Gigamon®

Two Reasons to Make Network Visibility a Foundation of Your Zero Trust Architecture

Presidential Executive Order 14028 on Improving the Nation's Cybersecurity directs federal agencies to transition to a Zero Trust Architecture (ZTA) as they modernize their approach to cybersecurity and move to secure cloud services.[1] The National Institute of Standards and Technology (NIST) has provided guidance on transitioning to a ZTA in Special Publication 800-207 Zero Trust Architecture (SP 800-207).[2] In addition, the Office of Management and Budget has released guidance prioritizing Zero Trust initiatives.[3]

One of the most strategic investments an agency can make to facilitate a successful ZTA implementation is complete, accurate, and timely network visibility into all data in motion across the enterprise, including data center, cloud, and multi-cloud environments.

Understanding NIST's Abstract Definition of a Zero Trust Architecture

Visibility into data in motion is an aspect of Zero Trust that falls within the "Activity Logs" logical component depicted in Figure 2: Core Zero Trust Logical Components from SP 800-207, as seen below.[4]

SP 800-207 defines this essential "network and system activity logs" component as follows:

> This enterprise system aggregates asset logs, network traffic, resource access actions, and other events that provide real-time (or nearreal-time) feedback on the security posture of enterprise information systems.

Many organizations in the federal government have also made investments in other areas that can bring value to ZTA approaches, including identity and access management (IAM), endpoint detection and response (EDR), and security information and event management (SIEM) technologies.

However, as organizations evolve towards more mature ZTA implementations, security gaps will remain after the deployment of these technologies. For example, specific nodes such as internet of things (IoT) devices may be incompatible with EDR software, and logs from hosts can be manipulated by sophisticated adversaries. A scalable, centralized approach to network visibility mitigates these risks. Moreover, deploying an advanced network visibility platform can further optimize the effectiveness and scalability of ZTA implementations by filtering out noise and duplicate data from the traffic analyzed by security tools.

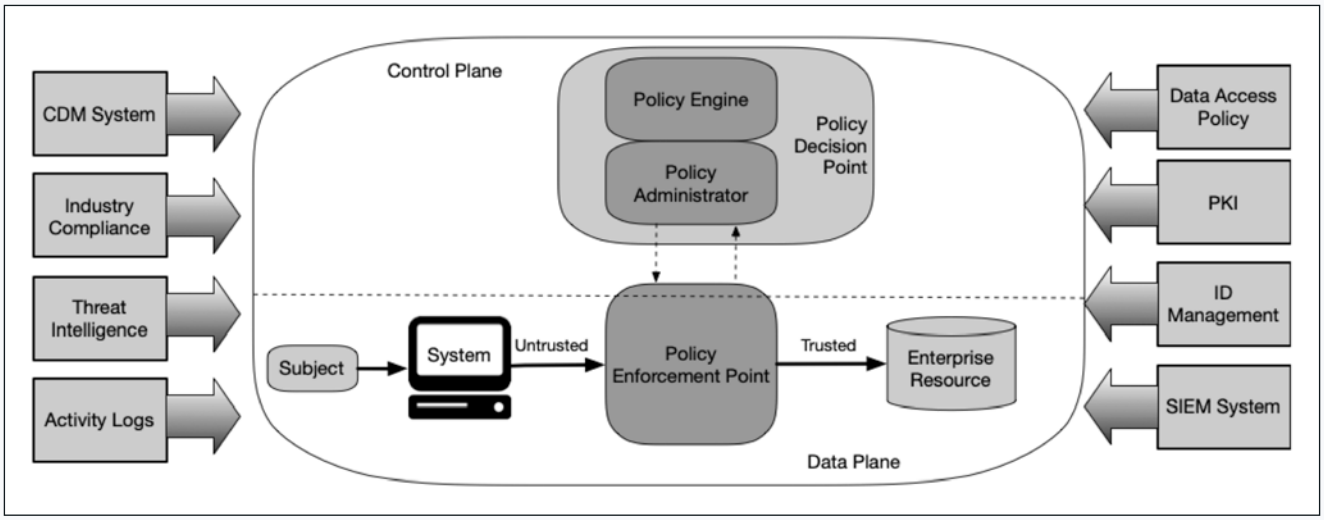

Figure 1. Figure 2 from SP 800-207: Core Zero Trust Logical Components.[5]

East-West traffic refers to how communication flows between nodes within a data center and/or cloud service provider (CSP) perimeter. Monitoring East-West traffic helps organizations detect and respond to attempts by adversaries to move laterally from the initial point of breach towards higher-value assets.

The following are two key reasons why pervasive visibility into all data in motion across the enterprise — including all East-West traffic — is central to ZTA and mitigates risks not otherwise addressed by IAM, EDR, and SIEM implementations.

Reason #1

Data about the network plays a central role in ZTA, and visibility into data in motion is a critical aspect of understanding the current state of the network.

Understanding the state of the network is a key tenet of ZTA as described in NIST SP 800-207:

> Tenet 7: The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. An enterprise should collect data about asset security posture, network traffic and access requests, process that data, and use any insight gained to improve policy creation and enforcement. This data can also be used to provide context for access requests from subjects[6] [emphasis added].

One of the primary ways organizations can gain this understanding is by collecting and analyzing data about network traffic, including access requests. When an advanced network visibility platform is used to address the Activity Logs component in Figure 2 of SP 800-207, it provides substantial insights about network activity to the Policy Engine — at leadingedge network speeds — to inform access decisions.[7]

In addition, analysis of data about network traffic complements — and can be used to validate the integrity of — other types of data that feed the Policy Engine while satisfying current and emerging federal government security requirements beyond ZTA.[8]

For more information, read "Gigamon Adds Crucial Network Visibility to Zero Trust at the Department of Defense."

Reason #2

Network visibility mitigates risks that cannot be addressed by EDR while also validating EDR telemetry.

Host-based security products such as EDR play a valuable role in ZTA. However, it is crucial to understand that EDR cannot be deployed on all endpoints. This leaves security gaps that require additional measures to mitigate.

Specialized devices such as IoT nodes may not be capable of running EDR agents. Similarly, operational technology (OT) and industrial control system (ICS) environments often contain hosts running proprietary or legacy operating systems that cannot run EDR agents or receive ongoing security patches. Unauthorized "shadow IT" nodes and instances of "malware IT," such as rogue virtual machines and microservices spawned by malware, will also operate without EDR when present. Therefore, monitoring network traffic for security threats is essential.

Risks may also persist even in cases where EDR software can be installed on hosts. While EDR products are designed to resist tampering, sophisticated threat actors have demonstrated their ability to exploit vulnerabilities in the operating systems that host EDR software, as well as firmware and hardware at levels below the operating system.

In its summary of the SolarWinds incident, threat intelligence and advisory firm Mandiant, Inc. found that once attackers compromised specific nodes, they took steps to circumvent or delete host-based logging mechanisms:

> Namely, Mandiant identified the threat actor disabling SysInternals Sysmon and Splunk Forwarders on victim machines that they accessed via Microsoft Remote Desktop in addition to clearing Windows Event Logs.[9]

Similar techniques were used during an insider attack against technology vendor Ubiquiti, Inc. According to security reporter Brian Krebs, the insider took steps to manipulate logging while also blaming the company for the lapses in leaks to the media:

> Among the claims made in those news stories was that Ubiquiti had neglected to keep access logs that would allow the company to understand the full scope of the intrusion. In reality, the indictment alleges, Sharp had shortened to one day the amount of time Ubiquiti's systems kept certain logs of user activity in AWS.[10]

Complementing host-based security technologies like EDR with optimized network detection and response (NDR) and SIEM capabilities based on network visibility data is the best way to mitigate these risks. For example, observation of network activity to a host that is not logged by EDR is a strong indicator of a compromise and possible efforts by adversaries to hide command and control traffic. In addition to serving as an additional point of validation, network visibility data is generated externally to any specific host, making it much more difficult for a threat actor to compromise.

Key Takeaways

- Network visibility provides important data about the state of the network, which is information organizations need to make accurate access decisions consistent with the guidance provided by SP 800-207.
- Network visibility mitigates risk associated with endpoints that cannot be protected by EDR solutions.
- Analysis of data about network traffic can validate the integrity of logs generated by network nodes such as endpoints.

To learn more about how Gigamon is enabling the adoption of ZTA principles at federal government organizations, download the following supporting materials:

Whitepaper

Pervasive Visibility: A Critical Foundation of Federal Zero Trust Architecture

Success Story

Gigamon Adds Crucial Network Visibility to Zero Trust at the Department of Defense

Gigamon Certifications and Authority to Operate (ATO)

- Department of Defense (DoDIN APL)
- DISA STIG and IPv6 compliant
- FIPS 140–2 validated
- NIAP Common Criteria
- Trade Agreement Act Compliant (TAA) + NEBS 3 compliant

Gigamon is authorized to operate in the U.S. Department of Defense's (DoD) Joint Regional Security Stack (JRSS) and many other DoD, intelligence community, and civilian agency networks.

- General Services Administration Schedules Program (GSA) Schedule 70
- NASA's Solutions for Enterprise-Wide Procurement (SEWP)

CAGE: 4XKN9
DUNS: 362737251

Gigamon is trusted by ten of the top ten U.S. federal agencies, leading DoD contractors, and vendors.

- Ten out of the top ten U.S. federal agencies have deployed Gigamon solutions
- 153 percent ROI improvement of the security stack[11]
- 50 percent decrease in costs associated with security efforts[11]
- 58 percent market share in the government sector, nearly five times the nearest competitor[12]
- #1 market leader with 38 percent market share, twice the market share of the nearest competitor[12]

References

1 Source: See Executive Order (EO) 14028 on Improving the Nation's Cybersecurity (accessed December 13, 2021), at Section 3.

2 Source: See NIST Special Publication 800-207 Zero Trust Architecture (accessed December 13, 2021)

3 Source: See OMB M-21-01 Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (accessed December 13, 2021) and OMB M-22-05 Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements (accessed December 13, 2021).

4 Source: See SP 800-207 at page 9.

5 Source: SP 800-207 at page 9. Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

6 Source: See SP 800-207 at Section 2.1 – Tenets of Zero Trust.

7 Source: See SP 800-207 at Section 3.4.1 – Network Requirements to Support ZTA.

8 Source: For example, network visibility provides helps organizations address log audit and validation requirements in OMB 21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (accessed December 13, 2021).

9 Source: See Suspected Russian Activity Targeting Government and Business Entities Around the Globe (accessed December 15, 2021).

10 Source: See Ubiquiti Developer Charged With Extortion, Causing 2020 'Breach' (accessed December 15, 2021).

11 Source: The Total Economic Impact™ of Gigamon, a commissioned study conducted by Forrester Consulting on behalf of Gigamon, April 2016.

12 Source: Network Monitoring Equipment Annual Market Report: Omdia, June 2020.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

04.23_02