

Seven Elements of Highly Successful Zero Trust Architecture

An Architect's Guide to the Zscaler Zero Trust Exchange.

Traditional security architectures leave businesses vulnerable

Status quo security approaches—using firewalls and VPNs—connect users to the network, enabling attackers to compromise users, devices, and workloads, and move laterally to reach high-value assets and extract sensitive data.

Today's hybrid workplace requires a zero trust approach to security

To protect their organizations, innovative business leaders are turning to zero trust, a holistic security approach based on least-privileged access and the idea that no user or application should be inherently trusted.

How is a zero trust architecture implemented?

True zero trust is delivered through the **Zscaler Zero Trust Exchange**—an integrated cloud-native platform that securely connects users, devices (IoT/OT), and workloads to applications without connecting to the network.

Seven elements form the foundation of a true zero trust architecture

With this unique approach, Zscaler eliminates the attack surface, prevents the lateral movement of threats, and protects your business against compromise and data loss.



1. Who is connecting?

Terminates the connection being requested, then verifies the user, IoT/OT device, or workload identity.

2. What is the access context?

Validates the context of the connection requester, looking at attributes such as role, responsibility, request time, and circumstances of the request.



3. Where is the connection going?

Confirms that the destination is known, understood, and contextually categorized for access. If the destination is unknown, flag for further analysis.

4. Assess risk

Leverages AI to dynamically compute a risk score associated with the connection based on factors including device posture, threats, destination, behavior, and policy.



5. Prevent compromise

Inspects traffic and content inline to identify and block malicious content.

6. Prevent data loss

Inspects outbound traffic to identify sensitive data and prevent its exfiltration.



7. Enforce policy

Enforces policy per-session and determines what conditional action to take regarding the requested connection. Once an “allow” decision is reached, a secure connection to the internet, SaaS app, or internal application is established.

Are you ready to learn how to apply these seven foundational elements of a zero trust design to your business to **eliminate your attack surface, prevent lateral threat movement, and protect your organization against compromise and data loss?**

[Read the ebook](#)