zscaler™ | e+ SECURITY

Ebook

10 Ways a Zero Trust Architecture Protects Against Ransomware

- **~250% increase in ransomware attacks over the past two years.** Every organization is at risk, with escalating scope and volume.
- **1 in 2 ransomware infections involve data theft.** Known as double extortion, this tactic forces victims to pay to protect data.[1,2]
- **An attack hits every 14 seconds worldwide.** Attackers hide attacks to bypass traditional security controls.

Ransomware is the biggest threat to digital business

While ransomware has been around for decades, its prevalence has exploded in the last few years. These attacks used to be perpetrated by individuals; now, they're launched by networked groups of affiliates who buy and sell each other's specialized skills and toolkits. Attacks were once unfocused and one-dimensional; now, they use targeted, multilayered tactics that are much harder to defend against and command much higher ransoms. **Ransomware is expected to cause $42 billion in damages by the end of 2024.**[1]

Arguably, the most impactful trend in modern ransomware is the advent of double-extortion attacks, in which attackers steal data and threaten to publish it in addition to encrypting it. Roughly 50% of ransomware attacks now include attempts to exfiltrate data.

There is one underlying strategy that maximizes an organization's chances at mitigating the damage a ransomware attack might cause: zero trust.

Zero trust is an approach to security that's based on the notion that a breach has already occurred. Architectures, access control policies, and monitoring and authentication tactics are put in place to mitigate the amount and severity of the damage an attacker can cause.

Here are 10 ways in which zero trust can help your organization defend against ransomware.

[1] *ThreatLabz 2023 State of Ransomware Report*
[2] *ThreatLabz 2022 State of Ransomware Report*

Understanding the ransomware attack sequence

While ransomware groups leverage many different technologies, tactics, and payloads to achieve their aims, their attack sequence remains largely the same. 1) In general, attackers will first perform reconnaissance to discover weak entry points in the enterprise attack surface. Most often, this includes scanning its broad set of internet-connected devices, applications, security tools like VPNs and firewalls — which have become primary attack vectors — and other routable infrastructure and networking resources. 2) Next, attackers will work to compromise a device, commonly by deploying a malicious payload or by compromising user credentials by way of social engineering. 3) This forms a beachhead, from which cybercriminals then scan the network environment to discover other exploitable resources, use them to move laterally, escalate privileges, and discover and exploit crown jewel applications — those with sensitive and business-critical data. 4) Finally, attackers steal and encrypt data, extorting the business to pay.

The best ransomware defense aligns with these attack stages. Enterprises must work to eliminate or dramatically shrink the external attack surface, prevent compromise across their devices, resources, and applications, stop lateral movement, and prevent data loss. Here, we will see how implementing a zero trust architecture helps achieve these goals across the attack chain.

The 7 key elements of a zero trust architecture

Before digging in, it's key to understand the seven layers of defense that a zero trust architecture provides. We know that ransomware groups work to compromise internet- and network-connect devices and infrastructure resources, or gain access to user credentials through social engineering, which they use as a beachhead to discover and exploit other resources, escalate privileges, and steal data.

Traditional enterprise security approaches that rely on castle-and-moat security to protect hub-and-spoke networks are particularly vulnerable to ransomware attacks. This is due to the ease of discovering weak entry points from across a large, discoverable, internet-facing attack surface comprised of connected devices, security appliances like VPNs and firewalls, and infrastructure resources. Once a single asset is compromised, through malicious exploits or tactics like social engineering, it becomes easy to move laterally across the broad, flat network, exploit other resources, escalate privileges, and steal and encrypt data.

In sharp contrast, a zero trust architecture securely connects users, devices, and workloads directly (and only) to the applications they are authorized to access — without ever placing them on a routable network where they can be discovered and exploited. In this model of least-privilege access, every connection is assumed to be untrusted and automatically terminated. Connectivity is only established once seven layers of identity, context, security, and policy have been verified—between users, devices, workloads, both internal and SaaS applications, IoT and OT devices, and more.

Diving deeper, a successful zero trust architecture contains 7 key elements to defend against ransomware.

Verify identity and context

When a connection is requested, the zero trust architecture terminates the connection and verifies identity and context:

1. **Who is connecting?** — Verifies the user/device, 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, and location.
3. **Where is the connection going?** — Confirms that the destination is known, understood, and contextually categorized for access.

Control content and access

Next, the zero trust architecture evaluates the risk associated with the connection request, and inspects traffic for cyber threats and sensitive data:

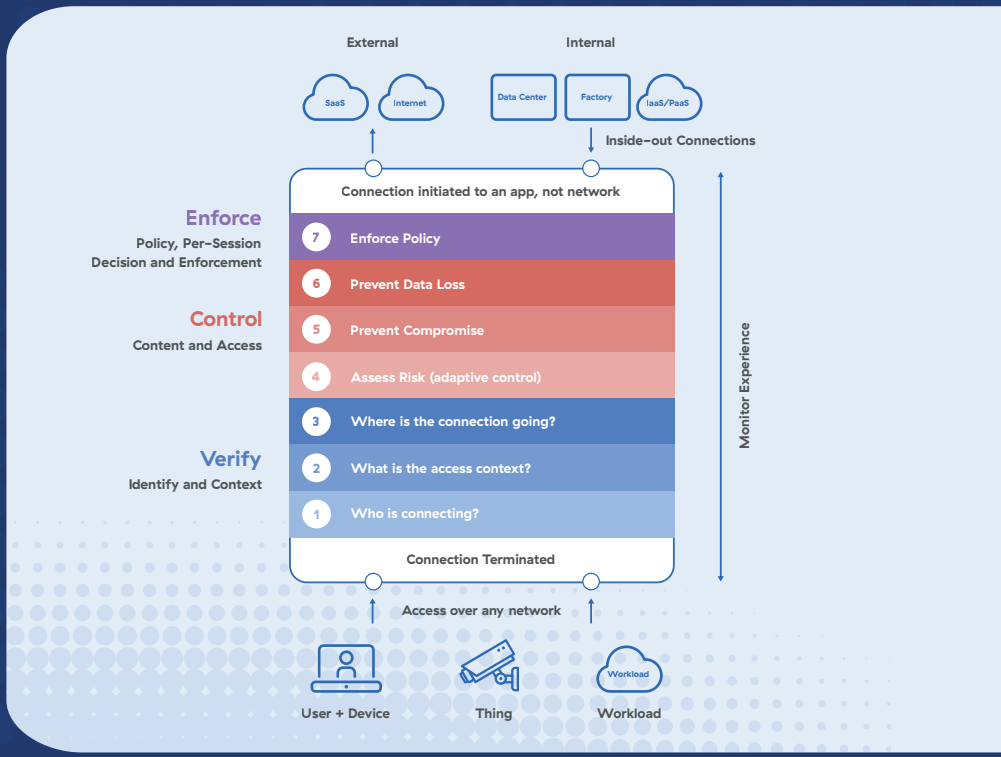
4. **Assess risk** — Leverages AI to dynamically compute a risk score of the requested access.
5. **Prevent compromise** — Inspects inbound traffic to identify and block malicious content.
6. **Prevent data loss** — Decrypts and inspects outbound traffic and content to prevent exfiltration of sensitive data.

Enforce Policy, per-session decision and enforcement

After controlling for risk, policy is enforced before ultimately establishing a connection to the internal or external application:

7. **Enforce policy** — 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. For internal apps, this is an encrypted, outbound-only tunnel that eliminates any attack surface.



#1

By making applications invisible to attackers, a zero trust architecture minimizes the attack surface.

When application, user, and device identities are openly discoverable on the internet, it's like putting your most valuable information assets on public display. When these assets are visible, attackers are readily able to find and exploit vulnerabilities—such as unpatched web server software or a weak password that can be cracked in a brute force attack—giving them an immediate and strong foothold in your environment.

Leveraging a solution like Zscaler Private Access™, enterprises can hide their private applications and servers from the internet, creating inside-out connectivity only to authenticated users.. With this form of connectivity, all applications remain private and thus invisible to attackers. Extending this approach across all devices and applications in your environment makes it near-impossible for attackers to conduct reconnaissance and instantly eliminate much of the attack surface.

#2

In a zero trust architecture, all traffic—including encrypted traffic—is subject to inline content inspection.

The vast majority of today's internet traffic leverages encryption, and malicious traffic is no exception. More than 90% of internet traffic is now encrypted, and encryption of ransomware is up roughly 250% over the past two years. Security teams can no longer assume that all SSL/TLS-encrypted traffic is safe.

However, now that inspecting all traffic, encrypted or not, is an essential part of a robust defensive strategy, architectures relying on next-gen firewalls and other perimeter-based defenses are no longer up to the task. It's simply impossible for even the most advanced on-premises security tools to inspect all SSL/TLS-encrypted traffic without introducing performance bottlenecks that get in the way of productivity. A proxy-based architecture in the cloud that was purpose-built to detect SSL/TLS-encrypted malware at scale will protect all of your traffic and eliminate blind spots.

#3

Zero trust strategies include controls to detect unknown and zero-day threats before they can cause harm.

Growing numbers of ransomware attacks are taking advantage of custom-crafted and advanced malware. To defend against these threats, you need to be able to detect and block novel threats. With AI-driven malware detection and prevention, you can rely on behavior analysis to discover previously unknown ransomware variants by quarantining and fully analyzing files before they're delivered to users or allowed to execute.

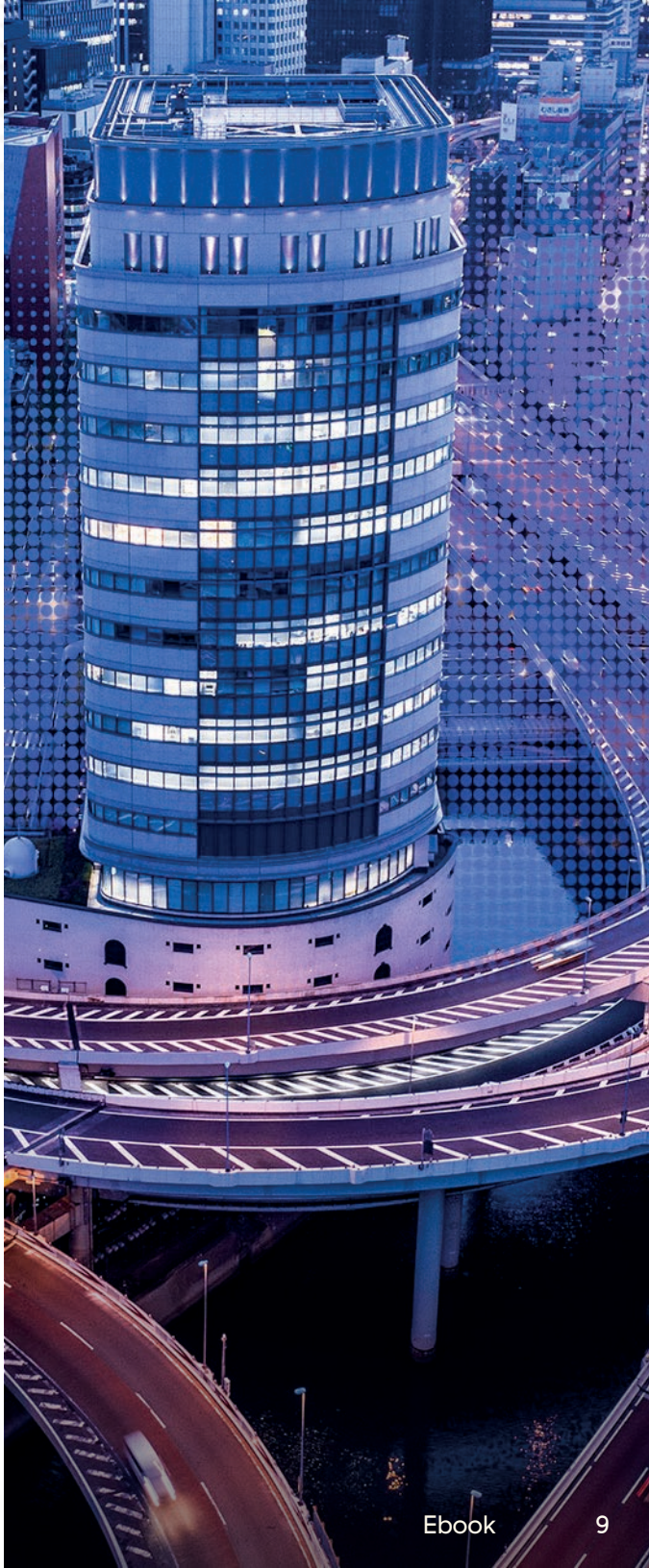
With a solution like the Zscaler Cloud Sandbox, you can define policies based on users, groups, and content types, giving you granular control over quarantine actions. Moreover, you can leverage an AI Instant Verdict to automatically quarantine likely malicious files and send them for deep inspection. Because this solution is part of the Zscaler Zero Trust Exchange™, you get near real-time file verdicts sourced from 300 trillion daily signals and a global community, which minimizes user impact while maximizing malware detection accuracy.

#4

Zero trust simplifies access control policies, enhances visibility, and improves effectiveness.

Microsegmentation is a core zero trust concept. It involves restricting access to applications and resources so that attackers that breach one can't cause damage to others. In the legacy network-based approach to microsegmentation, firewalls enforced rules by examining network addresses. This approach required oftentimes hundreds, thousands, or tens of thousands of policies to be redefined and updated as applications moved and networks evolved. This was challenging enough in the on-premises data center, but the cloud's ephemerality has increased its complexity to the point that it's unmanageable.

By providing a single policy set and enforcement mechanism, proxy architectures greatly reduce the complexity involved in implementing microsegmentation while providing more robust protection for workloads. Because policies and permissions are managed on the basis of resource identities, they're independent of the underlying network infrastructure and can automatically adapt—no matter how dynamic the network's architecture is or how rapidly business requirements change. This also simplifies management—you can protect a segment with just a few identity-based policies instead of hundreds of address-based rules.



#5

A zero trust architecture protects users and devices wherever they are.

With the need to enable work from anywhere, many organizations have turned to virtual private networks (VPNs) or remote desktop protocol (RDP) to enable employees working from home to connect to corporate networks and resources. Unfortunately, ransomware operators quickly followed in these organizations' footsteps, launching a new wave of RDP– and VPN–based attacks. In fact, a VPN was exploited in the now–infamous Colonial Pipeline attack that halted the transport of nearly half the fuel supply in the eastern US.

In a zero trust–based approach to securing remote users, every connection gets identical protection, regardless of where users are located. Adding a lightweight endpoint agent, Zscaler Client Connector, to every remote user's device gives them access to all the security, policy enforcement, and access controls available through the Zscaler Zero Trust Exchange. And because Zscaler is distributed across 150 data centers around the world, users always get a fast connection through a nearby data center, eliminating the inconvenience of VPN latency.

#6

A true zero trust architecture makes it impossible for attackers to move laterally across your network.

Far too many security teams continue to rely on legacy firewall–based network segmentation to keep malicious traffic out of corporate networks. These strategies are not only complex to deploy and manage, but they still leave internal resources exposed. If attackers successfully breach an application or firewall, they still have opportunity to move laterally across the environment—which allows attackers to encrypt and steal much more data than they could otherwise.

A true zero trust approach connects a user directly to the application that they need in a 1:1 segment, without ever exposing the network. Security teams can use a proxy architecture to continuously authenticate users and connect them directly to applications rather than trusting traffic from an internal network or subnet, eliminating the biggest digital risk that today's businesses face. And best of all, a proxy works no matter where your users, devices, or applications reside, providing secure connectivity both on–premises and off.

#7

A zero trust architecture keeps attackers from exploiting workloads.

In a zero trust architecture, security policies are enforced in accordance with the identity of the workloads that are attempting to communicate with one another. These identities are constantly being verified; workloads that are unverified are blocked from communicating with others. This means they can't interact with malicious remote command-and-control servers or with internal hosts, users, applications, and data.

A platform like the Zscaler Zero Trust Exchange automatically ensures that all traffic—regardless of where it originates—will adhere to all corporate policies when accessing your resources. It will apply these policies in an entirely uniform fashion, no matter if the resources in question are internal, external, or third-party SaaS. This is a much simpler approach to network microsegmentation than multilayered policy enforcement, but it's also more effective.

#8

Zero trust includes proactive strategies to beat adversaries at their own game.

Today's ransomware operators are sophisticated foes who are capable of bypassing initial prevention. Thus, a key aspect of zero trust is employing strategies to find and isolate attacks before they can cause damage. As the world's only zero trust platform that integrates deception capabilities, Zscaler Deception™ uses advanced deception tactics to lure, detect, and intercept attackers, no matter how advanced or targeted their strategies are.

This proactive approach to defense involves populating your IT environment with decoys, such as fake endpoints, directories, databases, files, and user paths. These decoys mimic high-value production assets, but they remain hidden from real users. Their sole purpose is to alert your security team to the presence of an adversary when they're touched. As there is no legitimate traffic to the decoys, alerts are extremely high-fidelity, providing solid evidence of a threat or breach that rises above the noise of other detection systems. This gives your security team an advantage, allowing them to disrupt adversaries' playbooks and mitigate damage.

#9

Zero trust architectures provide comprehensive protection against data loss.

The increasing prevalence of double-extortion ransomware attack strategies has made it necessary to consider every ransomware attack a data breach. Measures that prevent exfiltration and publication of your sensitive data will go a long way when it comes to mitigating the most devastating consequences of a ransomware attack.

Using a cloud access security broker (CASB) solution enables you to enforce granular controls over your cloud applications, protecting data at rest within SaaS platforms and preventing accidental oversharing as well as malicious acuity. An added benefit is that you'll enjoy enhanced visibility your cloud applications, making it easy to identify vulnerabilities, misconfigurations, and shadow IT—the use of unsanctioned cloud apps. With data loss prevention (DLP) capabilities, you'll be able to block data exfiltration automatically, curtailing the double-extortion threat.

#10

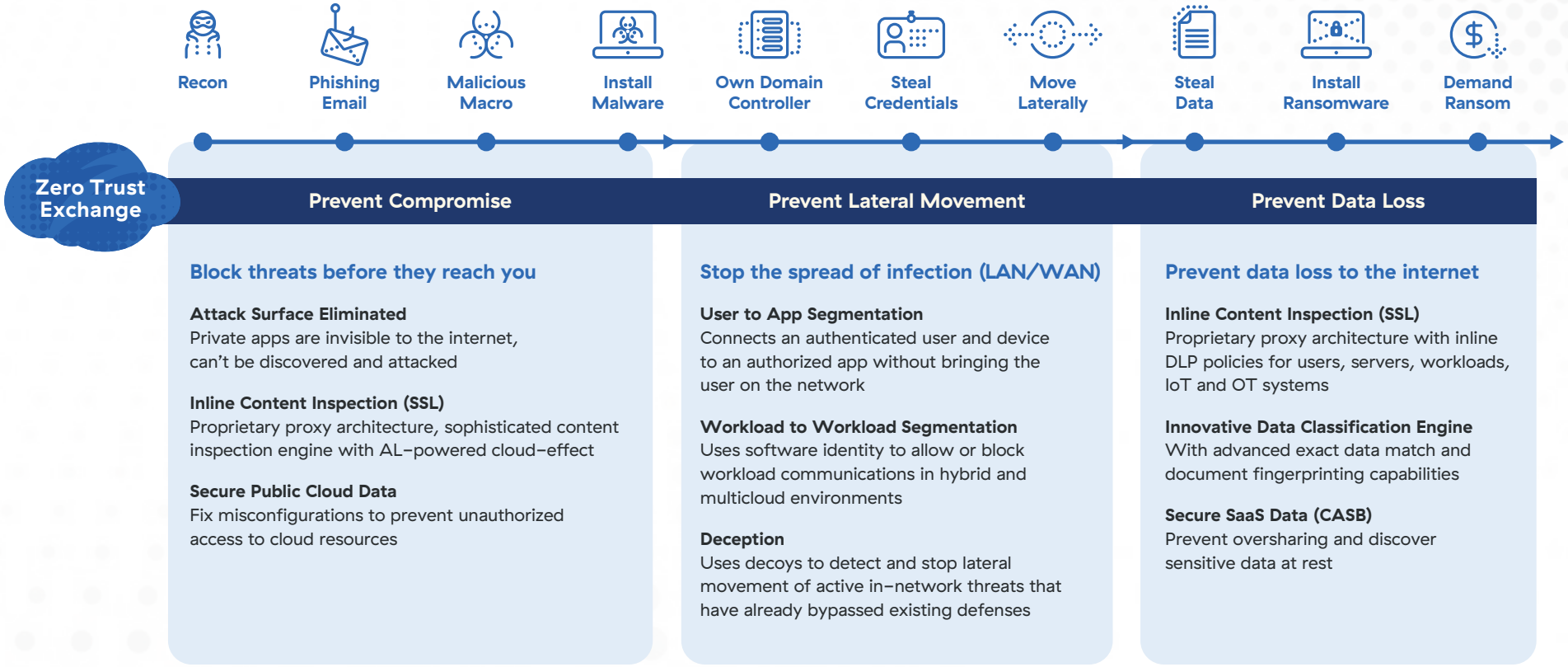
With full inline inspection of all outbound traffic, a zero trust architecture enables you to bring data theft to a halt.

If bad actors hide malware in SSL–encrypted inbound traffic, they can make use of the same strategy—leveraging encryption—to conceal the fact that they're exfiltrating sensitive and valuable corporate data. Being able to inspect SSL–encrypted traffic is critical to preventing data loss and identifying zero–day data exfiltration vulnerabilities.

A zero trust architecture–based solution such as the Zscaler Zero Trust Exchange ensures that every connection in your environment will be verified and secured individually, regardless of whether it's inbound or outbound. With a cloud–native proxy architecture, it's possible to perform SSL inspection at scale without impacting performance or incurring excessive costs. This eliminates the security gaps that ransomware operators have exploited to launch devastating double–extortion attacks.

Operationalize zero trust to protect against ransomware

The Zero Trust Exchange offers the most comprehensive defense against the full sequence of steps that attackers must take to succeed. See how Zscaler uses zero trust to deliver unmatched protection for your organization.



Stopping modern attacks requires modern security.

Safeguard your enterprise with the industry's most comprehensive ransomware defense.

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

Verify identity and context

When a connection is requested, the zero trust architecture terminates the connection and verifies identity and context:

1. **Who is connecting?** — Verifies the user/device, 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, and location.
3. **Where is the connection going?** — Confirms that the destination is known, understood, and contextually categorized for access.

Control content and access

Next, the zero trust architecture evaluates the risk associated with the connection request, and inspects traffic for cyber threats and sensitive data:

4. **Assess risk** — Leverages AI to dynamically compute a risk score of the requested access.
5. **Prevent compromise** — Inspects inbound traffic to identify and block malicious content.
6. **Prevent data loss** — Decrypts and inspects outbound traffic and content to prevent exfiltration of sensitive data.

Enforce Policy, per-session decision and enforcement

After controlling for risk, policy is enforced before ultimately establishing a connection to the internal or external application:

7. **Enforce policy** — 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. For internal apps, this is an encrypted, outbound-only tunnel that eliminates any attack surface.