National Security Agency | Cybersecurity Information Sheet

Advancing Zero Trust Maturity Throughout the Network and Environment Pillar

Executive summary

After gaining access to an organization's network, one of the most common techniques malicious cyber actors use is lateral movement through the network, gaining access to more sensitive data and critical systems. The Zero Trust network and environment pillar curtails adversarial lateral movement by employing controls and capabilities to logically and physically segment, isolate, and control access (on-premises and off-premises) through granular policy restrictions.

The network and environment pillar works in concert with the other Zero Trust pillars as part of a holistic Zero Trust security model that assumes adversary breaches occur inside the network, and so limits, verifies, and monitors activities throughout the network.

The concepts introduced in this cybersecurity information sheet provide guidance on enhancing existing network security controls to limit the potential impact of a compromise through data flow mapping, macro and micro segmentation, and software defined networking. These capabilities enable host isolation, network segmentation, enforcement of encryption, and enterprise visibility. As organizations mature their internal network control, they greatly improve their defense-in-depth posture and, consequently, can better contain, detect, and isolate network intrusions.

Introduction

According to public reports, an American retail corporation experienced a significant data breach in 2013 due to a lack of network segmentation. [1] Preceding the breach, cyber criminals managed to acquire the login credentials of a heating, ventilation, and air conditioning (HVAC) company that had been contracted by several of the retail corporation’s store locations. The locations had granted the HVAC company access to the corporate network to monitor energy and temperature levels. However, using the obtained login credentials, cyber actors successfully introduced malware into the corporation’s point of sale systems, stealing information for approximately 40 million debit and credit cards. While the HVAC company required access to the retail corporation’s network to carry out its responsibilities, findings suggest the corporation likely would have been able to mitigate third-party access to their payment systems by implementing network segmentation and access control. [2]

Traditional network security has emphasized a defense-in-depth approach; however, most networks invest primarily in perimeter defense. Once inside the network perimeter, end users, applications, and other entities are often given broad access to multiple corporate resources. If network users or components are compromised, malicious actors can gain access to critical resources from inside or outside the network. Ideally, organizations should manage, monitor, and restrict both internal and external traffic flows.

This cybersecurity information sheet (CSI) will discuss the network and environment pillar’s focus on implementing security controls close to resources and data in addition to perimeter defense, pursuant to the Zero Trust (ZT) security model. This pillar’s primary areas include mapping data flows within the network and implementing network segmentation with strong access controls to inhibit lateral movement. This shift enables host isolation, network segmentation, enforcement of encryption, and enterprise visibility. As organizations mature their internal network control, they greatly improve their defense-in-depth posture and, consequently, can isolate network intrusions to a small portion of the network.

Audience

This CSI provides guidance primarily intended for National Security Systems (NSS), the Department of Defense (DoD), and the Defense Industrial Base (DIB). However, it may be useful for owners and operators of other systems that might be targeted by sophisticated malicious actors. This CSI incorporates guidance from the DoD’s Zero Trust Strategy, Zero Trust Reference Architecture, and Cybersecurity Reference Architecture (CSRA). [3], [4], [5] Additional guidance for other system owners and operators is also available from the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA). [6], [7]

Background

The President’s Executive Order on Improving the Nation’s Cybersecurity (EO 14028) and National Security Memorandum 8 (NSM-8) direct the Federal Civilian Executive Branch agencies and NSS owners and operators to develop and implement plans to adopt a ZT cybersecurity framework. [8], [9]

The NSA CSI, Embracing a Zero Trust Security Model, defines the concept of ZT as a security strategy with core principles: acknowledgement of the ubiquity of cyber threats, and elimination of implicit trust favoring instead continuous verification of all aspects of the operational environment. ZT implementation efforts are intended to continually mature cybersecurity protections, responses, and operations over time. Progression of capabilities in each of the seven pillars of ZT— User, Device, Network & Environment, Data, Application & Workload, Automation & Orchestration, and Visibility & Analytics — should be seen as elements in a cycle of continuous improvement based on evaluation and monitoring of threats. [10]

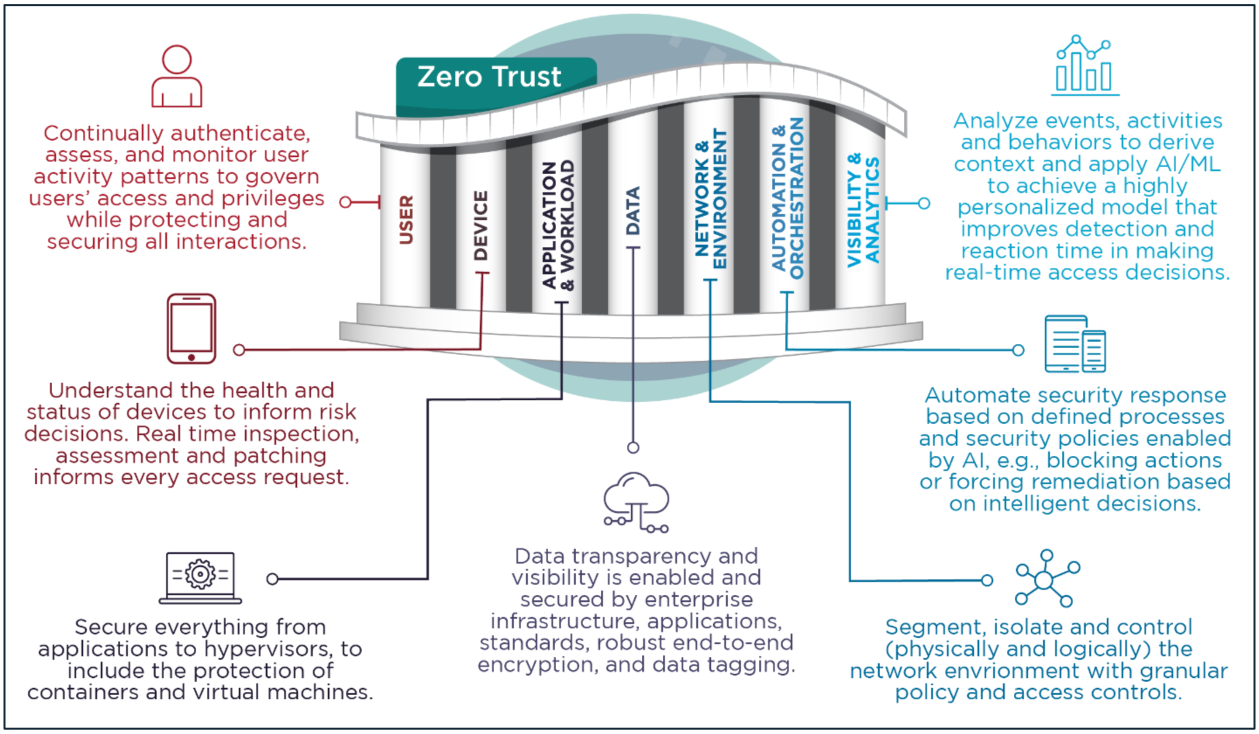
Zero Trust
USER
DEVICE
APPLICATION & WORKLOAD
DATA
NETWORK & ENVIRONMENT
AUTOMATION & ORCHESTRATION
VISIBILITY & ANALYTICS
Continually authenticate, assess, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.
Understand the health and status of devices to inform risk decisions. Real time inspection, assessment and patching informs every access request.
Secure everything from applications to hypervisors, to include the protection of containers and virtual machines.
Data transparency and visibility is enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.
Segment, isolate and control (physically and logically) the network envrionment with granular policy and access controls.
Automate security response based on defined processes and security policies enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.
Analyze events, activities and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

Figure 1: Description of the seven pillars of Zero Trust

Figure 1 depicts the ZT pillars, including the network and environment pillar. The capabilities and milestones for the network and environment pillar component of the ZT maturity model are described in detail throughout this CSI. The pillars are not independent; many capabilities in the network and environment pillar depend on, or align with, capabilities in other pillars as indicated.

Network and environment pillar

While a network is the connectivity of hardware and software, the cybersecurity environment as defined in the DoD CSRA and NIST SP 800-207 is the digital ecosystem encompassing all of the network components, non-person entities, and protocols for inter-communication. [5], [6] The ZT maturity model delivers a network secured in-depth through several key functions of each of the four networking and environment pillar capabilities:

- Data flow mapping
- Macro segmentation
- Micro segmentation
- Software Defined Networking

The network and environment serve this model through a segmented robust architecture that must be intentionally developed at the outset and maintained and improved upon throughout the environment’s lifecycle.

In addition to a secure network segmentation framework, ZT architecture employs secure network traffic management through strong encryption and persistent verification of all users, devices, and data. Automation and orchestration depends on defined processes and security policies, along with adaptive network capabilities to dynamically isolate or modify network segmentation as needed. Intuitive analytics monitor network and other events and activities for suspicious behaviors. Given proper application, these capabilities all support the ZT architecture and have the potential to greatly improve the network’s security.

The network and environment pillar isolates critical resources from unauthorized access by defining network access, controlling network and data flows, segmenting applications and workloads, and using end-to-end encryption. This is accomplished through proper network segmentation at the macro and micro levels, combined with software defined networking (SDN), to allow centralized control and automation. This pillar depends on an organization’s depth of awareness and understanding of their data – how it flows within standalone networks and across networks that interconnect physical infrastructure, cloud computing, and distributed work environments.

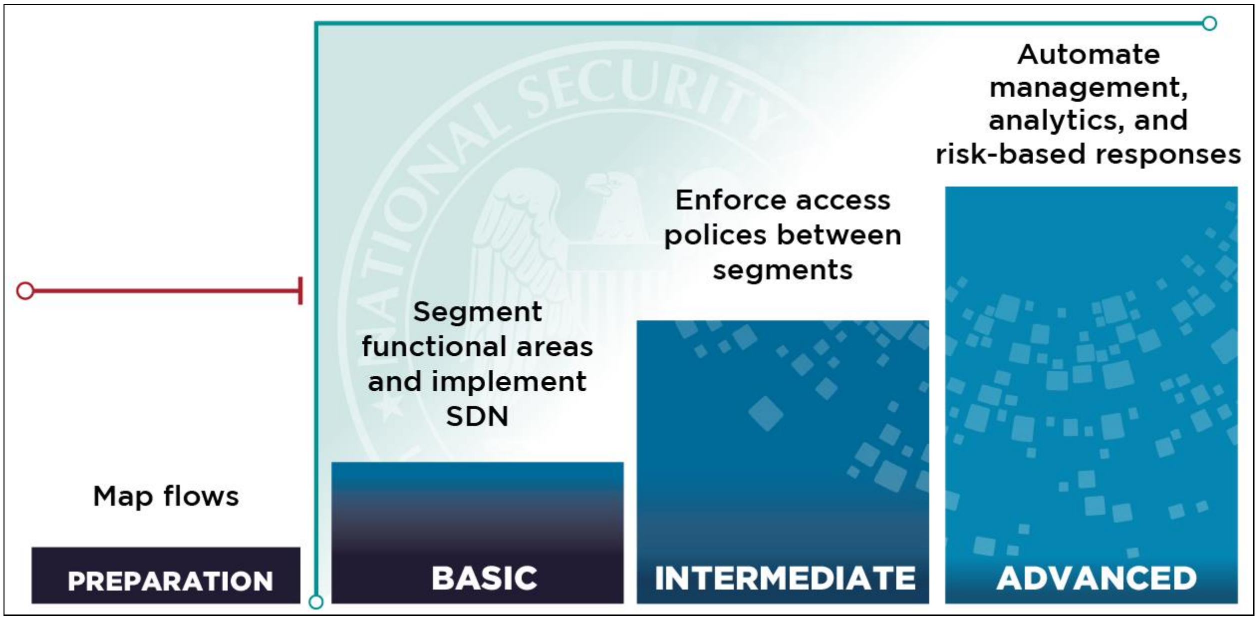
Map flows
PREPARATION
Segment functional areas and implement SDN
BASIC
Enforce access polices between segments
INTERMEDIATE
Automate management, analytics, and risk-based responses
ADVANCED

Figure 2: Zero Trust network and environment pillar maturity

Data flow mapping

Data flow mapping identifies the route data travels within an organization and describes how that data transforms from one location or application to another. This activity highlights the internal and external nodes on which data is stored or processed, which enables the discovery of any data misuse. Organizations should leverage data owners' and network teams' knowledge to form a comprehensive data flow map.

This map can also identify data flows where the data is not properly encrypted. In cases where data is not encrypted in transit, the data senders should enable end-to-end encryption where possible or leverage virtual private networks (VPNs) — or equivalent encrypted tunnels and protocols — to protect the data in transit.

In addition to discovering flows where data is insufficiently protected, this data flow mapping process is foundational for other network activities, such as macro and micro segmentation. Further, understanding how data flows through the network aids in efficiently identifying anomalous traffic behavior via analytics.

Table 1: Data flow mapping maturity

Preparation	Basic	Intermediate	Advanced
Identify locations where data is stored and processed and in which state the data components are stored.	Organizations begin the mapping of both physical and logical data flows. Mapping is primarily manual at this level. Unencrypted data flows are transitioned to encrypted data flows or within encrypted network tunnels or protocols.	Organizations have a complete list of applications and have identified critical data flows. Some automation has been implemented to maintain the accuracy of mappings. Any anomalous data flows identified should be isolated or eliminated at this level.	Organizations have a complete inventory of data flows. Automation monitors for controls, and mitigates all current, new, or anomalous data flows.

Macro segmentation

Network segmentation is crucial in designing and implementing a ZT architecture. It can be broken down as follows:

- Macro segmentation
- Micro segmentation

Macro segmentation provides high-level control over traffic moving between various areas of an organization's network by breaking up a network into multiple discrete components with each supporting a different security requirement. In other words, macro segmentation can be thought of as the separation of sub-organizations within a company. For example, an employee in the IT department should not have access to the accounting department's section of the network, and all of the data and resources residing there. These network boundaries, coupled with access controls, provide security by shrinking the attack surface to prevent lateral movement. Additionally, macro segmentation paves the way for automating security responses. As a result, this further minimizes the risks of loss from data breaches, denial of service, or malware proliferation.

In the case of the retail corporation's data breach detailed earlier, an HVAC company was given valid access to the network for service-related tasks. The network was not properly segmented however, allowing a cyber actor to access the network using credentials stolen from some of the HVAC company employees and pivot to point-of-sales systems. [1] According to public reporting, macro segmentation could have prevented this, saving millions of dollars in customer and corporate losses. [2]

Table 2: Macro segmentation maturity

Preparation	Basic	Intermediate	Advanced
Define different security levels on the network. Map the logical distinctions in network structure.	Organizations begin segmenting their networks based on business functions, locations, and asset criticality. Use of internal security controls are strengthened within any existing segments (e.g. VLANS)	Access policies restricting lateral movement between segments are defined and written into firewall rules based on security policies.	The network is further segmented into more granular components and an automated central management system is integrated and configured to manage the growth of the network.

Micro segmentation

Micro segmentation provides security at a granular level by breaking down a portion of the network into smaller components to limit how data flows laterally through strict access policies. Micro segmentation can be thought of as the network separation within a sub-organization; employees in the same department should not have access to each other's resources unless explicitly required. This provides for additional security enforcement closer to applications and resources, augmenting policies already established at the network perimeter. Therefore, micro segmentation involves isolating users, applications, or workflows into individual network segments to further reduce the attack surface and limit the impact should a breach occur.

While the intrusion into the retail corporation's network occurred ten years ago, the lessons learned continue to reverberate throughout the cybersecurity industry. For example, because micro segmenting the point-of-sales systems from each other and from other systems might have limited the impact, micro segmentation is now a primary component of many organizations' defense posture. Today's SDN technology makes this more manageable through central control and automated policy enforcement.

Table 3: Micro segmentation maturity

Preparation	Basic	Intermediate	Advanced
Define different security levels on the network based on identity and application access.	Organizations begin to transition toward service-specific interconnections and the isolation of critical data flows.	Organizations deploy endpoint and application isolation mechanisms to more of their network architecture with ingress/egress controls between micro segments. Controls are tested and refined as needed.	Organizations employ extensive micro segmentation based on application profiles and data flows, with continuous authentication of connectivity for service-specific interconnections. Central management platforms are refined to provide automated and optimal visibility and security monitoring, including alerting on anomalous behavior.

Software defined networking

SDN offers unique advantages in terms of granularity through micro segmentation, adaptability, and centralized policy management. Integrating SDN components into existing infrastructure also can enable customizable security monitoring and alerting.

Though micro segmentation can be achieved with traditional system components and manual configuration, the centralized nature of SDN allows for dynamic implementation and management across the network. SDN enables the control of packet routing by a centralized control server via a distributed forwarding plane, provides additional visibility into the network, and enables unified policy enforcement.

SDN is already a feature of many modern network devices currently in use and can allow flexible integration and control of new equipment. Additionally, SDN network management platforms are readily available and can automate manual tasks. This facilitates integration of network segments under a common centrally managed policy and reduces the risk of human error, such as misconfigurations as the network scales.

While security of the network overall benefits from micro segmentation through SDN, the SDN Controller (SDNC) itself can become a priority target that requires proper configuration and continuous monitoring. As scripts are written to make application programming interface (API) calls to facilitate necessary automation of tasks, SDNC configurations can expose those APIs. SDN improves network security by automating updates and security policies. However, to prevent exposing APIs, good cybersecurity practices (and discipline) are necessary to inhibit the unauthorized disabling of security controls and other compromises of SDN capabilities. Refer to Managing Risk from Software Defined Networking Controllers for more information about these risks and recommended practices. [11]

Dedicated API administrator roles should be created with restricted privileges that do not allow the same level of access as SDN administrators. The SDNC should only accept API calls from authorized API administrators. API calls should be secured using proper encrypted protocols (e.g., TLS v1.2 or newer, SSH v2 or newer) and mutual authentication (such as client and server certificates) when possible to protect the data in transit.

Table 4: Software defined networking maturity

Preparation	Basic	Intermediate	Advanced
Organizations map network segments within their administrative purview and identify a roadmap for SDN component integrations.	Integrate SDN components and develop a central control plane, along with management policy, network configuration rules, and task schedule (such as updates). Map SDN APIs, establish roles, and configure the SDNC to make API calls using encryption and authentication.	Test interconnectedness and set configurations to employ segmentation rules at the optimal level of granularity. Create alert systems to notify administrators of anomalous or suspicious behavior.	Employ advanced analytics and controls. Test the network to determine which network paths would allow an intruder to move between segments laterally or otherwise. Restrict the paths as appropriate with strict access controls.

Summary

Expanding and refining the network and environment pillar roadmap according to the maturity model developed here provides an organization with processes for resisting, detecting, and responding to threats that exploit weaknesses or gaps in their enterprise architecture. Those processes support an operational mindset in which it is assumed that threats already exist within the nominal boundaries of their systems. Vigilance is required to ensure that risks are continually assessed, and appropriate responses are enacted in a timely manner, with follow-up investigations and damage control as necessary.

NSA strongly recommends that network owners and operators strengthen their network and environment by developing capabilities commensurate with the advanced levels of maturity models described in this CSI. Network and environment security begins with establishing an accurate inventory of all current data flows. This ensures that access to these flows is properly protected, vetted, and appropriate.

To mature the network and environment capabilities, an organization should:

- Map data flows based on usage patterns and operational business requirements.
- Properly segment the network at both the macro and micro levels.
- For centralized control and automated tasking, use SDN where it is available and practical to do so.

- Automate security policies to gain operational efficiency and agility.
- Use risk-based methodologies to define access rules that include mechanisms to ensure malicious or unauthorized traffic is dropped prior to reaching network resources at the perimeter, macro, and micro boundaries.

Further guidance

NSA is actively assisting DoD customers in piloting ZT systems, coordinating activities with existing NSS and DoD programs, and developing additional ZT guidance to support system developers through the challenges of integrating ZT within NSS, DoD, and DIB environments. Upcoming guidance will help organize, guide, and simplify incorporation of ZT principles and designs into enterprise networks.

Works cited

[1] Computerworld. Target Breach Happened Because of a Basic Network Segmentation Error. 2014. https://www.computerworld.com/article/2487425/target-breach-happened-because-of-a-basic-network-segmentation-error.html

[2] Senate Committee on Commerce, Science, and Transportation. A “Kill Chain” Analysis of the 2013 Target Data Breach. 2014. https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883

[3] Department of Defense. DoD Zero Trust Strategy. 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[4] Department of Defense. DoD Zero Trust Reference Architecture. 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf.

[5] Department of Defense. DoD Cybersecurity Reference Architecture. 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf

[6] National Institute of Standards and Technology. NIST Special Publication 800-207: Zero Trust Architecture. 2020. https://csrc.nist.gov/publications/detail/sp/800-207/final

[7] Cybersecurity and Infrastructure Security Agency. Zero Trust Maturity Model. 2023. https://www.cisa.gov/zero-trust-maturity-model

[8] The White House. Executive Order 14028: Improving the Nation's Cybersecurity. 2021. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[9] The White House. White House National Security Memorandum 8: Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems. 2022. https://www.govinfo.gov/content/pkg/DCPD-202200025/pdf/DCPD-202200025.pdf

[10] National Security Agency. Embracing a Zero Trust Security Model. 2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.

[11] National Security Agency. Managing Risk from Software Defined Networking Controllers. 2023. https://media.defense.gov/2023/Dec/12/2003357491/-1/-1/0/CSI_MANAGING_RISK_FROM_SDN_CONTROLLERS.PDF.

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

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

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
General Cybersecurity Inquiries or Customer Requests: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov