Moving Closer to Zero Trust with Stronger Identity and Access Management

November 04, 2021

Senior Security Consultant

Submitted by Meral Daniel on 4, Nov 2021

Moving Closer to Zero Trust with Stronger Identity and Access Management

Zero trust architecture (ZTA) possesses numerous advantages as a security objective to limit internal and external risks. The problem? Achieving 100% ZTA is nearly impossible due to the considerable undertaking and expense required.

Few, if any, organizations can achieve true 100% ZTA. (Not even the U.S. military can get to 100%.) The goal should be to work *toward* 100% ZTA by building on a foundation of **stringent identity management, verification, and security** with the understanding that incremental changes bring progress.

Good identity and access management (IAM) practices are essential building blocks for allowing only authorized users and devices or machines to access applications and data. In this case, identity spans the full gamut of users, endpoints, and applications and is based on high-assurance digital credentials

The benefits of a zero trust, identity-centric model have the power to transform organizations for the better. They include:

- **Increased productivity**. Legacy remote access services like VPN, VDI, RDS, and DaaS all have limitations and aren’t designed for mobile-first, cloud-heavy

environments, nor do they provide robust security. ZTA allows employees to work much more securely from anywhere.

- **Eliminating passwords.** Credentials-based digital identities based on PKI standards are far more secure than passwords. Digital identities secure users, applications, endpoints, and even IoT devices.

Zero Trust Versus Binary Policies

Today's legacy networks rely largely on static, binary (permit/deny) policies on fixed gateways that determine whether to block or allow traffic. Legacy networks automatically trust traffic originating from hosts in the "private" network, unless a statically defined rule says otherwise. Higher-risk resources—like servers that communicate with the Internet—are isolated into de-militarized zones, where traffic passing to them can be subjected to a higher level of scrutiny.

ZTA, on the other hand, implements the principles of *least privilege*. It scrutinizes each transaction, including users, both source and destination machines, and the context of the transaction itself. Transactions may only occur if their evaluated risk score falls below an established threshold. This risk score is calculated from the point-in-time trustworthiness of each user and machine in the transaction—information which exists in the enterprise's identity management systems.

The Groundwork for ZTA

From an IAM perspective, organizations working toward zero trust should focus on maturing their identity infrastructure with a goal of providing a broad range of functionality.

This involves several traditional functions of an IAM foundation:

- **Lifecycle and governance of electronic identities:** Organizations need effective processes, technologies, and policies to ensure that digital identities used for authentication and authorization are accurate. This can include aligning digital identities with business requirements and managing the automated provisioning, modification, and de-provisioning of digital identities. Governance sets the framework that IAM enforces.

- **Comprehensive data classification:** Data classification is crucial to understanding which digital identities should have access to the organization's most important data. For instance, least privilege zero trust denies *all access* to data without proper credentials and authorization.

- **Verification of access requests:** Misappropriation or misuse of credentials is a common cause of breaches. Technologies such as single sign-on (SSO) and multi-factor authentication (MFA) strengthen an organization's authentication posture and validate the user behind the electronic identity. Policy enforcement should flag any access requests deemed inappropriate as violations, including role- and attribute-based access.

- **Privileged access management (PAM):** PAM puts a set of controls in place to ensure that users only receive the access they need to complete their jobs and to track the use of escalated credentials. Such controls can range from vaulting administrative credentials to blocking escalation of privileges on systems.

- **Role-Based Access Control (RBAC):** Like PAM, RBAC serves zero trust principles by using controls to ensure least privilege and limiting access to users assigned certain roles that align with business requirements.

- **Comprehensive logging and auditing:** An organization's identity management infrastructure can provide a wealth of information for detailed analysis. When combined with telemetry from other sources, logging enables advanced visibility provided by ZTA.

More Information Equals More Protection

In addition to the traditional IAM functions, enterprises need information from various sources to establish risk scores and access parameters. For example, if a device must be "known" in order for it to meet a risk score threshold, companies need precise inventories and device identification methods. Scores should factor in information beyond user identity and source machine, including:

- Device ownership
- Whether the user commonly uses this machine to make a request
- Location of the requesting device
- Time of day

- Other historical, associational, or behavioral factors

Similarly, application risks can be calculated by giving scores for:

- Number of users
- Classification of the data they contain
- Connected or disconnected status (connected applications have lower risk scores)
- Whether access to the application goes through a dedicated IAM team, even for PAM (which would generate a much lower risk score)

Those who prefer to allow users to connect to enterprise assets via personal devices need protocols for evaluating the risks. Because ZTA covers transaction requests made by users, processes, and applications alike, organizations need to consider how they'll manage tokens and APIs required to secure such authentications.

Digital certificates can help with risk evaluation of a specific user or host. For example, a certificate is often used to associate a user with the organization or ownership of a device. Meanwhile, encryption encourages trust of the session itself. Both require infrastructure for managing private keys and certificates.

Moving Closer to Zero Trust

While 100% ZTA isn't realistically attainable, organizations can incorporate IAM principles to take incremental steps toward that goal and considerably reduce their risks.

Stratascale provides expert guidance for this journey, starting with security posture reviews and asset analyses. As a solution- and brand-agnostic advisor, Stratascale helps organizations realize their desired level of security by first maximizing the technology they have on hand. It also steps in to fill any gaps with IAM and PAM solutions that fit your budgets and business requirements. This approach allows organizations to spread the costs and hours needed over a more tolerable time period.

Stratascale focuses on technology as well as methodology to account for the biggest contributor to hacks—the human element. We also help stakeholders understand the importance of patience and perseverance in transforming legacy security models.

Speak with a Stratascale cybersecurity representative today to learn how IAM principles can move your enterprise closer to 100% ZTA without breaking your budget.