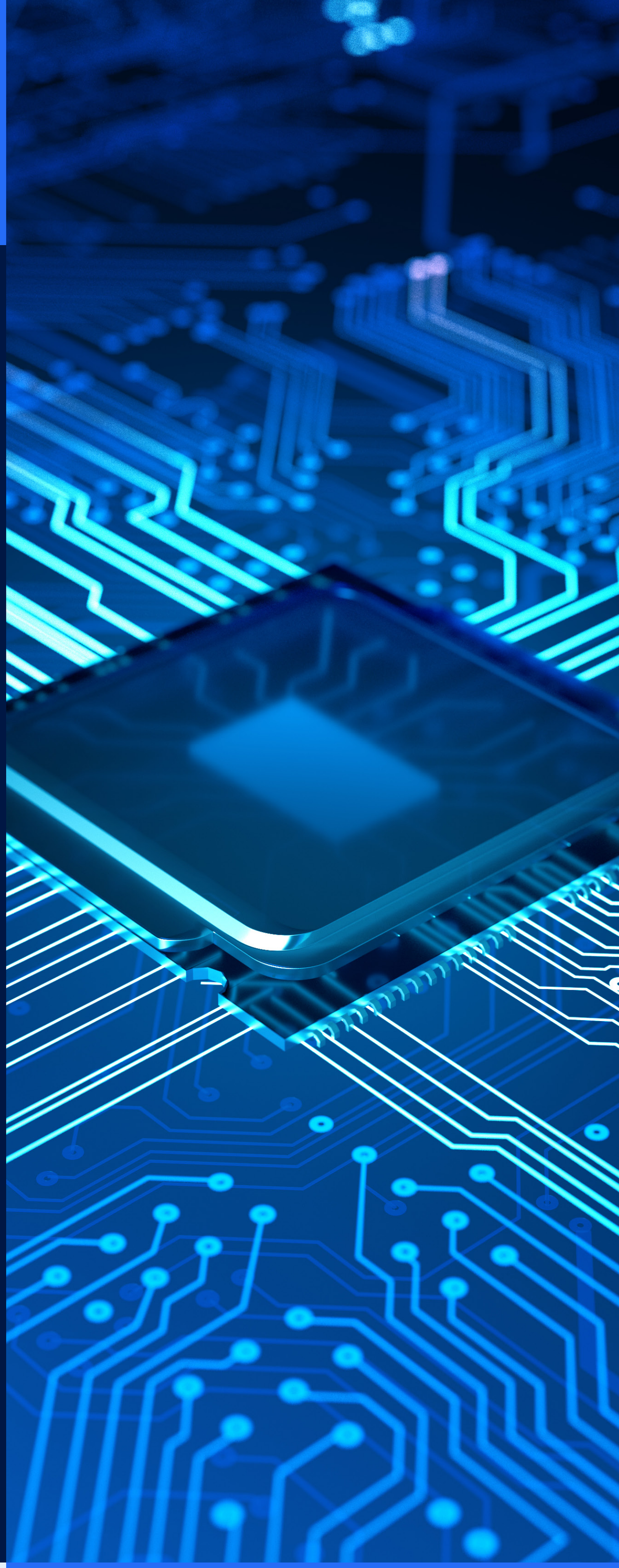
Aligning with the Modern Defensible Architecture

How Zscaler Enables a Zero Trust Foundation



WHITEPAPER

Table of Contents

Foreward

By Sean Connelly

The Australian Signals Directorate's Foundations for Modern Defensible Architecture (MDA) arrives at a critical moment. Threat activity is accelerating, environments are increasingly distributed, and legacy perimeter-centric assumptions no longer reflect operational reality. The MDA acknowledges this shift and provides an architectural foundation—grounded in layered design, traceability, and security-by-design—to help organisations build systems that are defensible by default.

This paper is intended as a practical companion to the MDA. It translates the MDA's core principles—layered and traceable architecture, comprehensive Zero Trust, and secure-by-design thinking—into concrete implementation considerations that organisations can use as a starting point for their Zero Trust journey. The intent is not to reinterpret the MDA, but to demonstrate how its principles can be operationalised in modern, cloud-first environments.

Through leading U.S. Federal Zero Trust initiatives, and as a co-author of NIST SP 800-207 (Zero Trust Architecture) and the DHS/CISA Zero Trust Maturity Model, I have seen that the most successful programmes treat Zero Trust not as a collection of controls, but as an operating model—anchored in architecture and measured through outcomes. Zscaler was built for this shift. The Zscaler Zero Trust Exchange connects users directly to applications rather than networks, continuously evaluates access using contextual signals, and reduces attack surface through least-privileged, policy-driven controls—helping organisations apply the principles of the MDA with speed, consistency, and scale.

Sean Connelly is a Senior Director for Governance, Risk and Compliance at Zscaler. Prior to Zscaler, Sean spent 11 years at CISA and co-authored NIST SP 800-207 – Zero Trust Architecture, CISA's Zero Trust Maturity Model and many other federal IT guidance documents.

Executive Summary

The Foundations for Modern Defensible Architecture (MDA) establishes a critical framework for organisations navigating today's complex and rapidly evolving cyber threat landscape. It champions a strategic, layered approach built upon the core principles of Layered Architecture, comprehensive Zero Trust, and Secure-by-Design methodologies. Zscaler's Zero Trust Exchange platform is a natural and foundational enabler for implementing these vital principles. Its cloud-native, "never trust, always verify" architecture fundamentally shifts security from perimeter defense to continuous verification of every user, device, and application interaction. By leveraging Zscaler, organisations can rapidly establish a robust MDA, realising significant benefits including enhanced security posture, streamlined operational efficiency, and dramatically improved resilience against advanced cyber threats.

Overview

The Foundations for Modern Defensible Architecture emphasises a strategic, layered approach to cybersecurity built on Zero Trust principles and Secure-by-Design practices. It defines ten foundational capabilities essential for organisations to achieve cyber resilience and adapt to evolving threats. Zscaler's Zero Trust Exchange platform is uniquely positioned to help organisations implement these foundations by delivering a comprehensive, cloud-native security architecture that inherently aligns with the document's core tenets.

The historical model of network connectivity first and security of the connection second, is no longer fit for a contemporary method of delivering application access. Zscaler's approach fundamentally shifts traditional network security by connecting users directly to applications and continuously verifying every interaction. This "never trust, always verify" model directly addresses the Zero Trust philosophy. Through its various services, Zscaler Internet Access (ZIA) for secure internet and SaaS access, Zscaler Private Access (ZPA) for zero trust access to private applications, Zscaler Digital Experience (ZDX) for endpoint and application monitoring, and the underlying Zscaler Client Connector (ZCC) for device posture, Zscaler provides the necessary components to build a robust and defensible architecture.

Specifically, Zscaler contributes to:

- **Establishing a robust authorisation model:** By integrating with identity providers and leveraging real-time context (user identity, device posture, application, location, threat intelligence), Zscaler continuously evaluates access requests and enforces granular, dynamic policies, fulfilling the requirements for Contextual Authorisation and High Confidence Authentication.

- **Reducing the attack surface:** ZPA eliminates inbound firewall ports and places private applications behind the Zero Trust Exchange, making them invisible to the internet. ZIA provides advanced threat protection for internet-bound traffic, preventing initial access and command-and-control attempts. This directly supports the Reduced Attack Surface and Resilient Networks foundations.

- **Enhancing visibility and control:** Extensive logging, correlation with threat intelligence, and integrations with SIEM/SOAR platforms enable Continuous and Actionable Monitoring. Device posture checks and continuous session evaluation contribute to Secure Endpoints and a Reliable Asset Inventory.

By adopting Zscaler, organisations can accelerate their journey toward a Modern Defensible Architecture, ensuring proactive threat mitigation, simplified operations, and improved resilience against sophisticated cyber threats as described in the document.

Aligning with the Modern Defensible Architecture

The contemporary cybersecurity landscape is characterised by an ever-increasing sophistication and volume of threats, from nation-state actors to organized criminal groups. This escalating complexity necessitates a fundamental shift from traditional perimeter-based defenses to a more proactive and resilient architectural approach. The Foundations For Modern Defensible Architecture provides precisely this blueprint, advocating for a systematic and layered strategy to safeguard critical assets. Zscaler's cloud-native Zero Trust Exchange platform is inherently designed to meet these challenges, offering a robust solution that aligns seamlessly with the document's vision for building a truly defensible architecture in the face of evolving cyber risks.

The Modern Defensible Architecture (MDA) is built upon three pillars:

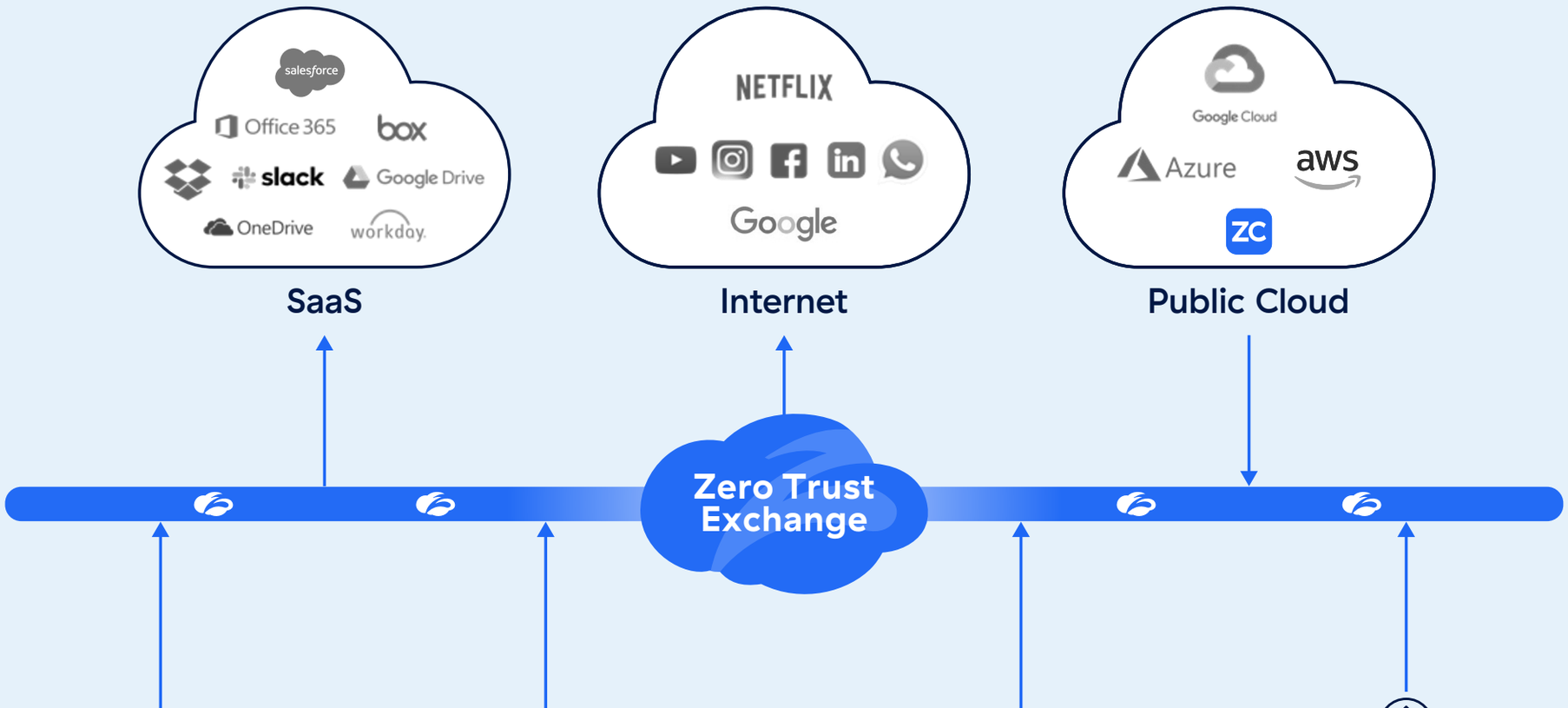
- a Layered Architecture and Traceability, ensuring security controls are directly linked to business objectives;
- a comprehensive Zero Trust model, embodying the principles of "never trust, always verify," "assume breach," and "verify explicitly"; and
- a Secure-by-Design philosophy, integrating security from the outset of all development and operational processes.

These pillars are further elaborated through ten foundations designed to create an environment of continuous security validation and adaptation. Zscaler's Zero Trust Exchange is not merely a collection of security tools; it is an architectural paradigm that natively implements these MDA pillars, providing a unified platform for enforcing Zero Trust access, securing all traffic, and enabling a secure-by-design posture across the enterprise.

Central to the MDA is a sophisticated authorisation model that moves beyond static permissions to dynamic, continuous validation. This model relies on Policy Enforcement Points (PEPs) to gate access, Policy Decision Points (PDPs) to make real-time judgments, and Policy Information Points (PIPs) to gather crucial context. These decisions are informed by a spectrum of "confidence signals," including device health, network location, user behavior analytics, and threat intelligence. Zscaler fundamentally enables this advanced authorisation by acting as the PEP, PDP, and PIP for all access. The Zscaler Client Connector (ZCC) and Zscaler Digital Experience (ZDX) gather essential device posture and user experience data, while Zscaler Private Access (ZPA) and Zscaler Internet Access (ZIA) leverage this intelligence, alongside integrated identity providers and real-time threat feeds, to enforce granular, context-aware policies. This ensures that every access request is rigorously verified against a dynamic set of confidence signals, empowering organisations to achieve the precise and continuous authorisation demanded by a modern defensible architecture.

Zscaler's Zero Trust Exchange: A Foundational Enabler for MDA

Zscaler's Zero Trust Exchange represents a paradigm shift from traditional network security, fundamentally embodying a cloud-native, proxy-based architecture. Instead of backhauling traffic to a corporate data center or extending the network perimeter, Zscaler securely connects users directly to the applications and data they need, regardless of location or device. This core principle, connecting users to applications, not the network itself, is the bedrock of Zscaler's Zero Trust implementation. The platform comprises key services like Zscaler Internet Access (ZIA) for securing all internet and SaaS traffic, Zscaler Private Access (ZPA) for providing zero trust connectivity to internal private applications, and Zscaler Digital Experience (ZDX) for monitoring end-to-end user experience. The Zscaler Client Connector (ZCC) acts as the intelligent agent on the endpoint, ensuring all traffic is routed through the Zero Trust Exchange and collecting crucial device context. This distributed, cloud-scale architecture provides comprehensive security and access control without exposing the underlying network.



At its heart, the Zscaler Zero Trust Exchange relentlessly enforces the core tenets of Zero Trust. "Never trust, always verify" is achieved through its inline, full-proxy architecture, which inspects all traffic, both known and unknown, for threats and policy violations before it reaches the destination. This continuous inspection and verification extend to every connection, ensuring that access is not granted implicitly based on network location. The principle of "assume breach" is addressed by Zscaler's advanced threat prevention capabilities, which identify and block malware, ransomware, and zero-day attacks, preventing initial compromise and containing lateral movement even if a breach were to occur. Finally, "verify explicitly" is central to every access decision, leveraging rich context derived from user identity, device posture, application criticality, and behavioral analytics to make granular, real-time access judgments.

This explicit verification directly supports the sophisticated authorisation model advocated by a modern defensible architecture. Zscaler's cloud acts as the Policy Enforcement Point (PEP), intercepting all traffic and access requests. The platform's powerful policy engine functions as the Policy Decision Point (PDP), evaluating requests against centrally defined policies, integrating with identity providers, and consulting various real-time data sources. These data sources, or Policy Information Points (PIPs), include dynamic "confidence signals" gathered continuously: the Zscaler Client Connector (ZCC) provides critical device health and posture information (e.g., OS version, patch level, encryption status, EDR presence); ZPA leverages network context (e.g., geographical location, network segment); and ZDX offers insights into user behavior and application performance. By fusing these dynamic signals, Zscaler ensures that authorisation decisions are not static, but continuously adaptive, enforcing precise access based on the least privilege principle and the current trustworthiness of the user, device, and application context.

Zscaler's Alignment with the 10 MDA Foundations

Foundation 1: Centrally Managed Enterprise Identities

A modern defensible architecture (MDA) emphasizes Centrally Managed Enterprise Identities to minimize authoritative identity sources, streamline identity lifecycle governance, and enforce the principle of least privilege. In today's distributed IT environments, reducing a sprawling array of identity stores is crucial for maintaining security and consistent policy enforcement.

Zscaler's Zero Trust Exchange integrates with authoritative Identity Providers (IdPs) like Azure AD, Okta, and Ping Identity, leveraging them as the single source of truth for user information rather than replacing them. This integration aligns with the MDA's goal of reducing authoritative sources by consuming identity attributes from the established enterprise identity backbone. This enables Zscaler to enforce granular, attribute-based access policies across its platform. When a user attempts to access an internet destination (ZIA) or a private application (ZPA), Zscaler's policy engine utilizes the user's identity and attributes from the IdP to ensure they only access authorized resources based on their role or other contextual data. Identity lifecycle changes in the central IdP are immediately reflected in Zscaler's policy enforcement, ensuring access rights are current and compliant.

Foundation 2: High Confidence Authentication

High Confidence Authentication is essential as credential compromise is a primary vector for cyberattacks. The MDA calls for strong, phishing-resistant authentication for all access events, coupled with cryptographic credential binding to enhance assurance. This moves beyond traditional password-based authentication, which is susceptible to phishing, to methods that verify the user's identity and link that identity to a trusted device or context, reducing the risk of unauthorized access.

Zscaler's Zero Trust Exchange supports High Confidence Authentication by leveraging and enforcing an organization's existing Identity Provider (IdP) for all user authentications. Zscaler integrates with IdP-driven Multi-Factor Authentication (MFA) mechanisms. By directing all user authentication requests to the IdP, Zscaler ensures organizations can deploy and enforce strong, phishing-resistant MFA technologies (such as FIDO2, WebAuthn, hardware tokens, or push notifications) for every user access event.

Beyond user MFA, Zscaler adds device authentication through the Zscaler Client Connector (ZCC). The ZCC establishes a secure, device-bound, and cryptographically protected tunnel to the Zero Trust Exchange. This tunnel acts as a form of cryptographic credential binding, linking the device to the secure access pathway. Before any application access is attempted or authenticated via the IdP, the ZCC ensures that the device is known, trusted, and meets predefined security posture requirements. This dual-layered authentication—strong user MFA via the IdP combined with ZCC's device-bound trust—elevates the confidence in every access request, aligning with the MDA's requirements for high confidence and cryptographically bound authentication.

Foundation 3: Contextual Authorisation

The Modern Defensible Architecture (MDA) is built on Contextual Authorisation, moving past static network-based controls to dynamic, continuous validation. This requires every access request to be evaluated in real-time, considering factors like user identity, device posture, location, behavior, and threat intelligence. The MDA's objective is to ensure access is not a one-time grant but is continuously verified and adjusted based on the evolving risk profile, aligning with the "never trust, always verify" principle to ensure access privileges are responsive to threats and user context.

Zscaler's Zero Trust Exchange is designed to deliver this level of contextual authorisation. The Zscaler Private Access (ZPA) policy engine acts as the central Policy Decision Point (PDP), evaluating every user-to-application request. It gathers context from various sources: user identity from the Identity Provider (IdP); device health and compliance (e.g., OS version, EDR presence) from the Zscaler Client Connector (ZCC); and other context like the application, network location, and time of day. Zscaler also integrates real-time threat intelligence into these decisions. This contextual data allows Zscaler to enforce granular and adaptive policies, aligning with the MDA. For instance, based on the data, Zscaler can dynamically adjust access or impose additional security measures, such as enforcing multi-factor authentication for critical applications accessed from an unusual location. If the device posture degrades, Zscaler can automatically restrict access until the device is remediated. This continuous, adaptive authorisation ensures access is always granted based on the principle of least privilege and the current trustworthiness of the entire user-device-application context.

Foundation 4: Reliable Asset Inventory

The Modern Defensible Architecture (MDA) emphasizes a reliable asset inventory as foundational for effective cybersecurity. In contemporary hybrid IT environments, organizations frequently lack a clear understanding of their digital assets, including hardware, software, applications, and their interdependencies. The MDA aims for comprehensive knowledge of all assets, their criticality, and their dependencies, as protection is impossible without knowledge of what exists. Without an accurate inventory, managing risk, enforcing policies, and responding to incidents is hampered, often resulting in blind spots and unmanaged assets that introduce vulnerabilities.

While Zscaler's Zero Trust Exchange is not a CMDB, it provides critical, real-time data that aids in building and maintaining a dependable asset inventory. Through Zscaler Private Access (ZPA), App Connectors discover and register private applications within the internal network, exposing previously uncatalogued internal services that users access. This capability is important for identifying shadow IT or legacy systems that represent potential risks.

Concurrently, Zscaler Digital Experience (ZDX) offers insights into the endpoints and applications in use by monitoring end-user device performance, application availability, and network paths. The extensive logging and reporting across Zscaler Internet Access (ZIA), ZPA, and ZDX further enrich the asset inventory by meticulously logging every user-to-internet and user-to-private application session. This telemetry details who is accessing what, from where, and on what device. Integrating these logs with a centralized asset management system allows organizations to validate existing inventories, identify discrepancies, discover unknown assets, and gain a more dynamic view of their digital estate. This data enables security teams to enforce policies against unapproved or unmanaged assets, ensuring only known, compliant resources are part of the secure ecosystem, thereby strengthening the security posture and aligning with the MDA's mandate for a reliable asset inventory.

Foundation 5: Secure Endpoints

The Modern Defensible Architecture (MDA) considers endpoints—laptops, desktops, and mobile devices—as critical components because they are frequent targets for attackers and primary points of user interaction. Therefore, Secure Endpoints must be resilient, consistently compliant with security policies, and able to provide contextual information for broader security decisions. MDA mandates moving beyond basic antivirus to a holistic approach where endpoints actively contribute to the overall security posture by verifying their integrity before granting access and continuously monitoring their state to detect and prevent threats.

Zscaler's Zero Trust Exchange integrates the Zscaler Client Connector (ZCC) into its endpoint strategy, making devices active participants in the Zero Trust model. ZCC is an agent deployed on every device to enforce and continuously verify device posture by checking attributes like the operating system version, security updates, disk encryption status, and EDR health. If a device fails compliance, ZCC can restrict access or quarantine the device until it adheres to policy, ensuring only healthy endpoints access resources. Beyond compliance, ZCC establishes an encrypted tunnel to the Zscaler cloud, routing all traffic through the Zero Trust Exchange for inspection, threat detection, and policy enforcement. Device health and compliance data from ZCC feed directly into Zscaler's policy engine for real-time, context-aware authorization. Zscaler Digital Experience (ZDX) further provides ongoing endpoint experience monitoring, offering insights into device performance, application responsiveness, and network connectivity. This approach ensures endpoints are secured, verified, and context-aware elements within the defensible architecture.

Foundation 6: Reduced Attack Surface

The Modern Defensible Architecture (MDA) prioritizes a Reduced Attack Surface, as every exposed element represents a potential vulnerability. Minimizing these exploitable surfaces is a proactive defense strategy. Traditional perimeter security often leaves numerous entry points exposed. The MDA aims to fundamentally shrink this surface area, ensuring that only necessary and securely controlled access points exist, making it harder for attackers to gain an initial foothold.

Zscaler's Zero Trust Exchange delivers on this MDA foundation. Zscaler Private Access (ZPA) makes internal applications "dark" to the internet. Instead of using traditional VPNs or exposing private applications via inbound firewall ports, ZPA establishes only outbound-initiated, authenticated, and encrypted microtunnels from App Connectors to the Zscaler cloud. Users connect via the Zscaler cloud without being on the same network.

This means private applications are never directly exposed, preventing reconnaissance or direct attacks, and mitigating MITRE ATT&CK techniques for Reconnaissance and Initial Access. Zscaler Internet Access (ZIA) further contributes by securing all internet traffic. ZIA inspects all web, SaaS, and cloud traffic inline for threats and policy violations. It blocks access to malicious websites, phishing sites, and prevents exploitation of known vulnerabilities that leverage web channels for initial access. By enforcing granular access policies and scrubbing internet traffic, ZIA reduces the avenues for threats to infiltrate. The combination of ZPA, making private applications invisible, and ZIA securing internet access shrinks the overall attack surface, establishing a more defensible architecture.

Foundation 7: Resilient Networks

The Modern Defensible Architecture (MDA) emphasizes Resilient Networks, defining them as infrastructures tolerant to failures, resistant to attacks, and specifically designed to restrict the lateral and vertical movement of threats. Traditional network architectures, often flat or broadly segmented, allow attackers significant opportunities for internal reconnaissance and rapid lateral propagation once an initial breach occurs. The MDA aims to build networks that can withstand disruption, contain threats, and minimize the blast radius of any successful compromise, ensuring business continuity and data integrity.

Zscaler's Zero Trust Exchange supports network resilience through its globally distributed, cloud-native architecture. The platform spans data centers worldwide, providing redundancy, automatic failover, and scalability, which ensures security services remain available and performant for users, even during regional outages or denial-of-service attacks against the platform. This distributed design eliminates a single point of failure. Furthermore, Zscaler Private Access (ZPA) implements application-level micro-segmentation. Unlike traditional segmentation, ZPA ensures users connect only to the specific applications they are authorized for. This is achieved by establishing secure, outbound-only microtunnels from ZPA App Connectors directly to the Zscaler cloud, which then brokers the connection to the user. Users are never directly placed on the network where the application resides, and there is no direct network routing between applications or between applications and user endpoints. Consequently, if an endpoint or user credential is compromised, an attacker's access is strictly limited to the single application that was initially targeted, effectively eliminating the ability for an adversary to move laterally or vertically across the network, thereby containing the blast radius of a breach and enhancing the network's resilience.

Foundation 8: Secure-by-Design

The Modern Defensible Architecture (MDA) advocates for Secure-by-Design, requiring security principles to be integrated proactively into every stage of hardware and software development. Security should be an inherent quality, engineered into system architecture from conception, rather than a reactive measure. This approach aims to build resilient and secure products, avoiding the costly process of retrofitting security controls, and establishing a culture where security is fundamental.

Zscaler's Zero Trust Exchange is a Secure-by-Design platform . Its global cloud infrastructure is developed and operated with high security standards, including adherence to industry compliance certifications (e.g., ISO 27001, FedRAMP, SOC 2), continuous security updates, and secure coding practices. Zscaler's architecture is built on least privilege, deep packet inspection, and continuous verification, designed to defend against evolving threats. Zscaler also enables customers to adopt these principles by simplifying network security.

Customers can leverage Zscaler as a consistent, standardized security foundation for all access, allowing their teams to focus on building security directly into their applications and business logic. By consolidating security at the cloud edge, Zscaler helps organizations integrate security earlier and more effectively into their development pipelines, aligning with the MDA's emphasis on foundational security.

Foundation 9: Comprehensive Validation and Assurance

The Modern Defensible Architecture (MDA) emphasizes Comprehensive Validation and Assurance, requiring continuous verification that security controls are effective, business objectives are met, and the security posture aligns with organizational and regulatory mandates. This foundation moves beyond theoretical security to demonstrable confidence in an architecture's resilience, necessitating ongoing assurance activities, auditing, measuring, and verifying protective capabilities. Without a constant feedback loop and data-driven validation, the defensibility of an architecture remains unproven.

Zscaler's Zero Trust Exchange provides the visibility and forensic data necessary for comprehensive validation and assurance. By operating as an inline proxy for all user-to-internet (via ZIA) and user-to-private application (via ZPA) traffic, Zscaler generates a detailed log of every transaction and security event. This includes user identity, destination, device posture, location, applied security policies, detected threats, and the action taken. Zscaler Digital Experience (ZDX) also contributes performance and experience metrics, aiding in the validation of business continuity objectives. Zscaler's Nanolog Streaming Service (NSS) facilitates the real-time streaming of these detailed logs to SIEM, SOAR, data lakes, or other analytics tools. This integration allows organizations to centralize, correlate, and analyze security events across their digital ecosystem. This capability is essential for meeting MDA's assurance requirements, enabling robust compliance reporting, facilitating thorough forensic investigations, and providing the data points necessary to continuously measure and demonstrate the effectiveness of implemented security controls against predefined security and business objectives. Zscaler empowers organizations to achieve the comprehensive validation and assurance necessary for maintaining a defensible architecture by providing verifiable proof of its security efficacy and insights into user and application interactions.

Foundation 10: Continuous and Actionable Monitoring

Continuous and Actionable Monitoring is the final cornerstone of the Modern Defensible Architecture (MDA), requiring real-time, automated visibility and rapid response fueled by trusted, high-fidelity inputs. This capability moves beyond passive logging and alerting, demanding a proactive system that can instantly detect anomalous behavior, correlate disparate events, and trigger automated defensive measures. In an environment where threats evolve rapidly, the ability to monitor continuously and respond decisively is paramount to minimizing the impact of any security incident and maintaining a truly defensible posture. It aims to reduce the "mean time to detect" (MTTD) and "mean time to respond" (MTTR) to security threats.

Zscaler's Zero Trust Exchange is fundamentally designed for continuous and actionable monitoring, leveraging its position as an inline security platform that processes all user-to-internet and user-to-private application traffic. From this vantage point, Zscaler generates rich logs and telemetry for every traffic and access event traversing its cloud, including granular details about user activities, application usage, network destinations, device security posture, and security event data.

Zscaler's Nanolog Streaming Service (NSS) enables near real-time, high-volume streaming of these logs to Security Information and Event Management (SIEM) systems, Security Orchestration, Automation, and Response (SOAR) platforms, or data lakes, providing security operations centers (SOCs) immediate access to network and application activity. This data is processed and enriched by Zscaler's integrated global threat intelligence, which continuously analyzes daily transactions to identify emerging threats and anomalous user or device behaviors, enabling real-time anomaly detection. When suspicious activity is identified, Zscaler's platform is engineered for immediate, automated response. This can include dynamically blocking suspicious connections, isolating potentially compromised users or devices, enforcing step-up authentication, or triggering automated playbooks within integrated SOAR systems. This immediate feedback loop from detection to automated action directly contributes to mitigating critical MITRE ATT&CK tactics, empowering organizations to maintain constant vigilance and react decisively against threats, thereby fulfilling the MDA's demand for continuous and actionable monitoring.

Key Benefits of Zscaler for MDA Implementation

By adopting the Zscaler Zero Trust Exchange, organisations gain an ally in their journey toward a Modern Defensible Architecture, reaping benefits that transcend traditional security paradigms. Foremost among these is Accelerated Zero Trust Adoption. Zscaler's cloud-native platform provides a complete and ready-to-deploy Zero Trust framework, allowing organisations to rapidly implement "never trust, always verify" principles across users, devices, and applications without complex network re-architecting, fundamentally transforming their security posture almost immediately.

This architectural shift leads to a Reduced Attack Surface. By making private applications invisible to the internet via ZPA and securing all internet-bound traffic via ZIA, Zscaler eliminates direct exposure of critical assets, preventing reconnaissance and initial access attempts that plague traditional perimeter-based defenses. Concurrently, Zscaler delivers Enhanced Threat Prevention and Data Protection. Its inline, full-proxy architecture provides advanced threat detection, including sandboxing, anti-malware, and phishing prevention, coupled with Data Loss Prevention (DLP) capabilities, ensuring sensitive information never leaves the organization without authorisation and thwarting sophisticated attacks in real-time.

Beyond security, Zscaler's platform Improves User Experience. By connecting users directly to applications, regardless of their location, Zscaler bypasses the latency and bottlenecks associated with backhauling traffic through a central data center or relying on traditional VPNs, providing fast, seamless, and high-performance access. For IT operations, this translates to Operational Simplicity and Scalability. As a cloud-native platform, Zscaler simplifies security management, removing the burden of deploying, patching, and scaling security hardware, allowing organisations to expand their digital footprint globally on demand without compromising security.

Finally, Zscaler provides Comprehensive Visibility and Auditability. Its extensive logging and reporting capabilities across ZIA, ZPA, and ZDX offer granular insights into every user activity, application access, and security event, empowering organisations to meet compliance requirements, facilitate incident response, and continuously validate their security controls. This positions Zscaler as a Future-Proof Security solution; its agile, cloud-delivered model continuously adapts to new threats and evolving technologies, ensuring that the Modern Defensible Architecture remains resilient and effective against the challenges of tomorrow.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform 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 SSE-based Zero Trust Exchange™ is the world's largest in-line 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**

zscaler™

Zero Trust Everywhere