zscaler™ | Brite

EBook

The Top Zero Trust Use Cases

The challenges organizations solve to reduce risk and cost

Contents

EBook

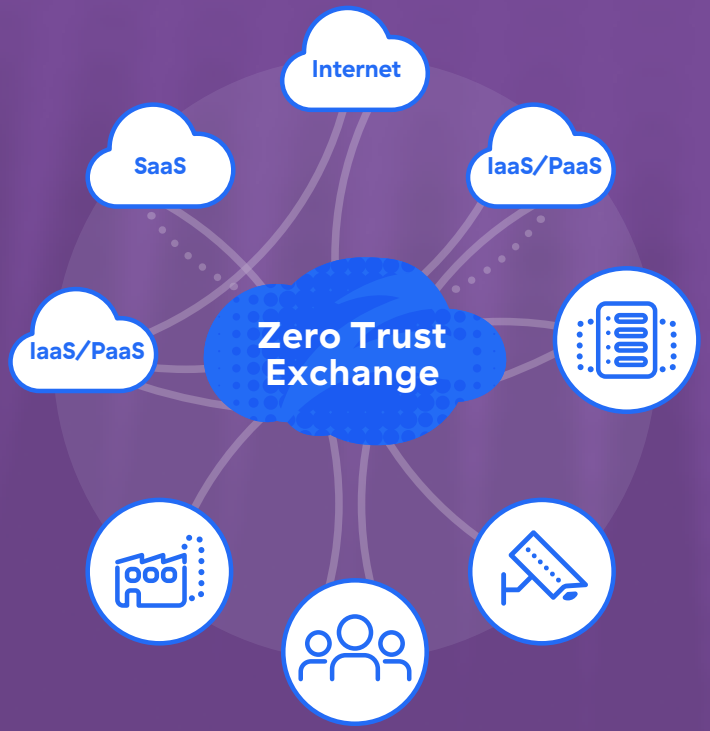
Zero Trust for Superior Security and Economic Value

Businesses have undergone rapid evolution over the last several years. Users, apps, and data all once resided on premises, but the web, remote work, and the cloud have enabled them to move off premises en masse. As a result, legacy security architectures that defend the network perimeter through patchworks of point products no longer offer sufficient protection.

Perimeter-based architectures are also highly expensive—and not just because of the costly breaches and noncompliance they can enable. Deploying expensive network and security appliances increases complexity and management burdens on admins, consuming time and money. User experience issues from backhauling traffic and poor capacity planning hamper productivity and waste resources, as well.

Organizations need a new security architecture in order to embrace digital transformation while reducing business risk and cost. Specifically, they need zero trust.

Rather than defending network access via countless costly appliances, a zero trust architecture leverages one holistic platform that secures user-to-app, app-to-app, and machine-to-machine communications. It does so based on the principle of least-privileged access, using context-based identity and policy enforcement.



The Zscaler Zero Trust Exchange is the world's largest, most high-performance security cloud. It is a comprehensive platform of integrated services that delivers zero trust security at the edge across all users, devices, apps, and locations. With Zscaler, organizations can also optimize their technology expenditures, reduce complexity, improve operational efficiencies for admins, and enhance user experience.

Zscaler has helped thousands of organizations transform their security while reducing complexity and cost. Read on to learn the use cases that customers leverage our zero trust architecture to solve.

Cyberthreat Protection

Modern threats easily bypass perimeter-based security architectures. These architectures expand the attack surface via VPNs and firewalls, which can be found and targeted on the public web. They enable lateral threat movement because they connect users to the network as a whole rather than to specific apps. The passthrough appliances that support legacy architectures also lack the scalability to inspect traffic at scale or stop threats in real time.

Zero trust defenses against zero-day attacks

The Zscaler Zero Trust Exchange stops threats at every step in the attack chain. With apps sitting behind Zscaler, the attack surface is eliminated. As users and apps are connected directly instead of placed on the network, lateral movement is prevented. Compromise is stopped through inline security policies and AI-powered threat prevention services, as well as out-of-band functionality that remediates threats at rest in the cloud.

The Zscaler advantage

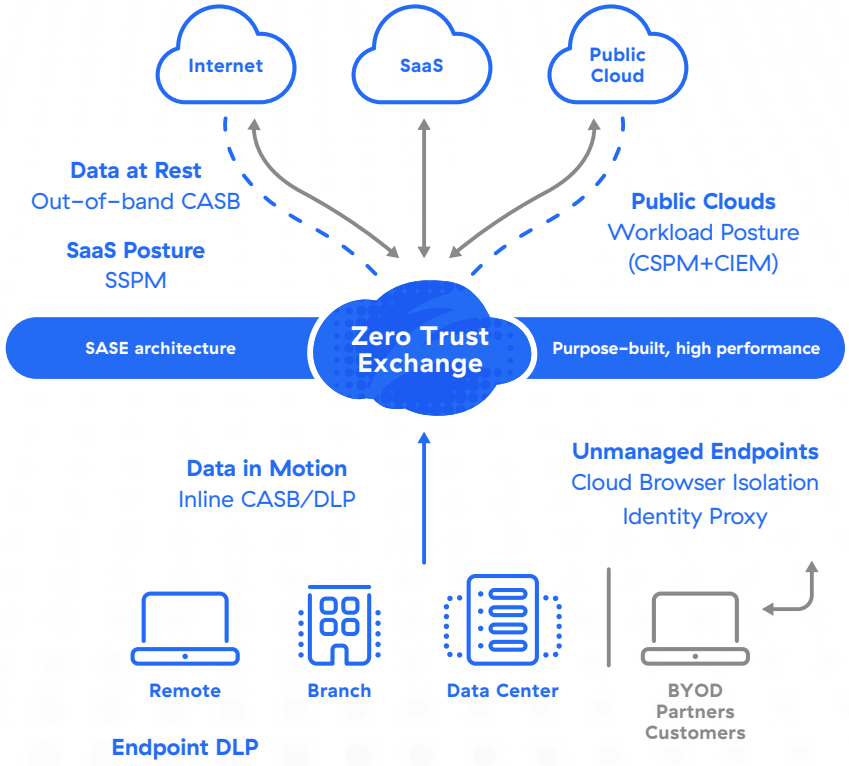
- Full, scalable, inline inspection of traffic—including encrypted traffic—with real-time policy enforcement
- The Zscaler cloud effect, whereby threats found anywhere are blocked automatically across all customers
- AI-powered cyberthreat detection and prevention to stop the most advanced known and unknown threats

Data Protection

Data is now highly distributed across remote workers, countless devices, SaaS, the web, and the globe as a whole. As a result, perimeter-based architectures that were designed to protect data on premises now leave data exposed. Network security tools can't follow data off premises, address modern use cases, or scale to protect data in encrypted traffic. Adding disjointed endpoint and cloud security tools leads to inconsistent protections and unnecessary complexity.

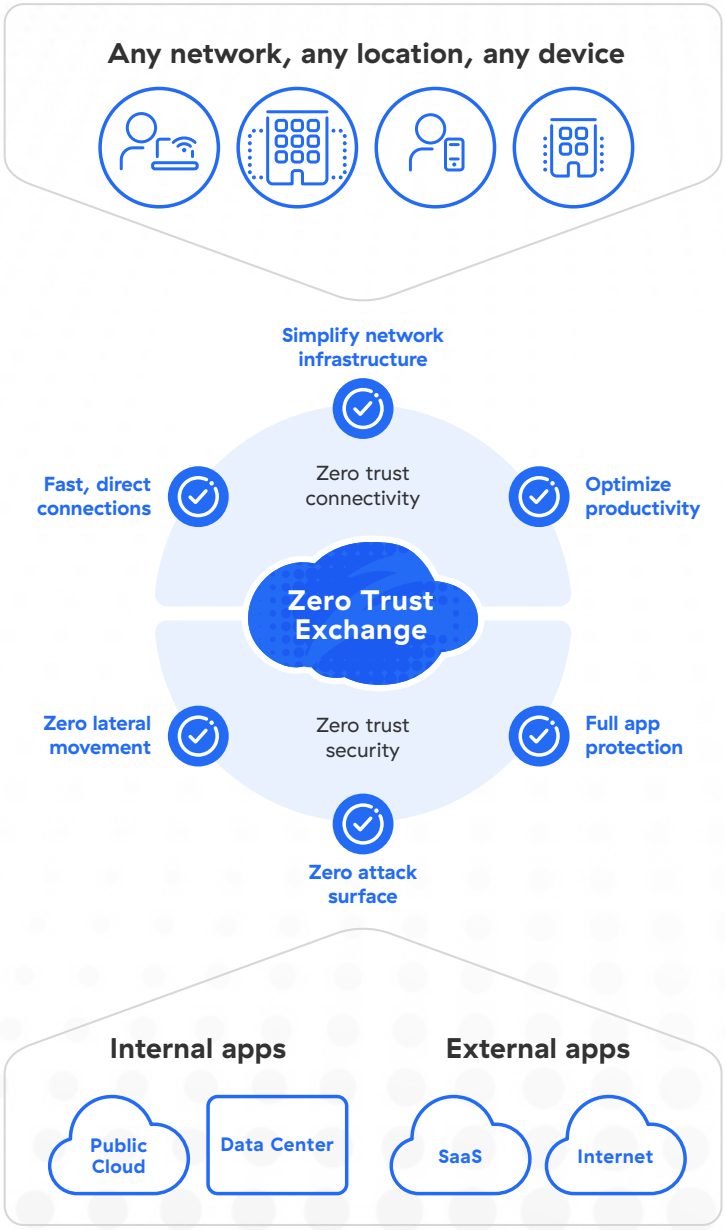
Zero trust protection wherever data goes

Zscaler Data Protection is a comprehensive offering that follows data wherever it goes to enforce zero trust policies. Traffic is scanned inline for real-time data classification and policy enforcement. Browser isolation streams data as pixels to unmanaged devices to stop exfiltration. Cloud data at rest is scanned for sensitive information and revocation of risky shares. Posture Control remediates cloud misconfigurations and excessive permissions.



The Zscaler advantage

- A unified policy engine, with predefined and customizable dictionaries, defends data consistently wherever it goes
- Full SSL inspection for real-time protection of encrypted traffic, powered by the world's largest security cloud
- Innovative Zero Configuration Data Protection discovers all sensitive data automatically so that it can quickly be secured



Securing the Hybrid Workforce

Today's hybrid workforce has created an urgent need to enable secure, fast, and reliable access to all applications—from any device, any location, and any network. But legacy architectures require backhauling traffic to appliances that put users on the network. This increases risk, harms user experience and productivity, and fails to address the security challenges that modern companies face.

Seamless connectivity and security everywhere

The Zscaler Zero Trust Exchange provides a cloud-delivered approach to ensuring fast, seamless, zero trust access across the entire business ecosystem—no matter where people are working. By providing policy-based access to external and internal apps, users can work securely from anywhere—without extending network access, and with better threat and data protection enforced.

The Zscaler advantage

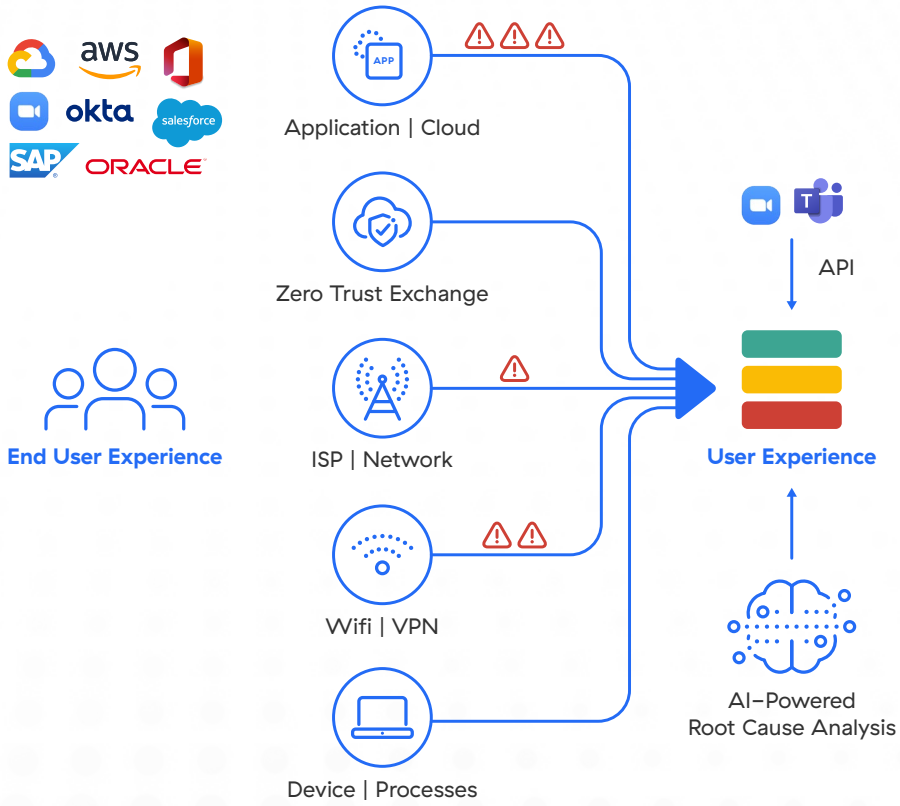
- Direct app connectivity that eliminates the need to backhaul to appliances that put users on the network
- A single-pass cloud architecture with CASB, SWG, ZTNA, and more that offers efficient, complete security everywhere
- Over 150 points of presence and digital experience monitoring ensure maximum performance globally

Optimizing Digital Experiences

With the cloud and remote work, today's digitally-enabled workforce needs fast and reliable connectivity. But siloed application, network, and device monitoring tools leave blind spots, requiring IT operations and service desk teams to manually export and correlate data from each tool. This lack of end-to-end visibility into digital experience forces IT teams into firefighting problems after they are reported, rather than resolving them before users are impacted.

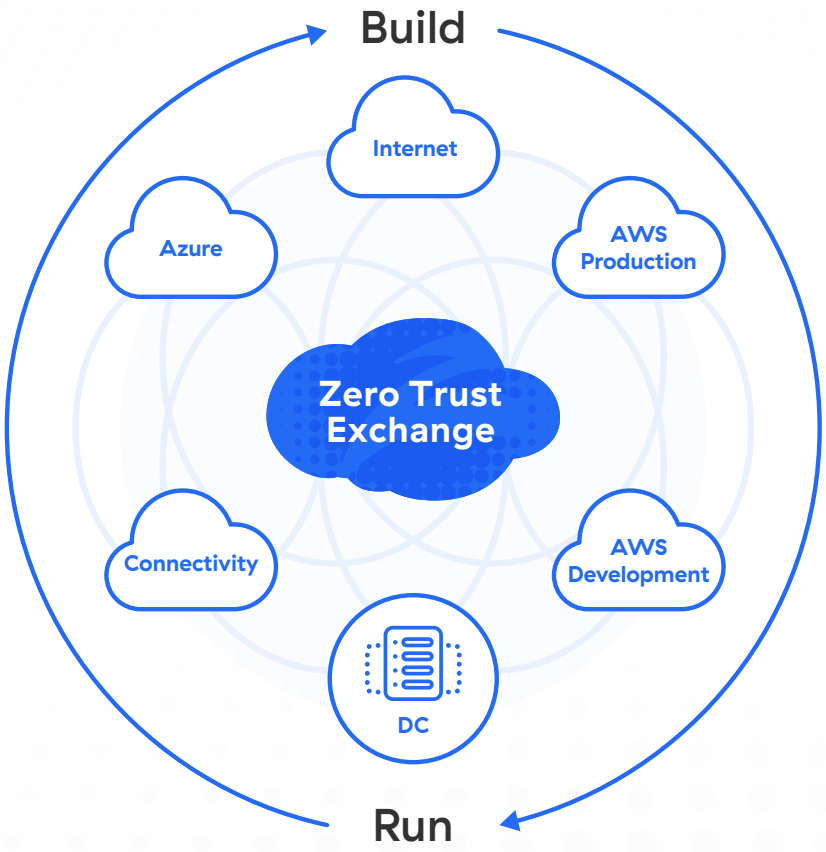
Enhancing user and administrator productivity

Zscaler Digital Experience (ZDX) is a digital experience monitoring solution delivered as a service from the Zscaler cloud. It provides end-to-end visibility and troubleshooting of end-user performance issues for any user or app anywhere. It continuously collects and analyzes metrics including app availability, response times, network hop-by-hop performance, and device health metrics like configuration, CPU, memory usage, process information, and device events.



The Zscaler advantage

- Quickly pinpoint and resolve root causes of poor user experience down to the offending device, wifi or regional network, and app
- Gain inline visibility into user traffic to identify and prevent issues before they impact workforce productivity
- Eliminate point products and simplify troubleshooting through one interface with end-to-end visibility



Protecting Cloud Workloads

As workloads migrate to the cloud, trying to secure them with perimeter-based tools creates challenges. Legacy solutions aren't designed to help build or run secure cloud workloads. Instead, they expand the attack surface, enable lateral threat movement, expose data, and hinder compliance. The sprawl of disjointed tools also creates security blindspots and silos for logs and data, reducing the pace of innovation for DevOps.

Build and run apps with zero trust security

Built on an innovative zero trust architecture, Zscaler for Workloads secures cloud-native app development and deployment, ensuring complete protection, from build-time to runtime, as well as regulatory compliance. This consolidated approach eliminates the need for point products, data silos, and security blind spots while fostering cross-team collaboration and accelerating digital transformation.

The Zscaler advantage

- Prevents misconfigurations, excessive entitlements, and security issues due to limited resources and skill sets
- Accelerates incident response with automated risk prioritization and remediation
- Secures workload-to-workload and workload-to-internet communications to stop threats and data loss

Wrap-Up

Digital transformation provides a wealth of productivity and flexibility benefits, but organizations must ensure that they transform both effectively and securely. With the Zscaler Zero Trust Exchange, companies can easily embrace a new security architecture that delivers unparalleled protection, connectivity, performance, and cost savings, empowering them to obtain the promised benefits of digital transformation.

To learn more about zero trust, read our book, **Seven Elements of Highly Successful Zero Trust Architecture.**

To learn more about the superior economic value that Zscaler provides its customers, read the **ESG Economic Validation Report.**

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**.

Brite

Brite
salesinfo@brite.com
800.333.0498
brite.com