ManageEngine

NIST'S GUIDANCE FOR A ZERO TRUST ARCHITECTURE

ROADMAP FOR DEPLOYING AN ENTERPRISE SECURITY MODEL

www.manageengine.com/ad360

TABLE OF CONTENTS

Traditional perimeter shortcomings

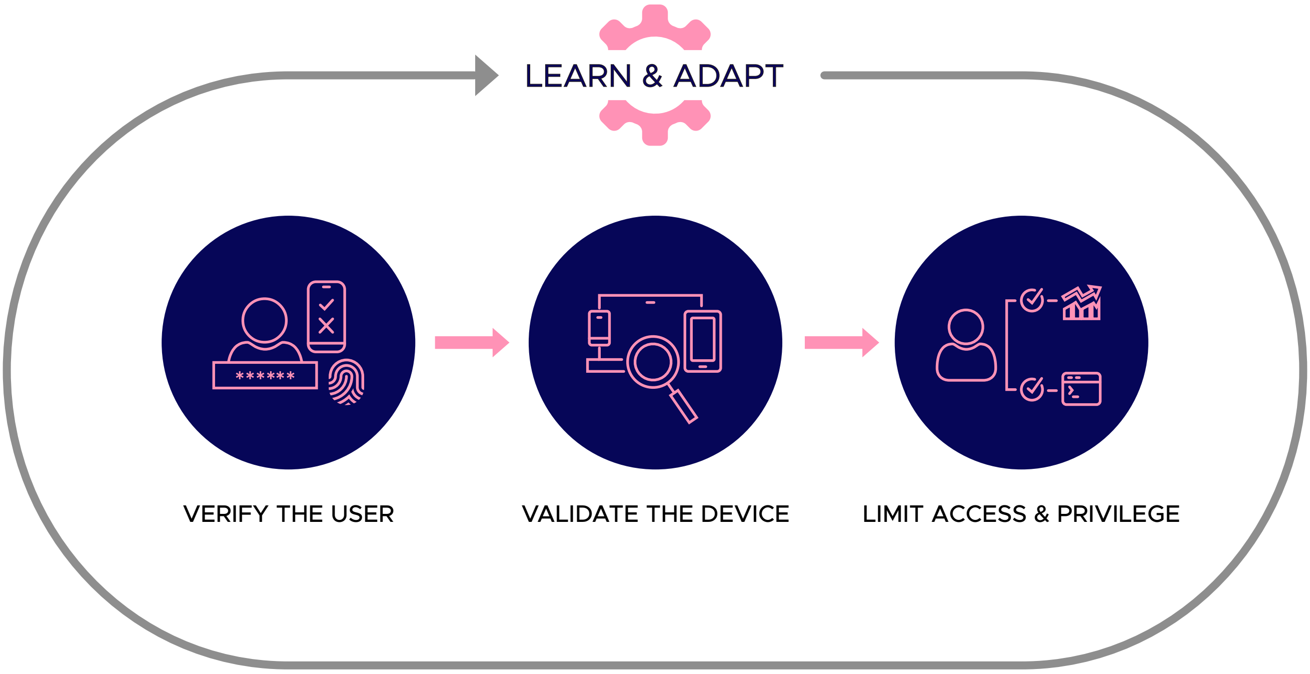
Traditional security methods classify everything (users, devices, and applications) inside the corporate network as trustworthy. These security models use technologies such as virtual private networks (VPNs) and network access control (NAC) to verify the credentials of users outside the network before granting access. With the proliferation of remote work, the new enterprise architecture is redefining the perimeter. Data is stored outside of corporate walls, and users access enterprise applications through various types of devices from locations outside the corporate network.

The Zero Trust model is a response to the fact that the perimeter-based security model doesn't work—innumerable data breaches have occurred because hackers got past corporate firewalls and were able to move through internal business-critical systems easily.

Identity security during remote work means Zero Trust

a. Principle of Zero Trust

The principle behind Forrester's Zero Trust is quite simple but compelling: trust is not an attribute of location. Enterprises shouldn't trust something simply because it is behind an enterprise firewall. Instead, everything including each user, device, and even the network itself should be considered untrustworthy until proven otherwise. Data transfer should occur only after trust has been established through strong authentication and authorization. Additionally, analytics, filtering, and logging should be deployed to monitor insider threats continuously.



b. Challenges addressed by Zero Trust

Insider threat:

Zero Trust can prevent a compromised account or system from accessing resources by enabling MFA for network access. It also uses context to detect any access activity outside of the norm and block account or system access.

Network visibility:

Some encrypted network traffic may be difficult for the enterprise to monitor. In these instances, a Zero Trust approach can help collect encrypted traffic metadata and analyze it to detect malware or attackers on the network.

Policy gaps:

An attacker exploits the gaps between different access policies that apply to the same asset. Zero Trust applies fine-grained contextual access policies, which are dynamically updated to mandate stronger authentication.

Vulnerable endpoints:

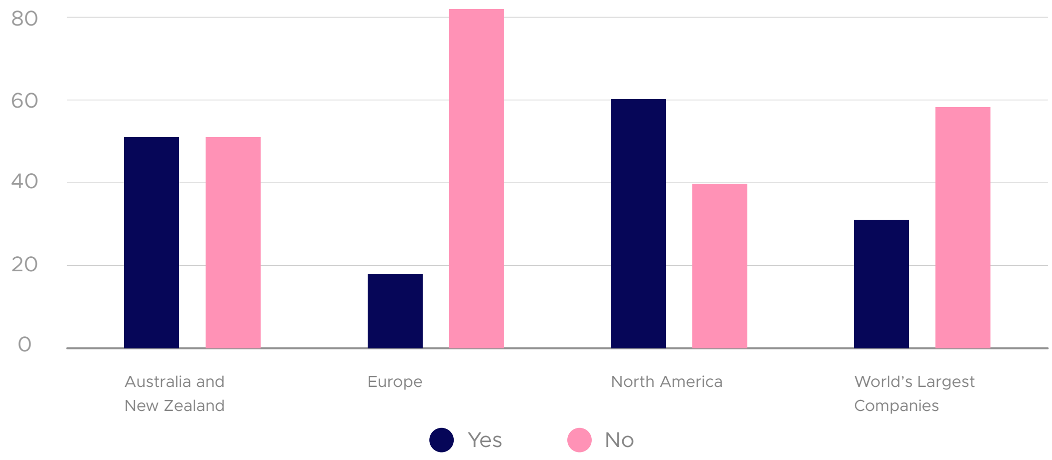
Legacy software containing security flaws is easily exploited by attackers. By splitting an organization's network into segments, Zero Trust reduces the attack surface by protecting the vulnerable systems and preventing lateral movement of threats through the network.

Current state of Zero Trust model with the flood of remote work

a. Zero Trust adoption is on the rise

Organizations are realizing the importance of implementing a comprehensive cybersecurity framework to survive in the future. According to a survey conducted by virtual private networking firm NetMotion Software, more than 70 percent of organizations are considering adopting a Zero Trust model following the pandemic and the shift to extensive remote work. The 2020 Zero Trust Progress Report shows nearly a third of cybersecurity experts expressed interest in applying Zero Trust to address hybrid IT security concerns.

Okta conducted another survey of 500 IT security leaders that shows a massive 275 percent year-on-year growth in the number of North American organizations that have or plan to have a defined Zero Trust initiative in the next 12-18 months.



Okta also found that 60 percent of organizations in North America, and 40 percent globally, are currently working on Zero Trust projects.

b. Zero Trust powers digital transformation

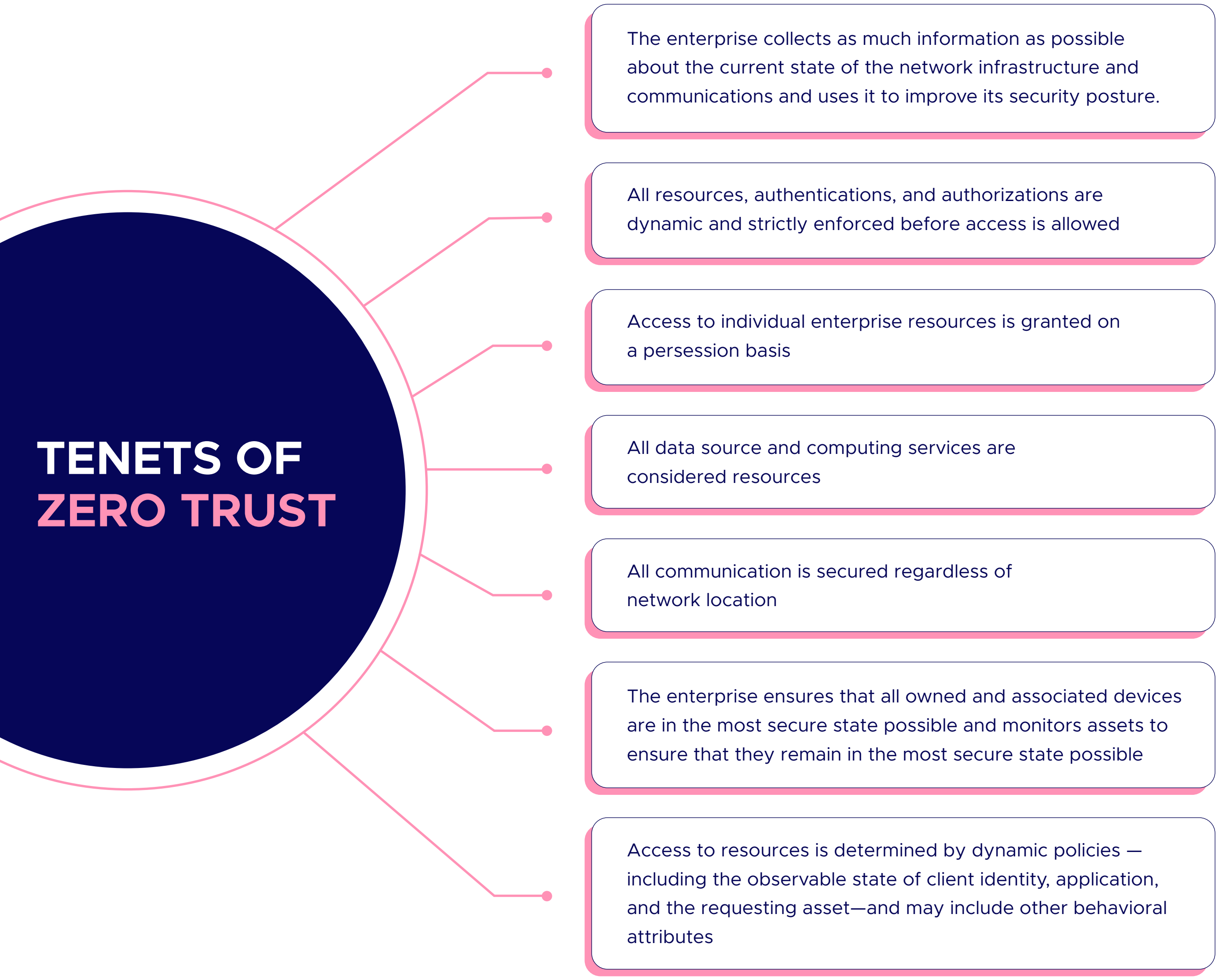
As digital transformation strategies diversify, the risk of privileged credential abuse increases multifold. Forrester estimates that 80 percent of data breaches are caused by privileged access abuse. Enterprises urgently need to replace their legacy identity management approaches to a “never trust, always verify” approach.

IT teams need to improve how they’re protecting the most privileged access credentials by granting just-enough, just-in-time privilege. Of the many cybersecurity frameworks available today, Zero Trust is the most effective, enabling IT to grant the least privilege access to users upon verifying who is requesting access, the context of the request, and sensitivity of the access environment.

Steps to build a Zero Trust model on NIST's Zero Trust Architecture

a. Tenets of Zero Trust Architecture

NIST lists out a few conceptual guidelines that the design and deployment of a Zero Trust Architecture should align with (summarized below):



TENETS OF ZERO TRUST

The enterprise collects as much information as possible about the current state of the network infrastructure and communications and uses it to improve its security posture.

All resources, authentications, and authorizations are dynamic and strictly enforced before access is allowed

Access to individual enterprise resources is granted on a persession basis

All data source and computing services are considered resources

All communication is secured regardless of network location

The enterprise ensures that all owned and associated devices are in the most secure state possible and monitors assets to ensure that they remain in the most secure state possible

Access to resources is determined by dynamic policies — including the observable state of client identity, application, and the requesting asset—and may include other behavioral attributes

You need not comply with all of these tenets. Pick and choose the ones that will make your network more secure.

Here are a few logical points an enterprise implementing a Zero Trust Architecture should consider for network connectivity:

- ✓ Consider the entire enterprise private network insecure. This requires actions such as authenticating all communications and encrypting network traffic before assets are granted access to enterprise-owned resources.

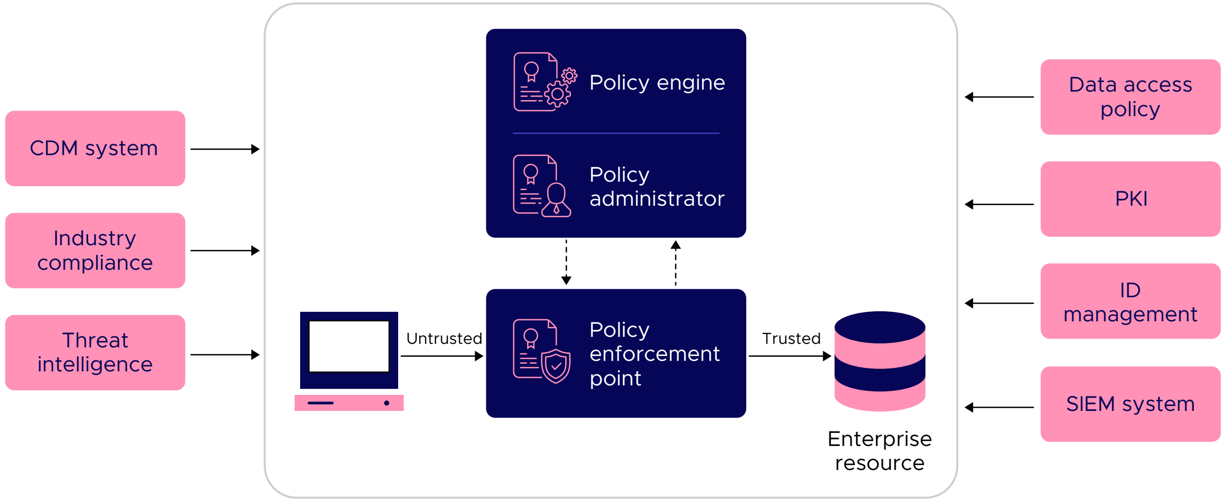
- ✓ With bring your own device (BYOD) policies in place, not all enterprise resources are on enterprise-owned infrastructure. Similarly, not all devices on the enterprise network are owned by the enterprise.

- ✓ Remote subjects should not trust the local (i.e., non-enterprise owned) network. All connection requests should be authenticated and authorized, and all network traffic should be monitored securely.

- ✓ Assets and workflows migrating form enterprise on-premises data centers to non-enterprise cloud instances should follow access policies and maintain proper security posture.

- ✓ Identify the places where the identities need to interact with the resources and control the level of access provided at various levels of interaction.

b. Logical components of Zero Trust Architecture



LOGICAL COMPONENTS OF ZERO TRUST ARCHITECTURE

According to NIST, the several logical components that make up a Zero Trust system can be categorized into three levels:

Policy Engine (PE):

component is charged with deciding who gets access to the enterprise's resources and who doesn't. Further, it makes the access decision based on several factors and lets the Policy Administrator (PA) execute it.

Policy Administrator (PA):

This component is in charge of establishing and/or shutting down the communication path between a subject and a resource. The PA can only connect a user to a resource if the PE deems the connection safe.

Policy Enforcement Point:

This system is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource.

The functioning of these components is enabled by several local and external data sources that work together to make access decisions. These include continuous diagnostics and mitigation (CDM) systems, compliance systems, threat intelligence programs, data access policies, identity management systems, and security information and event management (SIEM) systems.

c. Role of security analytics in a Zero Trust environment

It’s essential that organizations are equipped to monitor their entire IT environment for signs of malicious activity. While external attackers first need to penetrate the network before they can find the information they seek, malicious insiders already know where all the valuable data is and how to access it.

A Zero Trust environment utilizes automated security operations as a method of staying ahead of such security threats. Therefore, security analytics plays a crucial role in implementing a solid Zero Trust model. With automations and machine learning, you can generate risk scores for potential threats as they occur. Based on these scores, automated workflows can be triggered to respond to these risks, allowing organizations to mitigate legitimate threats quickly and effectively.

Organizations need to align themselves with the current cybersecurity landscape by leveraging machine learning (ML) models and user-behavior analytics (UBA) to predict, detect, and prevent insider threats, access abuse, and cyber-fraud. ML-based behavior analytics can extract context from big data, so there's no dependency on traditional rule-based security controls that are often offered by SIEM systems.

Organizations can continuously monitor behavior and dynamically calculate risk scores for real-time responses to anomalies. Unfortunately, cyber threats are becoming increasingly advanced, and the speed at which threats should be detected and eliminated has to be machine-speed. Security analytics rely on algorithms to provide in-depth analysis that otherwise cannot be achieved through manual processes.

Zero Trust is the first step to Gartner's CARTA

Block/allow security solutions don’t allow enough contextual decision-making and real-time security evaluation—they cannot simply block user access to corporate networks, because the user is not located within the organization’s four walls.

Building on the idea of Zero Trust, Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA) strategy is specially designed for continuous adaptation that goes beyond basic allow or deny models to provide contextually relevant access. In this model, all systems and devices are considered potentially compromised and their behaviors are continuously assessed for risk and trust.

Gartner notes that Zero Trust is the first step on the road to the CARTA framework, where observations continue after logins and logins are reassessed regularly. In this way, trust can be initially established upon authentication, but can also be revoked based on the pattern of behavior.

CARTA takes the Zero Trust idea further by introducing:

- ✓ Continuous monitoring, assessment, discovery, and risk mitigation
- ✓ Contextual access control
- ✓ Continuous device visibility
- ✓ Automated device control
- ✓ Dynamic risk assessments and responses

Both CARTA and Zero Trust support real-time assessments and monitoring. CARTA’s additional security measures not only reduce the risk of a breach, but also improve attack containment in case a hacker does manage to gain network access.

IMPLEMENTING ZERO TRUST IN YOUR ORGANIZATION

NIST warns that the Zero Trust Architecture is not a single off-the-shelf product. It's comprised of a set of principles that operate thematically. There are six key steps to follow before implementation.

- ✓ Classify data sources based on their sensitivity or toxicity.
- ✓ Identify the roles of users, and assign users roles with proper access policies.
- ✓ Map the flow of activities associated to business-critical data.
- ✓ Build your Zero Trust network based on the tenets specified by NIST.
- ✓ Set rules on policy gateways based on expected user behavior.
- ✓ Continuously monitor the network for anomalies, and update rules based on user behavior analytics.

Migrating to a Zero Trust environment is a strategic exercise that does not require an outright replacement of existing infrastructure or security frameworks. Instead, it's a journey that involves practicing Zero Trust principles and processes, and then moving towards technology solutions and workflows.

If you're looking to implement Zero Trust in your organization, we can help. Our IAM and cybersecurity consultants will work with your team to walk you through the six steps of Zero Trust implementation. Write to us and we can schedule a call.

About the author

Debanjali Ghosh is a cybersecurity strategist who helps IT leaders and global enterprises overcome complex cybersecurity challenges. Debanjali's primary focus is on emerging IT trends and security concerns. She has conducted research studies and authored e-books that provide insights on leveraging the latest technology for better IAM and cybersecurity.

Debanjali Ghosh
debs@manageengine.com