Embracing a Zero Trust Security Model

Executive Summary

As cybersecurity professionals defend increasingly dispersed and complex enterprise networks from sophisticated cyber threats, embracing a Zero Trust security model and the mindset necessary to deploy and operate a system engineered according to Zero Trust principles can better position them to secure sensitive data, systems, and services.

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses.

The Zero Trust security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting critical assets (data) in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, allowing or denying access to resources based on the combination of several contextual factors.

Systems that are designed using Zero Trust principals should be better positioned to address existing threats, but transitioning to such a system requires careful planning to avoid weakening the security posture along the way. NSA continues to monitor the technologies that can contribute to a Zero Trust solution and will provide additional guidance as warranted.

To be fully effective to minimize risk and enable robust and timely responses, Zero Trust principles and concepts must permeate most aspects of the network and its operations ecosystem. Organizations, from chief executive to engineer and operator, must understand and commit to the Zero Trust mindset before embarking on a Zero Trust path.

The following cybersecurity guidance explains the Zero Trust security model and its benefits, as well as challenges for implementation. It discusses the importance of building a detailed strategy, dedicating the necessary resources, maturing the implementation, and fully committing to the Zero Trust model to achieve the desired results. The following recommendations will assist cybersecurity leaders, enterprise network owners, and administrators who are considering embracing this modern cybersecurity model.

Contact

Cybersecurity Inquiries: 410-854-4200, Cybersecurity_Requests@nsa.gov

Media Inquiries: 443-634-0721, MediaRelations@nsa.gov

U/OO/115131-21 | PP-21-0191 | February 2021 Ver. 1.0

Falling behind

Today's IT landscape is empowered by a connected world that is more susceptible to malicious activity due to its connectedness, user diversity, wealth of devices, and globally distributed applications and services. Systems and users require simple and secure methods of connecting and interacting with organizational resources, while also keeping malicious actors at bay. The increasing complexity of current and emerging cloud, multi-cloud, and hybrid network environments combined with the rapidly escalating and evolving nature of adversary threats has exposed the lack of effectiveness of traditional network cybersecurity defenses. Traditional perimeter-based network defenses with multiple layers of disjointed security technologies have proven themselves to be unable to meet the cybersecurity needs due to the current threat environment. Contemporary threat actors, from cyber criminals to nation-state actors, have become more persistent, more stealthy, and more subtle; thus, they demonstrate an ability to penetrate network perimeter defenses with regularity. These threat actors, as well as insider threat actors, have succeeded in leveraging their access to endanger and inflict harm on national and economic security. Even the most skilled cybersecurity professionals are challenged when defending dispersed enterprise networks from ever more sophisticated cyber threats. Organizations need a better way to secure their infrastructure and provide unified-yet-granular access control to data, services, applications, and infrastructure.

By implementing a modern cybersecurity strategy that integrates visibility from multiple vantage points, makes risk-aware access decisions, and automates detection and response actions, network defenders will be in a much better position to secure sensitive data, systems, applications, and services. Zero Trust is an "assumed breach" security model that is meant to guide cybersecurity architects, integrators, and implementers in integrating disparate but related cybersecurity capabilities into a cohesive engine for cybersecurity decision-making. However, to be fully effective, Zero Trust principles need to permeate most aspects of the network and its operations ecosystem to minimize risk and enable robust and timely responses. Organizations that choose to migrate to a Zero Trust solution should fully embrace this security model and the mindset necessary for planning, resourcing, and operating under this security model to achieve the cybersecurity outcomes that a Zero Trust solution can deliver [1] [2].

Increasingly sophisticated threats

Embracing a Zero Trust security model, and re-engineering an existing information system based on this security model, is a strategic effort that will take time to achieve full benefits. It is not a tactical mitigation response to new adversary tools, tactics, and techniques. However, several recent, highly publicized system breaches have exposed widespread vulnerabilities in systems, as well as deficiencies in system management and defensive network operations. These incidents show that purely tactical responses are often insufficient. A mature Zero Trust environment will afford cybersecurity defenders more opportunities to detect novel threat actors, and more response options that can be quickly deployed to address sophisticated threats. Adopting the mindset required to successfully operate a Zero Trust environment will further sensitize cybersecurity defenders to recognize ever more subtle threat indicators. Tactical responses will likely still be necessary even in a Zero Trust environment, but with the appropriate security model, mindset, and response tools, defenders can begin to react effectively to increasingly sophisticated threats.

What is Zero Trust?

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. Zero Trust repeatedly questions the premise that users, devices, and network components should be implicitly trusted based on their location within the network. Zero Trust embeds comprehensive security monitoring; granular, dynamic, and risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus specifically on protecting critical assets (data) in real-time within a dynamic threat environment. This data-centric security model allows the concept of least privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where, and how are critical for appropriately allowing or denying access to resources [3].

NSA strongly recommends that a Zero Trust security model be considered for critical networks to include National Security Systems (NSS), Department of Defense (DoD) networks, and Defense Industrial Base (DIB) systems. Integrating

these principles within certain environments, especially within a large enterprise, can become complicated. To address these challenges, NSA is developing additional guidance to organize, guide, and simplify the Zero Trust design approach.

Adopt a Zero Trust mindset

To adequately address the modern dynamic threat environment requires:

- Coordinated and aggressive system monitoring, system management, and defensive operations capabilities.
- Assuming all requests for critical resources and all network traffic may be malicious.
- Assuming all devices and infrastructure may be compromised.
- Accepting that all access approvals to critical resources incur risk, and being prepared to perform rapid damage assessment, control, and recovery operations.

Embrace Zero Trust guiding principles

A Zero Trust solution requires operational capabilities that:

- **Never trust, always verify** – Treat every user, device, application/workload, and data flow as untrusted. Authenticate and explicitly authorize each to the least privilege required using dynamic security policies.
- **Assume breach** – Consciously operate and defend resources with the assumption that an adversary already has presence within the environment. Deny by default and heavily scrutinize all users, devices, data flows, and requests for access. Log, inspect, and continuously monitor all configuration changes, resource accesses, and network traffic for suspicious activity.
- **Verify explicitly** – Access to all resources should be conducted in a consistent and secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access decisions to resources.

Leverage Zero Trust design concepts

When designing a Zero Trust solution:

- **Define mission outcomes** – Derive the Zero Trust architecture from organization-specific mission requirements that identify the critical Data/Assets/Applications/Services (DAAS).
- **Architect from the inside out** – First, focus on protecting critical DAAS. Second, secure all paths to access them.
- **Determine who/what needs access to the DAAS to create access control policies** – Create security policies and apply them consistently across all environments (LAN, WAN, endpoint, perimeter, mobile, etc.).
- **Inspect and log all traffic before acting** – Establish full visibility of all activity across all layers from endpoints and the network to enable analytics that can detect suspicious activity.

Examples of Zero Trust in use

The fundamental purpose of Zero Trust is to understand and control how users, processes, and devices engage with data. The combination of the user, device, and any other security-relevant contextual information (e.g., location, time of day, previous logged behavior of the user or device) to be used to make an access decision is called a tuple. As part of this tuple, explicit authentication of both the user and the device is required to have reliable information in the tuple. The Zero Trust decision engine examines the tuple in the access request and compares that to the security policy for the data or resource being requested. It then makes a risk-informed decision on whether to allow access and sends a log entry of that access request and decision to be part of future suspicious activity analytics. This process is conducted for every individual access request to each sensitive resource and can be repeated periodically during extended access to a resource.

The following are a few example cases where a mature Zero Trust implementation can detect malicious activity better than a traditional architecture usually can.

Compromised user credentials

In this example, a malicious cyber actor compromises a legitimate user's credentials and attempts to access organizational resources. In this case, the malicious actor is using an unauthorized device, either through remote access

or with a rogue device joining the organization's wireless LAN. In a traditional network the user's credentials alone are often sufficient to grant access, but in a Zero Trust environment the device is not known, so the device fails authentication and authorization checks and so access is denied and the malicious activity is logged. In addition, Zero Trust requires strong authentication for user and device identities. Use of strong multi-factor authentication of users, which is recommended for Zero Trust environments, can make stealing the user's credentials more difficult in the first place.

Remote exploitation or insider threat

In this example, a malicious cyber actor compromises a user's device through an Internet-based mobile code exploit. Or, the actor is an inside authorized user with malicious intentions. In a typical, non-Zero Trust scenario, the actor uses the user's credentials, enumerates the network, escalates privileges, and moves laterally through the network to compromise vast stores of data and, ultimately, persist. In a Zero Trust network, the compromised user's credentials and the device are already assumed to be malicious until proven otherwise, and the network is segmented, limiting both enumeration and lateral movement opportunities. While the malicious actor can authenticate as both the user and the device, access to data will be limited based on security policy, user role, and the user and device attributes. In a mature Zero Trust environment, data encryption and digital rights management may offer additional protections by limiting which data can be accessed and the actions that can be taken with the sensitive data even if access was allowed. Further, analytic capabilities continuously monitor for anomalous activity in accounts, devices, network activity, and data access. While a level of compromise occurs in this scenario, damage is limited and the time for defensive systems to detect and initiate appropriate mitigating responses is greatly reduced.

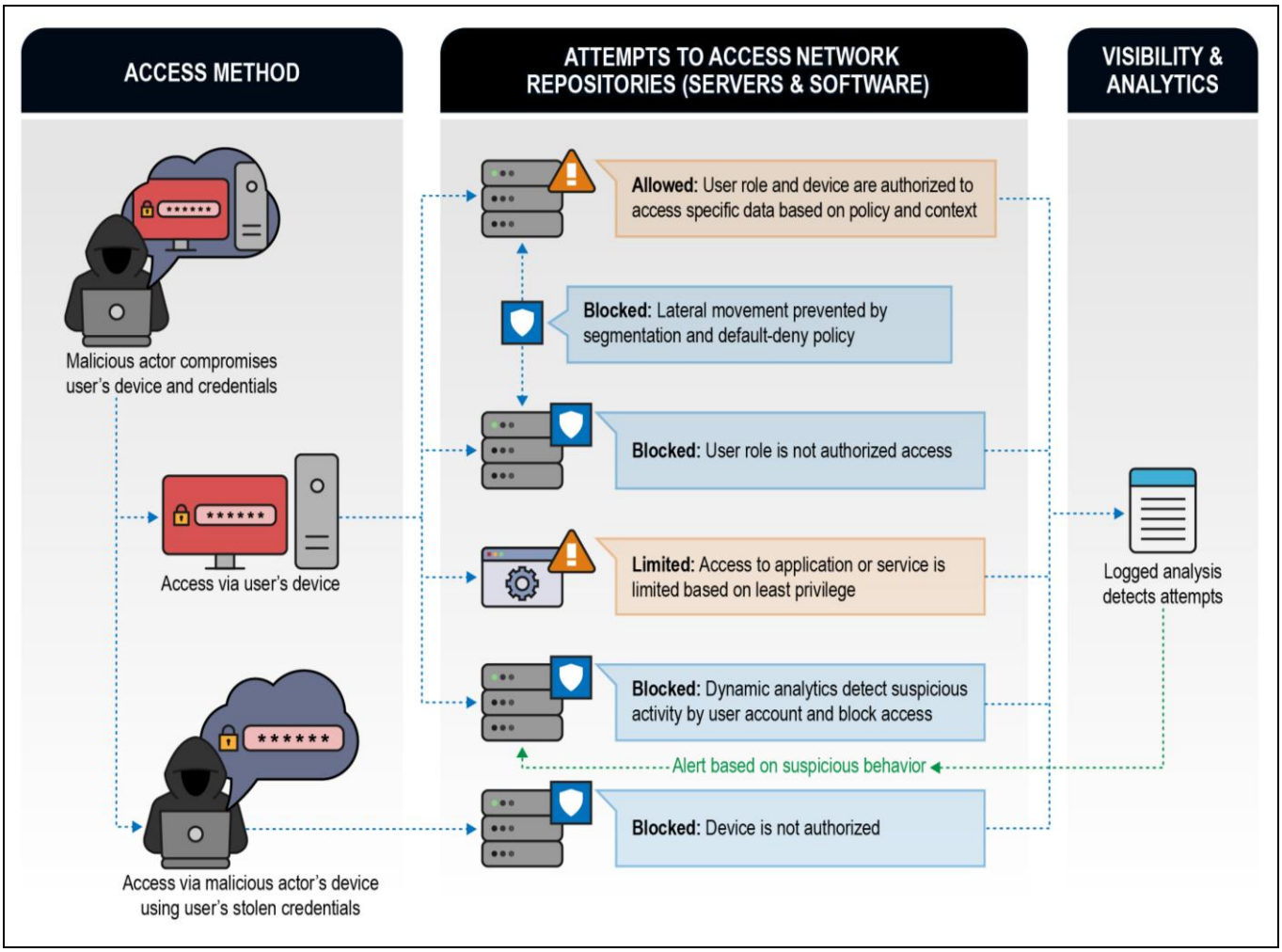

Figure 1: Example of Zero Trust remote exploitation scenarios where most attempts would have been successful in non-Zero Trust environments.

Compromised supply chain

In this example, a malicious actor embeds malicious code in a popular enterprise network device or application. The device or application is maintained and regularly updated on the organization's network in accordance with best practices. In a traditional network architecture, this device or application would be internal and fully trusted. While this type of compromise can be particularly severe because it is implicitly so trusted, in a mature implementation of a Zero Trust architecture, real defensive cybersecurity benefits are obtained since the device or application would not be inherently trusted. Its privileges and access to data would be tightly controlled, minimized, and monitored; segmentation (macro and micro) would be enforced by policy; and analytics would be used to monitor for anomalous activity. In addition, while the device may be able to download signed application updates (malicious or not), the device's allowed network connections under a Zero Trust design would employ a deny-by-default security policy, so any attempt to connect to other remote addresses for command and control would likely be blocked. Also, network monitoring could detect and block attempted lateral movement from the device or an application not associated with an authorized access request.

Zero Trust maturity

Implementing Zero Trust takes time and effort: it cannot be implemented overnight. For many networks, existing infrastructure can be leveraged and integrated to incorporate Zero Trust concepts, but the transition to a mature Zero Trust architecture often requires additional capabilities to obtain the full benefits of a Zero Trust environment. Transitioning to a mature Zero Trust architecture all at once is also not necessary. Incorporating Zero Trust functionality incrementally as part of a strategic plan can reduce risk accordingly at each step. As the Zero Trust implementation matures over time, enhanced visibility and automated responses allow defenders to keep pace with the threat.

NSA recommends embracing the Zero Trust security model when considering how to integrate Zero Trust concepts into an existing environment. Zero Trust efforts should be planned out as a continually maturing roadmap, from initial preparation to basic, intermediate, and advanced stages, with cybersecurity protection, response, and operations improving over time.

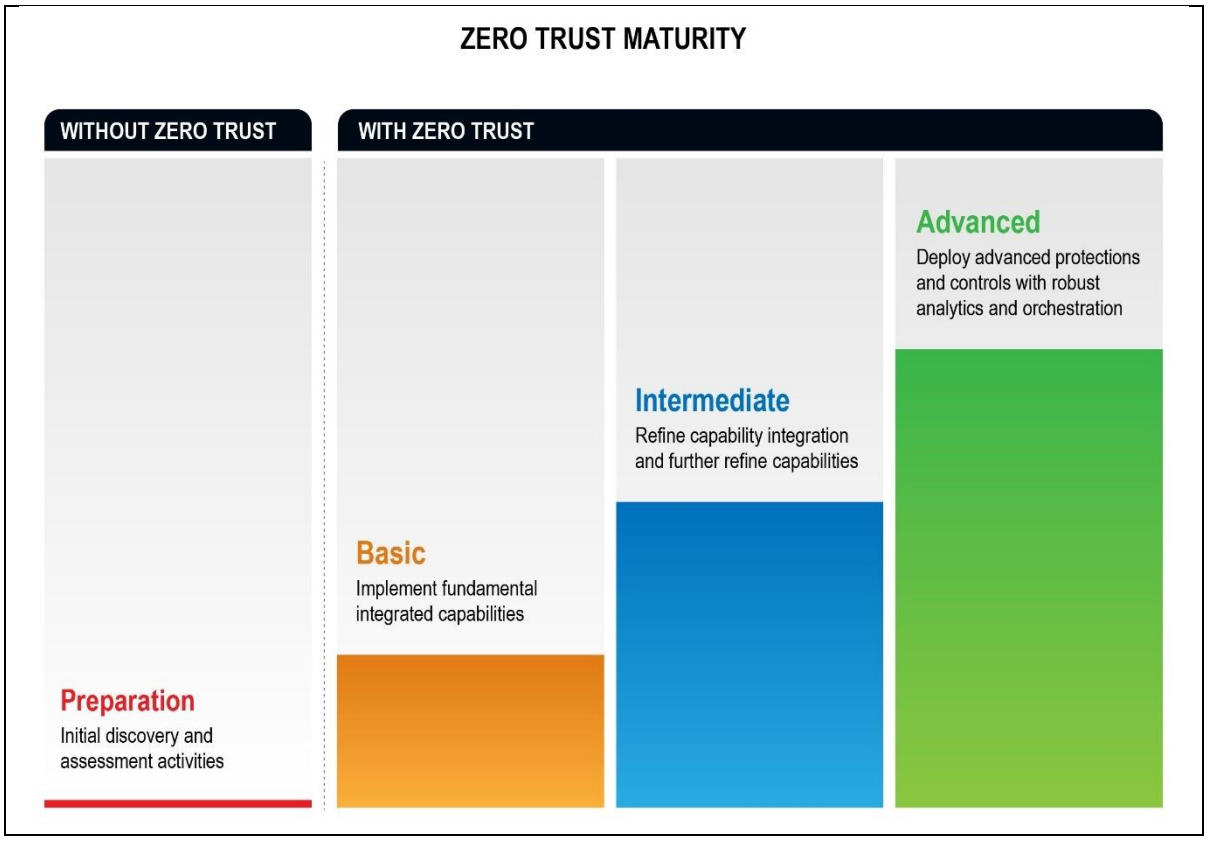

Figure 2: Maturing a Zero Trust implementation

Potential challenges on the path to Zero Trust

When implementing Zero Trust in enterprise networks, several challenges may arise that reduce the effectiveness of the solution. The first potential challenge is a lack of full support throughout the enterprise, possibly from leadership, administrators, or users. The mindset required for Zero Trust must be embraced fully for any solution to be successful. If leaders are unwilling to spend the necessary resources to build and sustain it, if administrators and network defenders do not have buy-in or the requisite expertise, or if users are allowed to circumvent the policies, then the benefits of Zero Trust will not be realized in that environment. Once even basic or intermediate Zero Trust capabilities are integrated into a network, follow-through is necessary to mature the implementation and achieve full benefits [4].

With the pervasive need for Zero Trust concepts to be applied throughout the environment, scalability of the capabilities is essential. Access control decisions that may have only occurred once for each access previously will now be performed continuously as access to the resource is used, requiring a robust infrastructure for making, enforcing, and then logging these access decisions. In addition, elements of the network that previously were not part of access control decisions may become essential elements whose reliability and consistent use are required, such as data tags and additional network sensors.

Persistent adherence to the mindset, and application of the Zero Trust security model over time is also a key requirement. Administrators and defenders may become fatigued with constantly applying default-deny security policies and always assuming a breach is occurring, but if the Zero Trust approach falters, then its cybersecurity benefits become significantly degraded or eliminated.

Carefully minimizing embedded trust empowers a more secure mission

The ever-increasing complexity of network environments and the ability of adversaries to compromise them requires a change in defensive focus. The Zero Trust mindset focuses on securing critical data and access paths by eliminating trust as much as possible, coupled with verifying and regularly re-verifying every allowed access. However, implementing Zero Trust should not be undertaken lightly and will require significant resources and persistence to achieve. When properly and fully implemented, Zero Trust should be able to prevent, detect, and contain intrusions significantly faster and more effectively than traditional, less integrated cybersecurity architectures and approaches.▪

Further guidance

NSA is assisting DoD customers in piloting Zero Trust systems, coordinating activities with existing NSS and DoD programs, and developing additional Zero Trust guidance to support system developers through the challenges of integrating Zero Trust within NSS, DoD, and DIB environments. Upcoming additional guidance will help organize, guide, and simplify incorporating Zero Trust principles and designs into enterprise networks. The National Institute of Standards and Technology also has related Zero Trust architecture guidance [3].

Supplementary NSA guidance on ensuring a secure and defensible network environment is available at https://www.nsa.gov/cybersecurity-guidance. Of particular relevance are:

- NSA's Top Ten Cybersecurity Mitigation Strategies
- Defend Privileges and Accounts
- Continuously Hunt for Network Intrusions
- Segment Networks and Deploy Application-aware Defenses
- Transition to Multi-factor Authentication
- Actively Manage Systems and Configurations
- Performing Out-of-Band Network Management
- Hardening SIEM Solutions
- Mitigating Cloud Vulnerabilities

Works Cited

[1] Department of Defense (2019), DoD Digital Modernization Strategy. Available at: https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF
[2] Director, Operational Test and Evaluation (2021), FY 2020 Annual Report. Available at: https://www.dote.osd.mil/Portals/97/pub/reports/FY2020/other/2020DOTEAnnualReport.pdf
[3] National Institute of Standards and Technology (2020), Special Publication 800-207: Zero Trust Architecture. Available at: https://csrc.nist.gov/publications/detail/sp/800-207/final
[4] Institute for Defense Analysis (2015), In-Use and Emerging Disruptive Technology Trends. Available at: https://apps.dtic.mil/sti/pdfs/AD1013834.pdf

Disclaimer of Endorsement

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media Inquiries / Press Desk: Media Relations, 443-634-0721, MediaRelations@nsa.gov