyond the traditional confines of your organization. Successfully implementing zero trust requires a detailed strategy that addresses challenges and opportunities across **people, processes, and technology platforms.** →
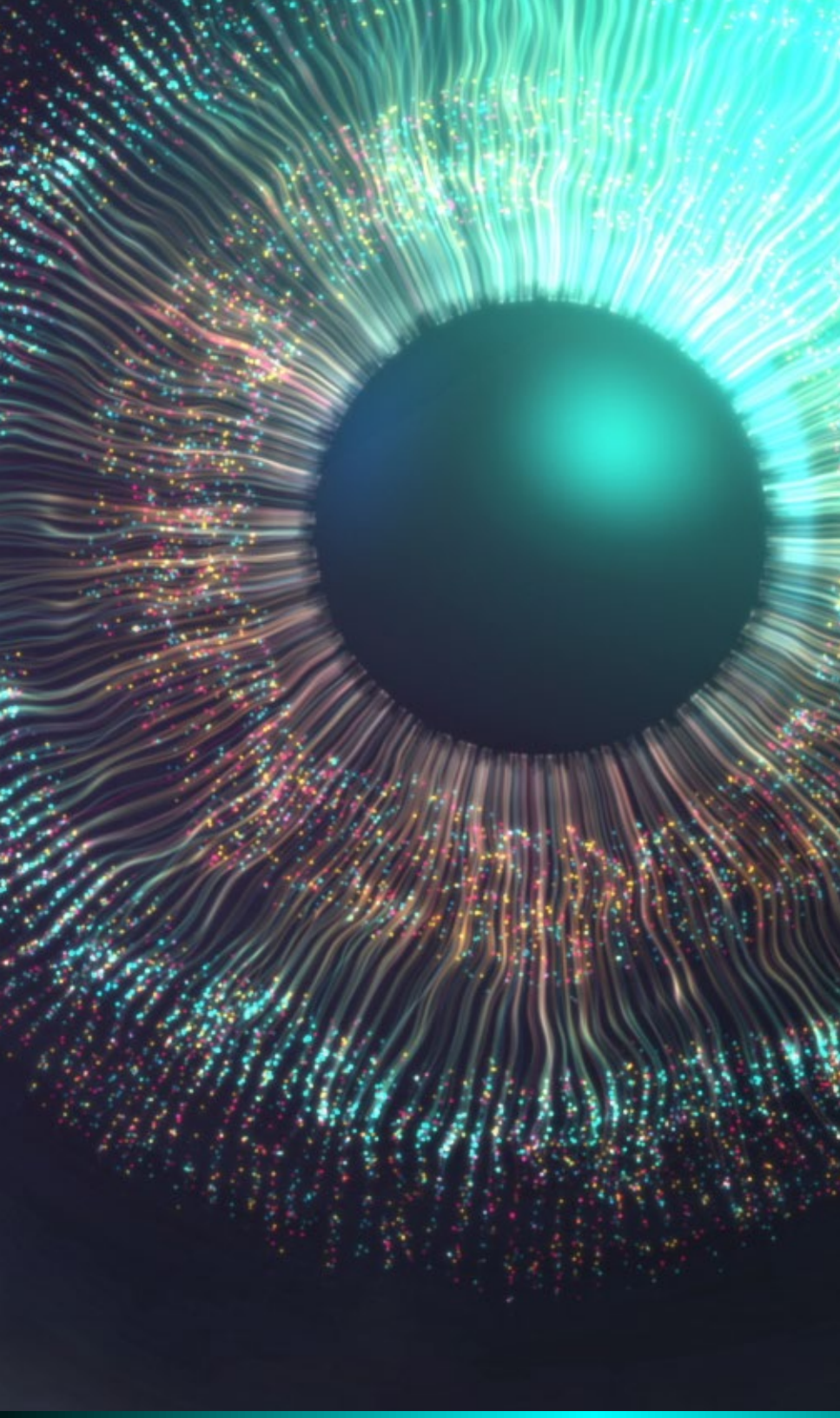
Platform

Zero trust is not simply about a single technology like identity or application segmentation. Zero trust is a strategy, **a foundation upon which to build your security ecosystem.** It securely connects users to applications using business policies over the internet. At its heart lies a zero trust technology platform guided by three key tenets:

① Connectivity based on **identity and policy**

② Making **applications invisible**

③ **Proxy-based architecture** to connect to apps and inspect traffic

Platform

1 Connectivity based on identity and context

2 Making applications invisible

3 Proxy-based architecture to connect to apps and inspect traffic

Traditional VPNs and firewalls put users on the network for application access. Once on the network, the inherent trust placed in the user increases the risk of lateral movement by threats or would-be attackers. Conversely, zero trust uses identity and policy based on context to securely connect authenticated users to only a specific authorized application based upon granular access and security policies, without ever putting users on the corporate network. Limiting access prevents lateral movement and reduces business risk. And because no network resources ever need to be exposed to the internet, you can protect against DDoS and targeted attacks.

The migration of applications to the cloud greatly expands the attack surface. Traditional firewalls publish your apps on the internet which means they can easily be found by users and hackers. A zero trust approach should avoid exposing the corporate network to the internet by concealing source identities and obfuscating IP addresses. By making apps invisible to adversaries and accessible only by authorized users, the attack surface is reduced, and access to applications—on the internet, in SaaS, or in public or private clouds—are always secure.

Next-generation firewalls struggle to inspect encrypted traffic. As a result, organizations often end up bypassing the inspection of encrypted traffic, increasing the risk of cyberthreats and data loss. Furthermore, firewalls use a "passthrough" approach, allowing unknown content to reach its destination before any analysis is complete. If a threat is detected, an alert is sent, but that can be too late. Instead, effective threat protection and comprehensive data loss prevention requires a proxy architecture designed to inspect SSL sessions, analyze the content within transactions, and make real-time policy and security decisions before allowing traffic to move on to its destination. And it needs to do all of this at scale—without impacting performance, no matter where your users connect.

Recommended action: Evaluate a zero trust platform like the **Zscaler Zero Trust Exchange™**

People

The successful adoption of zero trust starts with the right platform, but it is dependent on the organization **developing new skills and embracing a new cultural mindset.** From the IT leaders faced with the need to transform quickly and safely, to the IT practitioners on the ground implementing zero trust, everyone from your executive team to your end users and extended ecosystem must be included to ensure success.

A CULTURAL SHIFT

People

IT leaders

As an IT leader, you must be both an innovator and a strategist. Your zero trust journey requires you to align business and IT priorities, break down silos, and apply the right technologies and architecture to drive transformation and achieve the desired outcomes for your business. On your journey to zero trust, you will need to:

- **Understand best practices and strategies** for transformation from peers and organize the company to implement those changes

- **Help your IT practitioners develop the skills and knowledge** required to successfully shift from a network-centric architecture to a zero trust architecture

- Make zero trust **invisible to your end users**

Recommended action:
Connect with like-minded innovators about zero trust and digital transformation best practices in a forum such as **Zero Trust REvolutionaries** ↗

People

IT practitioners

Your IT teams are experts in networking and security, accustomed to working on hardware and setting policy based upon 30 years of IT networking and security principles. Migrating to zero trust **directly impacts your IT practitioners.** Many of the skills they've relied upon in the past will need to be updated, and they'll need to develop new skills for digital transformation, but the outcome will be that they'll have a far greater impact on the organization and a more valuable, future-oriented body of knowledge.

Success hinges upon providing **advanced training to transition your IT workforce,** ensuring that they understand new business processes as well as the best practices and procedures for using zero trust services. At the same time, you can demonstrate how zero trust will **save them time** and enable them to **deliver more value** to the organization.

Recommended action:
Help your IT practitioners get up to speed on zero trust with a certified training program, the **Zscaler™ Zero Trust Academy**

People

Your users

If done correctly, zero trust is an invisible enabler for your end users, allowing employees to work from anywhere on any device. Because zero trust access is always based on identity and business policies, and the cloud service automatically connects users to applications via the fastest access path, the physical location of the user no longer matters. A user working in the office has the **same fast and consistent access experience** when working from home, or anywhere for that matter.

At the same time, a robust zero trust solution enables organizations to **dramatically reduce risk without blocking application access** for users. For example, cloud browser isolation technology can provide safe access to active content by delivering webpages as pixels rendered in an isolated environment without impacting the user experience. It can also be leveraged to limit the ability to copy and paste data, prevent file downloads, or confine downloads to the isolation container to protect endpoint devices from ransomware and other sophisticated threats. In this way, zero trust leverages technology to limit risk based upon context.
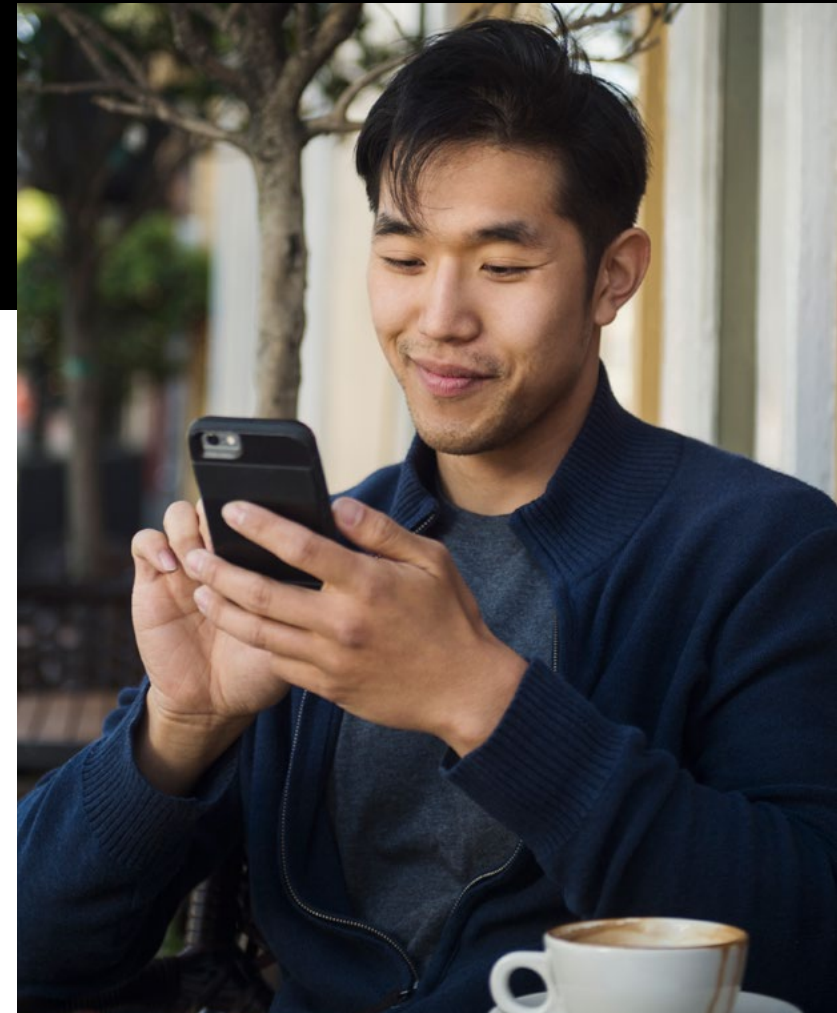
Recommended action:
Leverage zero trust architectures that include tools that ensure your users have a great experience, such as **Zscaler Digital Experience** ↗

Process

What are the steps for getting to zero trust and how can you accelerate your business transformation? Knowing where to begin may be the hardest part of this journey, but it doesn't have to be that way. Zero trust starts with a platform, and must extend to **encompass data, people, devices, and workloads.**

As such, robust product integrations with your identity provider, endpoint security solution, and SIEM solution are essential pieces of the zero trust puzzle to add additional context and simplify adoption.

A PROGRAMMATIC PATH

Process

In light of the need for integration, we recommend a **zero trust platform and technology partner ecosystem** that provides the following tools to inform your design and empower your adoption of zero trust:

- **Solution blueprints** that provide use-case reference architectures

- **Design guides** that share design principles and integration best practices

- **Deployment guides** that provide configuration guidance as you activate integrations for Proof of Value (PoV) and production deployment

Implementing a holistic zero trust solution becomes much easier with the right blueprint. Seek out vendors with jointly validated reference architectures designed to address a specific set of use cases, and prescriptive design guidance for security architects on using these platforms together based on best practices.

Such guidance provides a more structured framework that simplifies deployment, ensures efficient operations and the best user experience, and enables enforcement of optimal security. All of which will allow you to accelerate adoption of zero trust across your organization.

Recommended action: Leverage solutions with deep partner integrations that provide validated designs and blueprints, such as those found in the **Zscaler zero trust ecosystem** ↗

Seize your zero trust moment

Digital transformation makes enterprises more agile and efficient—but it requires you to rethink your network and security architectures. Zero trust provides **the foundation for cloud-first organizations to accelerate digital transformation** and empower employees to work productively and securely from anywhere. As you begin your journey, developing a strategy that incorporates the right platform, people, and processes will help ensure success.

Select a platform that uses identity and business policy to establish trust, and connects users to resources without placing them on the corporate network. Protect applications by making them invisible to adversaries and accessible only by authorized users. And use a proxy architecture, not a passthrough firewall, to secure your data and ensure effective cyberthreat protection.

Engage your peers to capture best practices and strategies for transformation. Align your organization to adopt a new cultural mindset and develop the skills necessary to implement and manage a zero trust architecture, while ensuring zero trust is invisible and seamless to your end users. This all becomes easier with the right blueprint. Leverage **a zero trust platform with robust partner integrations that provide jointly validated reference architectures and prescriptive design guidance** for using these platforms together.

Keeping these elements in mind will help you **seize your zero trust moment, accelerate your digital transformation, and make IT a true business enabler.**

Explore the countless benefits of **a true zero trust platform.**

Start your journey ↗

⌀zscaler™