What Are Practical Projects for Implementing Zero Trust?

Published 17 March 2021 - ID G00744839 - 4 min read

By Analysts John Watts, Neil MacDonald

Initiatives: Infrastructure Security

Vendor marketing abuses the overloaded term “zero trust” to imply improved security. Security and risk management leaders must move beyond the hype and implement two key projects to reduce risk with least privileged access and adaptive security.

Quick Answer

What are practical projects for implementing zero trust?

- “Zero trust” is an overused, widely misunderstood term used by many organizations.
- The majority of organizations interested in zero trust are in the planning or strategy phase.
- Organizations looking to move to practical implementation should focus on two primary projects: user-to-application segmentation (ZTNA) and workload-to-workload segmentation (identity-based segmentation).

More Detail

Gartner observes, based on client inquiry, that most organizations are in the strategy phase for zero trust. However, “zero trust” is an overloaded term used by vendor marketing as a shorthand for “new and improved” security. Zero trust is seen by many security leaders as a silver bullet, but it does not cover all aspects of threats and security, such as phishing and sensitive data protection. A complete zero trust security posture may never be fully achieved, due to limitations such as legacy applications, organizational resistance, complexity of managing granular security controls and other factors.

However, the term “zero trust” has value as a shorthand way of describing a paradigm where implicit trust is removed from all of our computing infrastructure. Implicit trust is replaced with explicitly calculated, real-time adaptive trust levels for just in time, just enough access to enterprise resources.

There are two primary projects that organizations should focus on when looking to implement zero trust (see Figure 1).
Most zero trust strategies start with networking-related initiatives due to the excessive implicit trust in traditional network security models. Zero trust networking initiatives break into two areas:

1. Front-end network access focused on user-to-application segmentation (ZTNA)
2. Back-end network access focused on workload-to-workload segmentation (identity-based segmentation)

Before starting these projects, a solid identity foundation must be in place.

Federated Identity Systems

Zero trust requires a secure, common federated identity management system. For large organizations, there is unlikely to be a single source of truth for user and machine identity. Security and risk management leaders should:

- Document the existing federation relationships.
- Identify the source of truth for user identities, including the process for third-party identities.
- Define policies where stronger authentication is required (MFA, CAC card, PIN, etc.).
- Develop a standardized way to determine if a given device is managed or unmanaged (e.g., certificates).
- For workloads, define how machine and application identities are established.
- Architect for managing machine identities at scale for container and Kubernetes environments.
Adaptive Access Controls

Adaptive access applies context such as device security posture and location for more granular resource access control. Security and risk management leaders should:

- Require stronger authentication for all remote access and SaaS application access.
- Make context-based access mandatory for all SaaS applications (e.g., cloud SSO or CASB).
- Integrate device security posture assessment into access control decisions.
- Integrate with the federated identity systems to control access on-premises and in the cloud.

After a solid foundation is in place, focus on these projects and critical questions:

User-to-Application Segmentation (ZTNA)

ZTNA reduces excessive implicit trust for access to resources, primarily from remote locations, by employees, contractors and other third parties. Start with a pilot of a ZTNA product. Plan rollouts to the organization by prioritizing contractor and third-party access. Then conduct a proof of concept (POC) to test applications with the ZTNA product, and use observation mode to learn patterns of access by user and role to build policies from there.

Security and risk management leaders should:

- Inventory all instances of VPN that allow access to the network. Replace these over time.
- Identify applications and servers in the DMZ with named sets of users. Replace these over time.
- Make unmanaged device access a mandatory part of the ZTNA architecture.
- Test ZTNA solutions for legacy application compatibility.
- Define policies for combining user attributes and services to enforce who has access to what.
- Determine if an on-premises policy management and policy controller is needed.

Workload-to-Workload Segmentation (Identity-Based Segmentation)

Identity-based segmentation reduces excessive implicit trust by allowing organizations to move individual workloads to a default deny model for communication, rather than an implicit allow model. Implement network segmentation to reduce excessive trust zones, starting with high level segmentation of campus and server networks. Like ZTNA, observation mode will be necessary to learn the patterns of communications by workloads and applications in order to build policies. Then, evaluate machine identity management techniques such as SPIFFE, OpenID Connect and SAML across workloads to support granular segmentation. When starting an identity-based strategy, start with a small collection of critical assets to build initial implementations and expand from there.
Security and risk management leaders should:

- Develop a strategy to address heterogeneous workloads spanning on-premises, hybrid, virtual and container environments.
- Identify workloads that require segmentation using means other than agents, such as network-based or API-based orchestration.

**Recommended by the Authors**

- Market Guide for Zero Trust Network Access
- Three Styles of Identity-Based Segmentation
- Market Guide for Cloud Workload Protection Platforms
- Market Guide for Network Access Control
- IAM Leaders' Guide to Access Management
- Designing Security for Remote-Work-First Enterprises
- Quick Answer: Cost Effectively Scaling Secure Access While Preparing for a Remote Workforce