White Paper

Implementing the NIST Zero Trust Architecture with Zscaler

© 2022 Zscaler, Inc. All rights reserved.

White Paper

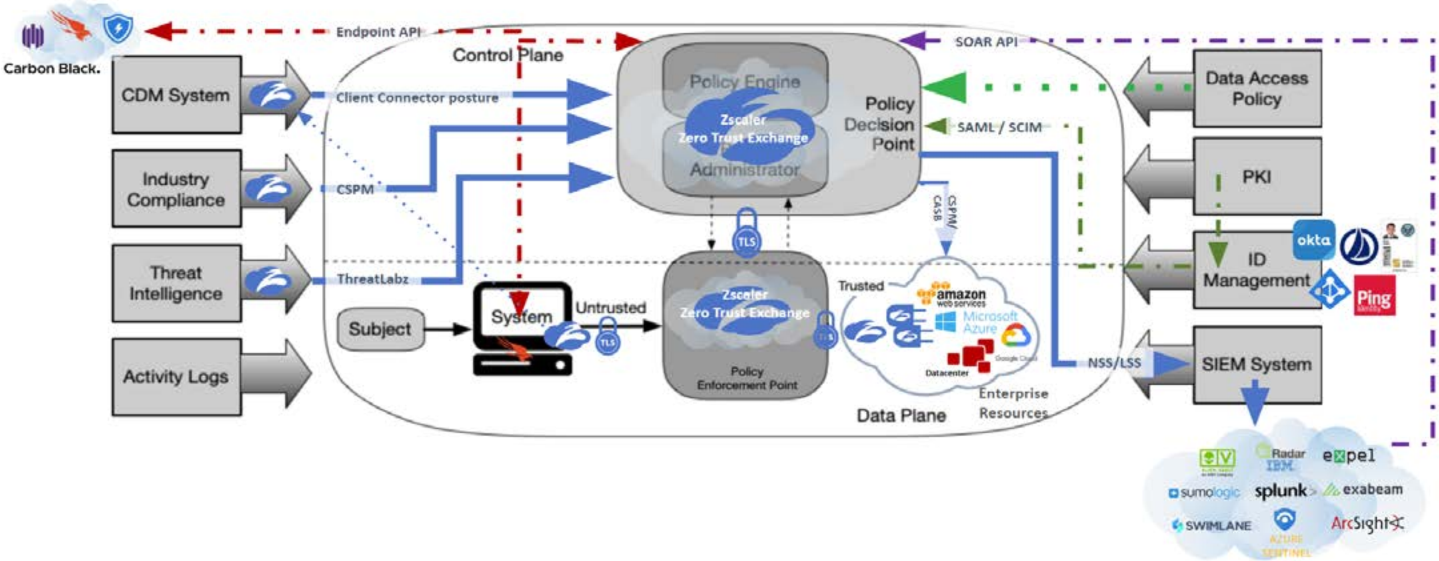
Implementing the NIST Zero Trust Architecture with Zscaler

The National Institute of Standards and Technology (NIST) has defined the core components of zero trust principles in Special Publication 800-207. This document supports the drive toward zero trust as the security standard in government as outlined in the Executive Order on Improving the Nation's Cybersecurity.

© 2022 Zscaler, Inc. All rights reserved.

Zscaler is proud to be a key collaborator in helping government and industry implement zero trust architecture (ZTA). The Zscaler Zero Trust Exchange enables fast, secure connections for employees to work from anywhere without having to access the enterprise network. Based on the zero trust principle of least-privileged access, it provides comprehensive security using context-based identity and policy enforcement.

Our solutions are aligned with the seven tenets of zero trust and provide core components. Policy engine (PE), policy administrator (PA), and policy enforcement point (PEP) all reside in the Zscaler cloud; PE and PEP can be virtualized to run locally in the enterprise environment, as well. Zscaler integrates with existing data sources, including direct integration with IdP, SIEM, PKI, and compliance solutions (such as EDR). Zscaler also has indirect integration with CDM and threat intel solutions.



NIST Special Publication 800-207, Zero Trust Architecture https://doi.org/10.6028/NIST.SP.800-207, Page 9

Zscaler aligns with NIST's identified architecture approaches and deployment models. Most importantly, the Zero Trust Exchange enables all of the use cases highlighted in the NIST guidance.

Enterprise with satellite facilities

For scenarios where geographically dispersed users have to access a headquarters-based physical network, Zscaler allows those users to access the enterprise resources they need without having to access the network. The Zero Trust Exchange provides users with fast and secure access to internally-managed apps in the data center and public clouds. For users, Zscaler offers a seamless experience. There's no need to fire up a VPN for application access; you just go to the application and it works. The access infrastructure is not exposed, so targeted and DDoS attacks are impossible. And, because users are never placed on the network, Zscaler reduces the risk of lateral movement and the spread of malware.

Multi-cloud/cloud-to-cloud enterprise

Since most organizations utilize multiple cloud providers, the ability to simultaneously connect users to applications in multiple clouds — as well as traditional data centers — is critical. Zscaler enables a multi-cloud environment while reducing the complexity that architecture introduces, eliminating the single ingress point and internal backhauling required by legacy access solutions. It enables continuous inventory, monitoring, and automatic remediation of all cloud services, and it also provides an easy way to deploy and configure cloud-to-cloud and app-to-app communication.

© 2022 Zscaler, Inc. All rights reserved.

Enterprise with contracted services and/or non-employee access

For organizations with on-site, non-employee users that need access to enterprise resources, Zscaler can allow micro-segmented access from any visiting party to only authorized applications. The Zero Trust Exchange makes enterprise resources invisible to unauthorized users, while allowing application access based on identity, context, and policy.

Collaboration across enterprise boundaries

A zero trust approach can better enable cross-agency collaboration, allowing separate organizations to share needed data without opening up their entire network. The Zero Trust Exchange modernizes the collaboration playbook with our software-delivered zero trust approach. On the industry side, key business processes can be enabled immediately following a merger or acquisition, without the overhead in time, cost, and complexity of traditional approaches. There is no need for complex network integration and the resulting potential risk exposure – connect key users directly to critical applications on both sides.

Enterprise with public- or customer-facing services

To achieve customer/citizen service goals, agencies can implement zero trust practices to ensure authorized users have access to all of the services they need. The Zero Trust Exchange provides a simple, seamless, and secure customer experience – without requiring those services to be fully public or exposed to unauthorized users.

To meet these diverse use cases, Zscaler supports various approaches to enacting ZTA workflows, including the NIST-identified enhanced identity governance, microsegmentation, and software-defined perimeters. In addition, the Zero Trust Exchange maps to multiple deployment models. Zscaler's Client Connector enables device agent/gateway-based and enclave-based deployment, while clientless browser-based access enables resource portal-based deployment.

Zscaler utilizes criteria-based trust algorithms and independent control plane/data plane to control data flow and access. Security is maintained through continual mitigation of threats with special attention given to subversion of the decision process, denial of service, insider threat, network visibility, and storage of metadata and policies.

In addition, the Zero Trust Exchange is not limited to the basic NIST ZTA framework; it offers zero trust protection not only for users, but also for workloads and Internet of Things (IoT) / Operational Technology (OT) environments. Advanced features such as active defense and dynamic risk scoring augment the zero trust policy decision and enforcement capabilities, providing a comprehensive modern toolset for cybersecurity.

Zero trust is the right direction for both public and private-sector systems, and the practice will continue to evolve to meet the threat landscape. The Zscaler Zero Trust Exchange was designed for this moment, a time when organizations need to focus on protecting resources, rather than just network segments. To learn more, visit https://www.zscaler.com/platform/zero-trust-exchange

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**.

© 2022 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at **zscaler.com/legal/trademarks** are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.