zscaler™

eBook

The Secure Enterprise Starts with Zero Trust

Accelerate your business transformation

Make security the foundation for successful transformation

Digital transformation can only help your business achieve its strategic goals—sustainable competitive advantage, market leadership, new business models, revenue opportunities, and more—if you have a secure foundation.

Yet, the technologies that make transformation possible—cloud, mobility, SaaS, internet of things (IoT), and others—can also significantly increase the risk of damaging cyberattacks. The traditional corporate perimeter simply can't keep your organization safe in a cloud-first world, where users, applications, and data are everywhere, all of which exponentially increase your attack surface. Legacy approaches to security are inadequate in modern cloud environments, resulting in increased complexity, cost, and operational overhead, creating roadblocks and speed bumps that delay transformation.

That's why businesses must transform security and make it the foundation for their company's digital transformation. Success starts with security, and security starts with zero trust.

We'll show you how.

Say goodbye to the moat

The traditional security approach (known as a castle-and-moat architecture) relied on perimeter defense (the moat) to secure the organization (the castle) from outside attacks. Perimeter defenses protected the network and assumed that everything operating within the network and the four walls of the data center was safe and could be trusted.

The world has changed:

- **It's a cloud-first world:** Business happens in the cloud, making it—not the data center—the new center of gravity for the business. Application modernization in the cloud is well underway and SaaS usage continues to grow. So, how can companies protect their business in the cloud if it's not within the castle and protected by the moat?
- **Internal traffic can no longer be trusted:** The perimeter is long gone, as BYOD, mobility, and remote work have demonstrated. Damaging cyberattacks take advantage of implied trust within porous perimeter defenses. Flat legacy networks allow for unrestricted lateral movement by increasingly sophisticated adversaries. Attackers then pivot from an infected user to one machine (or domain controller, server, or workload) after another. The entire network is at risk.
- **Legacy security approaches are outdated:** Despite the name, next-generation firewalls (NGFWs) and other legacy network security solutions are not designed for modern IT architecture and cloud transformation. They can't support zero trust, the most-recommended, context-driven security model that removes implied trust to make users, devices, applications, and data safe, no matter where they are. NGFWs and other legacy solutions are too brittle, complex, and expensive to support zero trust principles effectively to reduce risk and better protect the enterprise.

DATA STATISTICS

The state of cloud security

8 of 10

top attacks exploited internet exposed services[1]

26%

of servers expose their Secure Shell (SSH) ports to the internet[2]

20%

of servers expose Remote Desktop Protocol (RDP) ports to the internet[3]

#1

concern of CEOs in the US is cyberthreats[4]

63%

of cybersecurity transformations are either lagging behind digitization or only keeping pace[5]

Sources: 1. NSA 2020; 2–3. Zscaler, "The 2020 State of Cloud (In)Security;" 4–5. PwC, "Cyber-ready — Today and for Tomorrow," June 2021

Realize the limitations of traditional security in the cloud

Extending traditional security approaches such as NGFWs to a modern cloud, hybrid, or multicloud environment results in far more challenges than benefits, including an expanded attack surface that puts your business at even greater risk than before.

Organizations use two main approaches to retrofit their legacy security infrastructure for the cloud: either extend the network and security infrastructure to the cloud or stretch the perimeter to include the cloud. Neither approach delivers the secure foundation companies need to confidently accelerate digital transformation.

APPROACH #1:

Extend legacy network and security to the cloud

- Extend the network to the cloud via site-to-site VPN
- Extend the network to all users via VPN
- Extend the network to branch locations via MPLS

CHALLENGES

Poor user experience.
Backhauling traffic introduces latency and impacts application performance.

Risk of lateral threat movement.
Extending the WAN increases risk. A single infected user can spread malware to everything on the corporate network.

High cost and operational overhead.
As the network and security stack proliferate, so do costs.

APPROACH #2:

Stretch the perimeter to include the cloud

- Extend the network to the cloud via site-to-site VPNs
- Extend the network to users via VPN to virtual cloud firewalls
- Extend the network to branch locations via site-to-site VPNs

CHALLENGES

Large attack surface.
Every firewall and application that is internet-facing can be discovered and potentially exploited.

Risk of lateral threat movement.
The perimeter becomes extremely large, and once inside, there's nothing to stop an attacker.

High operational overhead and costs.
While this approach can reduce MPLS costs, managing a rapidly expanding number of firewalls and swarms of alerts from firewalls increases operational overhead and costs.

Start with zero trust to transform security

Secure transformation requires a fresh, new approach that fundamentally reimagines security as the foundation for all transformation. That foundation starts with zero trust.

Zero trust is a modern approach to security based on the principles of least-privileged access and that no user or application should be trusted by default. A zero trust architecture implements these principles to securely connect users, devices, and applications using business policies.

With a secure foundation built on zero trust, you get the security and confidence your business needs to accelerate transformation. For a zero trust architecture that is agile, transparent, scalable, and simple, you can't use traditional NGFWs, security appliances, and network approaches. You need a modern cloud native solution.

A zero trust architecture

- Protects against sophisticated cyberthreats
- Prevents data loss
- Prevents lateral movement of threats
- Delivers a great user experience
- Reduces cost and complexity

Create a secure foundation with Zscaler

The world's most transformative enterprises depend upon the world's most transformative security platform to accelerate their secure digital transformation. The Zscaler Zero Trust Exchange™ accelerates business transformation by making the cloud safe. It secures users and applications, regardless of their location, using context-based identity and policy enforcement.

Unlike traditional NGFWs and security point products, the Zero Trust Exchange is built to protect today's cloud-first, hybrid workforce with highly proactive, intelligent, and radically simple security that significantly reduces business risk.

We've created the world's only true zero trust platform, disrupting decades of legacy approaches by abstracting security from the underlying network to securely connect users and devices directly to applications. We ensure threats and data theft attempts are found, stopped, and contained, so you can lead your business forward with confidence.

The Zero Trust Exchange is built on three tenets that make it superior to traditional approaches:

THE ZSCALER ZERO TRUST EXCHANGE	CASTLE-AND-MOAT / PERIMETER-BASED APPROACH
1 **Zero network access.** Connect users to applications, not corporate networks, to prevent lateral movement.	**Network access.** Connect users to networks for application access.
2 **Zero attack surface.** Make applications invisible so they can't be attacked.	**Increased attack surface.** Applications are published on the internet, increasing the attack surface.
3 **Zero passthrough connections.** Deny all privileges using our proxy architecture for improved cyberthreat and data protection.	**Passthrough connections.** Passthrough firewall architecture provides limited ability to inspect traffic and protect data.

WHY ZSCALER?

Reduce your risk with our proxy architecture

The Zero Trust Exchange uses a proxy–based architecture that can inspect SSL sessions, analyze the content within transactions, and make real–time policy and security decisions. This proxy approach fully terminates the connection and then reestablishes it.

By comparison, a traditional network security or firewall approach uses a passthrough connection, which cannot perform proper inspection for security and data protection, and allows zero day threats to infect organizations.

TENET #1

Prevent compromise by blocking threats before they reach you

Instead of expanding your attack surface as you transform and expand into the cloud, the Zero Trust Exchange eliminates the internet attack surface by making applications invisible. At the same time, you can protect users, servers, applications, and IoT/OT systems with a platform that delivers all critical enterprise security controls as an edge service, close to every user.

With Zscaler, you can prevent compromise by:

- Instantly detecting, preventing, and containing the most sophisticated attacks and ransomware attempts inline, across all traffic, including SSL, with best-of-breed, AI-powered security services
- Stopping attacks with autonomous zero trust policies that continuously adapt to the evolving threat landscape, powered by the world-class Zscaler ThreatLabz experts and threat intelligence from the world's largest security cloud
- Preventing attackers from discovering, exploiting, or infecting users and applications by making them invisible to the internet and only accessible to authorized users or devices through the Zero Trust Exchange
- Monitoring, validating, and automatically addressing gaps in entitlements, security policy, and compliance caused by misconfigurations and overly permissive access across all cloud environments

TENET #2

Prevent lateral movement and stop the spread

One of the biggest security risks with traditional corporate networks is lateral movement. Once malware gets on the network, it can propagate freely within the organization, leading to widespread damage.

With Zscaler, you eliminate the risk of lateral movement by directly connecting users and devices to applications, not the network. Using Zscaler, your organization can:

- Mitigate the damage potential of any compromised user or device with our integrated zero trust network access (ZTNA) capability for remote and on-campus users
- Extend zero trust-based lateral movement prevention to cloud workloads and data centers with groundbreaking identity-based microsegmentation that allows or blocks workload communications in hybrid and cloud environments
- Detect, trap, and analyze attacks with proactive decoy applications and lures that generate high-confidence alerts and provide critical insights into attack sequences

TENET #3

Prevent data loss

Stop data loss caused by accidental exposure or malicious exfiltration with our holistic data protection capabilities, spanning managed and unmanaged devices, servers, public cloud, and cloud applications. With the Zscaler platform, your organization can:

- Control sanctioned and unsanctioned cloud applications while securing sensitive data at rest from theft or accidental exposure with best-of-breed integrated CASB capabilities
- Safeguard sensitive data in motion with granular DLP controls that identify and block data leakage or theft across all inline and SSL traffic in real time
- Extend DLP controls to unmanaged and BYOD devices with unique, integrated Cloud Browser Isolation technology
- Identify and fix dangerous misconfigurations in SaaS and public clouds to prevent cloud breaches and data loss

Security transformation starts with zero trust

Confidently accelerate your move to the cloud with the Zscaler Zero Trust Exchange.

Learn More

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE–based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com