CISA Zero Trust Maturity Model Whitepaper

WHITEPAPER

Executive Summary

In today's rapidly evolving cybersecurity landscape, organizations face a growing range of sophisticated threats. Traditional perimeter-based security models are increasingly ineffective in securing networks, as digital transformation accelerates and work everywhere becomes the norm. Cybersecurity must evolve to protect data and systems regardless of where the users or devices are located. In response to these challenges, the Cybersecurity and Infrastructure Security Agency (CISA) has developed a Zero Trust Maturity Model to guide organizations in adopting and implementing Zero Trust principles effectively.

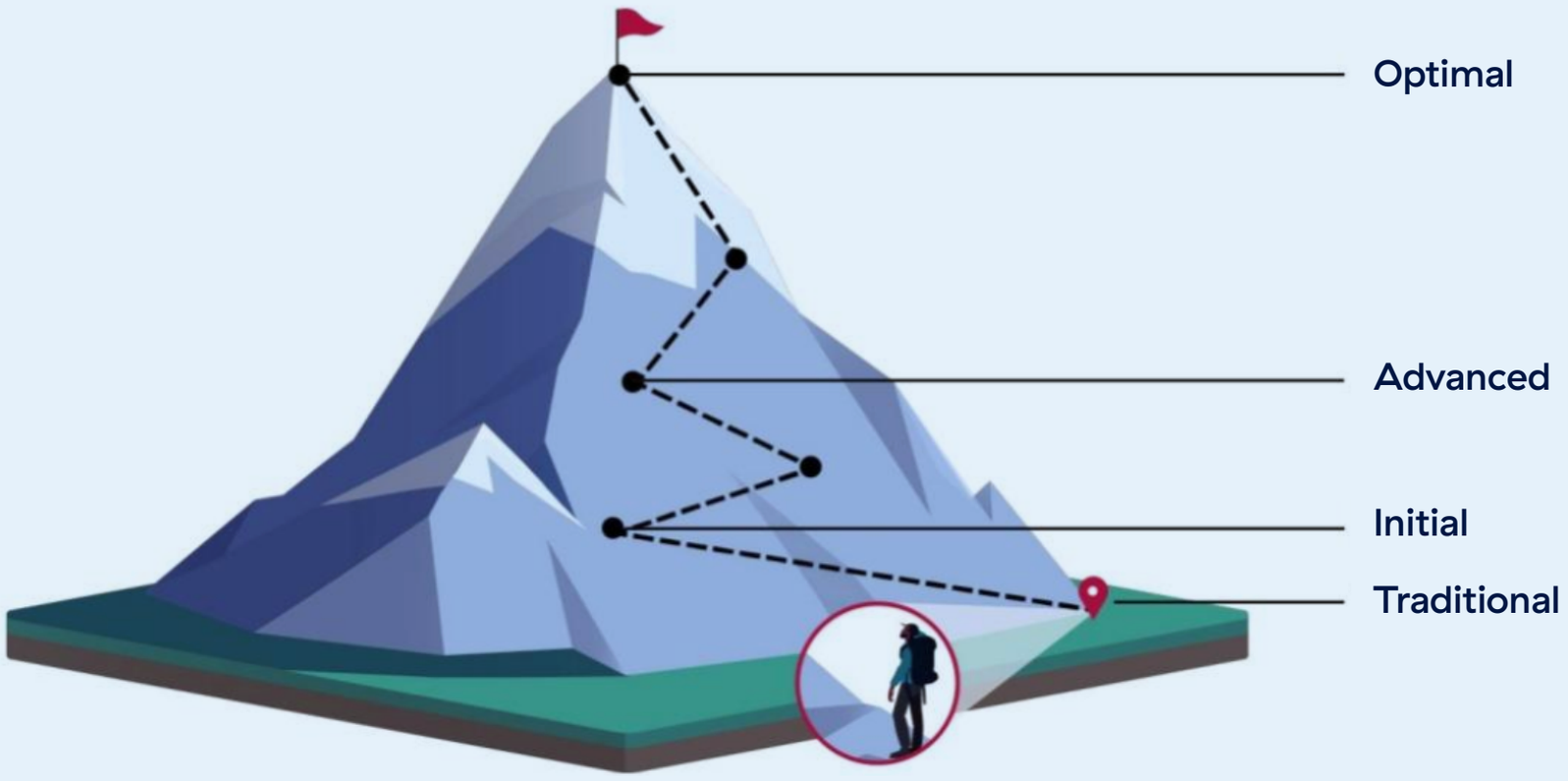
What is Zero Trust?

Zero Trust is a security model that operates on the assumption that threats could be internal or external, and therefore, no user or device should be trusted by default. Every request for access—whether from inside or outside the network—is rigorously authenticated, authorized, and continuously monitored. The Zero Trust framework focuses on ensuring that security is maintained throughout an organization's infrastructure, with a heavy emphasis on identity, access management, and real-time monitoring.

What is the CISA Zero Trust Maturity Model?

The CISA Zero Trust Maturity Model provides organizations with a framework for progressively adopting and maturing Zero Trust principles. This model outlines a phased approach to implementing Zero Trust across an organization, from initial awareness and planning to fully mature, integrated security operations. It provides a structured method for understanding where an organization stands in its Zero Trust journey and what steps it should take next to improve security.

Zero Trust Maturity Journey



Source: CISA

The CISA model divides Zero Trust into several key areas, including identity and access management, device security, network security, data security, application security, and visibility and analytics. The maturity model helps organizations assess their current capabilities in each of these areas and define a clear path to strengthen their security posture. Organizations are gauged against four stages of maturity (traditional, initial, advanced, and optimal), with each stage requiring a greater level of protection, with exponential growth in efforts and benefits.

CISA's Zero Trust Maturity Model is increasingly being leveraged as a global benchmark for Zero Trust implementation. International governments, including the UK and Australia, have aligned their cybersecurity strategies with the Maturity Model recognizing its structured approach to advancing Zero Trust capabilities. Beyond governments, the Cloud Security Alliance has also mapped its Zero Trust Advancement Center to the Maturity Model, further reinforcing its role as a common framework for organizations worldwide. As Zero Trust adoption grows, the Maturity Model provides a shared language and maturity roadmap, helping both public and private sector entities assess their progress and refine their security strategies.

KEY COMPONENTS OF THE MODEL

1. **Identity and Access Management (IAM):** Establishes strong authentication mechanisms, such as multi-factor authentication (MFA), to verify user identities before granting access.

2. **Device Security:** Ensures that devices are secure, managed, and compliant with security policies before accessing organizational resources.

3. **Network Security:** Implements segmentation and monitoring to restrict lateral movement and detect suspicious activities within the network.

4. **Data Security:** Protects sensitive data by applying encryption, strict access controls, and monitoring data usage.

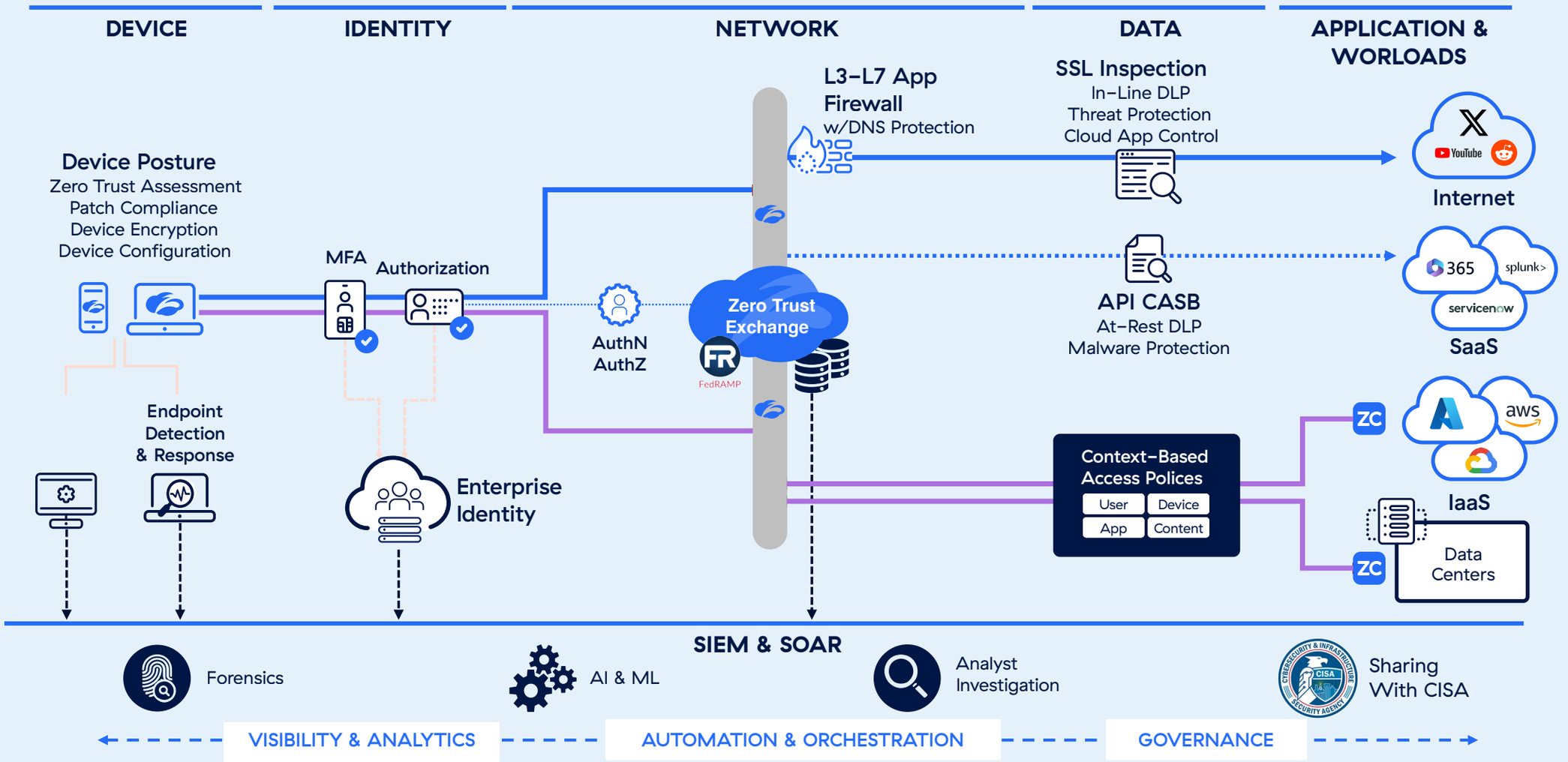
5. **Application Security:** Ensures that applications are secure by implementing secure development practices, continuous monitoring, and vulnerability management.

6. **Visibility and Analytics:** Enhances situational awareness by continuously monitoring all traffic and events, identifying anomalous behavior, and providing real-time alerts.

7. **Automation & Orchestration:** Integrates and automates systems to improve the effectiveness and efficiency of cyber systems.

8. **Governance:** Establishes policies, procedures and oversight mechanisms to ensure effective implementation.

Zero trust maturity model 2.0



Implementing the CISA Zero Trust Maturity Model with Zscaler

Implementing Zscaler ZTE immediately enhances your security posture by shifting from traditional perimeter-based security to a more comprehensive, layered defense. By continuously verifying users, devices, and data, organizations can reduce the risk of data breaches, insider threats, and external attacks. This approach minimizes the attack surface and prevents lateral movement of attackers. Zscaler also enables organizations to advance their CISA Zero Trust Maturity Model strategy by providing robust products and features that support the key areas, including identity and access management, device security, network security, data security, application security, and visibility and analytics.

IDENTITY

- **Least-Privileged Access:** Zscaler minimizes over-permissioned accounts by enforcing granular, role-based access controls (RBAC) and contextual policies (e.g., user location, device posture).

- **Single Sign-On (SSO) and Multi-Factor Authentication (MFA):** Zero Trust policies are bolstered with SSO/MFA integration, ensuring strong authentication and reducing the risk of credential compromise.

- **Continuous User Monitoring:** ZTE ensures users are continuously authenticated and their behavior is monitored to mitigate risk.
- **Integration with Identity Providers (IdPs):** Zscaler integrates seamlessly with leading identity providers like Okta, Microsoft Azure AD, and Ping Identity to enforce strong user authentication and authorization policies.

DEVICES

- **Device Posture Checks:** Zscaler uses integrations with endpoint detection and response (EDR) tools to perform posture checks and ensure only secure, managed devices can access sensitive resources.
- **Agent-Based Enforcement:** Zscaler's lightweight Zscaler Client Connector (ZCC) software agent ensures all user traffic is routed through the Zscaler security cloud, enabling visibility and consistent enforcement of security policies.
- **Zero Trust for IoT/Unmanaged Devices:** Zscaler solutions include capabilities to control access by unmanaged devices—including IoT—using behavioral policies and granular access controls.

NETWORK

- **Zero Trust Network Access (ZTNA):** Zscaler Private Access (ZPA) replaces traditional VPNs with ZTNA. Users are granted "least-privileged" access to specific applications, not the entire network.
- **Secure Access Service Edge (SASE):** Zscaler meets SASE architecture requirements by delivering scalable security services, such as Secure Web Gateways (SWG) and Cloud Firewall, across distributed environments.
- **Microsegmentation:** Zscaler ensures that users and workloads are segmented at the application level, minimizing lateral movement in the event of a breach.
- **End-to-End Encryption Monitoring:** Zscaler inspects encrypted internet traffic via SSL/TLS interception without compromising performance or privacy.

APPLICATIONS AND WORKLOADS

- **Application Segmentation:** Zscaler ZPA provides application-based segmentation rather than traditional network segmentation, enabling direct, secure, user-to-application connections.
- **Workload Security:** Zscaler Workload Segmentation (ZWS) secures communications between workloads in public and private cloud environments by ensuring "identity-based microsegmentation."
- **Continuous Monitoring:** Application-level monitoring tracks user activity and access patterns for anomalies, ensuring compromised accounts cannot escalate privileges.
- **SaaS Security:** Zscaler's Cloud Access Security Broker (CASB) controls access to sanctioned and unsanctioned SaaS applications, preventing unauthorized data access and usage.

DATA

- **Data Loss Prevention (DLP):** Zscaler's cloud-based DLP helps protect sensitive data across email, web, SaaS, and private applications. It identifies and prevents the exfiltration of intellectual property (IP) and personally identifiable information (PII).

- **Cloud Security Posture Management (CSPM):** Zscaler provides insights and remediations to misconfigurations in cloud data storage systems, reducing exposure risks.

- **Encryption Control:** Zscaler enforces strict encryption protocols for both data-in-transit and at-rest, ensuring that sensitive information is safeguarded end-to-end.

- **Shadow IT Discovery:** Zscaler CASB identifies and limits the use of unapproved or high-risk apps/services, protecting data from accidental leakage or malicious misuse.

GOVERNANCE, VISIBILITY, AND ANALYTICS, AUTOMATION & ORCHESTRATION

- **Centralized Security Management:** The Zscaler Zero Trust Exchange offers a single-pane-of-glass view of traffic, policies, and security incidents.

- **Integrated Security Analytics:** Zscaler provides real-time visibility into user and application activity through advanced dashboards and logs, integrating with SIEM/SOAR platforms for streamlined incident response.

- **Threat Intelligence:** Zscaler leverages global threat intelligence and behavior analytics to proactively detect and respond to threats across the ZT fabric.

- **Policy Enforcement:** Zscaler automates policy changes and compliance checks, ensuring consistent governance across users, apps, and data.

Zscaler's ZT implementation approach and CISA's ZT MM are very similar and align in several key areas, not just the ZT pillars. Zscaler's architecture supports key ZTMM functions such as dynamic policy enforcement, centralized visibility, and adaptive risk-based access controls—critical elements in maturing a Zero Trust strategy. By leveraging a cloud -native, inline approach, Zscaler helps organizations advance their maturity levels outlined in CISA's model, reducing attack surfaces while streamlining secure access.

Strategic Roadmap for Zero Trust Adoption

Both Zscaler Implementation and the CISA Zero Trust Maturity Model offer a strategic roadmap for organizations to follow when adopting Zero Trust principles. We break the implementation process into manageable stages, which allows organizations to set realistic goals and timelines for each phase. This roadmap ensures that organizations take a structured approach to Zero Trust implementation, reducing the risk of gaps or missteps.

Incremental Implementation

Incremental implementation enables organizations to gradually improve their Zero Trust capabilities over time. This phased approach makes it easier to implement Zero Trust without overburdening existing systems or resources. It also allows organizations to monitor progress and adjust strategies as needed. This allows Zscaler to continuously release new products to enhance our customers security posture but also will allow CISA in the future to move the goal posts. What is considered “optimal” today may be “advanced” in the future.

No Organization is Alike

Each organization’s cybersecurity needs and infrastructure are unique. Zscaler’s ZTE implementation and the CISA Zero Trust Maturity Model are flexible enough to be customized to align with the specific goals, challenges, and resources of an organization. Whether an organization has fully embraced Zero Trust or just started on the journey, the model provides the necessary guidance to tailor the Zero Trust framework to fit their requirements.

Measuring Progress and Success

The maturity model includes clear metrics and assessment criteria, which allows organizations to track their progress over time. By measuring success against predefined stages, organizations can identify areas for improvement and ensure they are moving in the right direction toward achieving a mature Zero Trust environment.

Conclusion

The CISA Zero Trust Maturity Model 2.0 provides organizations with a clear, structured framework for adopting and advancing Zero Trust principles. By implementing this model, organizations can significantly enhance their cybersecurity posture, mitigate risks, and ensure compliance with regulatory requirements.

As the threat landscape continues to evolve, the importance of Zero Trust will only increase, making the CISA model a crucial tool for organizations seeking to secure their digital environments against today’s advanced threats. Through strategic, incremental implementation, organizations can adopt Zero Trust in a way that aligns with their specific needs and capabilities, ensuring long-term success in their cybersecurity journey.

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

zscaler™

Zero Trust Everywhere