How Gigamon Supports Department of Defense Zero Trust 152 Activities

A guide to managing cybersecurity risk with the Gigamon Deep Observability Pipeline.

BY STEPHEN GOUDREAULT

Table of Contents

Foundation for Zero Trust

Several years ago, the NSA, DISA, and U.S. Cyber Command (CYBERCOM) executed a multi-phase, ground-up Zero Trust reference architecture project to:

1. Establish stronger defenses against unauthorized lateral (East-West) movement inside the network perimeter
2. Protect against privilege escalation, including preventing adversaries from garnering privileges and gaining unauthorized system access
3. Eliminate and monitor blind spots identified by testing across the entire network, including physical and cloud infrastructure

During the initial planning and design process at the Technology Advancement Center (formerly MISI), which is CYBERCOM's open facility for innovation and collaboration with the private sector, the project team determined that a scalable, centralized visibility approach was a key requirement for the reference architecture. This led to reliance on the Gigamon Deep Observability Pipeline in various Zero Trust architecture (ZTA) implementations, beginning with their pilot site in a DoD network.

Gigamon provided a centralized approach for network traffic collection and routing, giving the tools responsible for enforcing ZTA policies the visibility they needed to be effective. The flexibility and modularity of the Gigamon architecture also helped the project team reduce traffic volumes and optimize performance. Gigamon capabilities such as Application Intelligence, Flow Mapping®, Tunneling, and De-duplication were used together to ensure that only relevant traffic data was sent to the tools for analysis, reducing performance load and costs. All of these functions were orchestrated through a single pane of glass with the GigaVUE-FM intent-based management and monitoring interface.

Gigamon continues to play an essential role in various pilot projects, including Dell Fort Zero, through its ability to support physical, virtual, and cloud networks with a unified deep observability pipeline.

Architectural Overview

Most organizations do not fully understand assets and traffic, and this represents a high level of vulnerability and organizational risk. While this issue, and the need to build security into all systems, is generally understood by network and security professionals, the challenge is how this can best be done. Modern systems are built in layers, and upper layers generally do not know or understand how lower layers work. A problem at a lower layer can have an impact on applications at a higher layer. Conversely, visibility at a lower layer can enrich applications running at higher layers.

Gigamon packet brokering capabilities are well situated to help with this lower layer lateral visibility. You can't protect what you can't see, and this is a foundational solution to any mature Zero Trust implementation. These packet broker capabilities that can sit in line or on taps that can then mirror or duplicate selected traffic to selected tools that can process the traffic.

Gigamon expanded beyond simple packet broker functions with deep packet inspection to bring deep observability that provides greater context into applications up to Layer 7. The focus is on seeing standard applications and protocols in flight. This can provide broad lateral visibility within a network. This broad lateral footprint in the network can extend to hybrid cloud deployments. You can't see where you don't sit, and a network tap cannot be evaded. Since Gigamon does not participate in the Layer 3 traffic stream, it has a wealth of visibility capabilities from Layer 2 to Layer 7. Layer 2 MAC addresses, DHCP options, Layer 3 protocol identification along with retransmits/errors, Layer 4 encryption and flow data, Layer 7 application identification, and lastly, performance instrumentation. Much of this information is discarded as one travels up and down the OSI stack. Gigamon deep observability can for the first time broadly answer the question, 'What is on the network?'

This visibility has been expanded into virtual environments. In on-premises, virtualized, and containerized (private cloud) environments, Gigamon can tap v-switches and workloads and see container

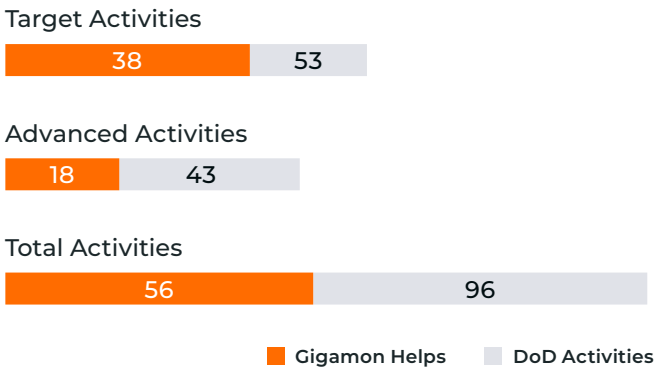
traffic. In the public cloud, Gigamon mirrors or duplicates traffic either through cloud provider tooling or the cloud-native GigaVUE® Universal Cloud Tap (UCT). This solution does not sit inline and can provide instrumentation of the traffic in hybrid environments, thereby unifying visibility.

Network logging is application blind, and it is being asked to solve a problem it was never designed to solve for. Network logs in their current form are important; SIEMs and analysts are typically overwhelmed by the volume of logs to process and do not provide the needed context to make them actionable. MITRE ATT&CK nonstandard port technique lists 41 threat actors observed using that technique and 51 forensic reports. Not once was the nonstandard port lateral movement detected internally by the network. It was detected by the EDR on forensic investigation or the NGFW on traffic egress. Known and unknown compute can be discovered; Gigamon can help solve for this visibility gap, which is critical to Zero Trust.

Threats and Zero Trust have evolved to the point where any single point of truth is insufficient. Workloads have EDR and MELT logging to back each other up. Routers and firewalls are the single source of truth in most designs. Gigamon can be an additional source of network logging that is performed in parallel to existing systems. The benefit of this system's behavior can be observed regardless of its internal state.

Gigamon has robust decryption solutions in classic on-premises configuration for North-South and lateral decryption. Additionally, Gigamon offers Gigamon Precryption™ technology, the industry's first solution to offer plaintext visibility into all encrypted communications across the cloud before the payload is encrypted, with no decryption required. This will not replace classic decryption but will open a whole new area of visibility into virtual environments.

Gigamon Helps Activities Across the Seven Pillars of the DoD Zero Trust Strategy



18% — 5 of 28 — User activities

36% — 9 of 24 — Device activities

6% — 1 of 18 — Application and Workload activities

19% — 6 of 31 — Data activities

86% — 11 of 13 — Network and Environment activities

50% — 10 of 20 — Automation and Orchestration activities

78% — 14 of 18 — Visibility and Analytics activities

Pillars, Activities, and Gigamon

The DoD Zero Trust Strategy outlines 152 activities across 45 capabilities and 7 pillars, each representing a critical area of protection. We have mapped Gigamon capabilities to these activities and will highlight how Gigamon aids or solves for each activity to provide architects with a quick and concise understanding of these activities. For completeness, all activities will have at least a single entry, even if Gigamon does not aid or solve for them, along with the DoD description of each activity.

For more detailed information, you can reference the appendix, which includes a practitioner-level breakdown of each activity.

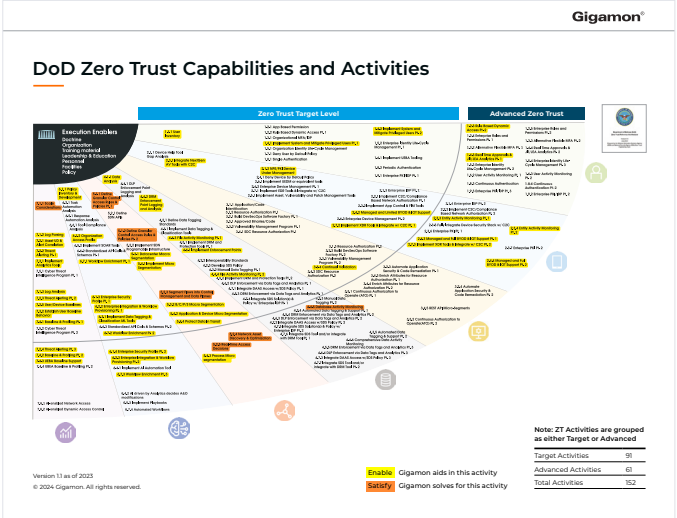


Figure 1. Activities Gigamon aids or solves for. View the detailed chart.

DoD Zero Trust Capabilities and Activities

User

1.1 User Inventory

1.2 Conditional User Access

1.3 Multi-Factor Authentication

1.4 Privileged Access Management

1.5 Identity Federation & User Credentialing

1.6 Behavioral, Contextual ID, and Biometrics

1.7 Least Privileged Access

1.8 Continuous Authentication

1.9 Integrated ICAM Platform

Device

2.1 Device Inventory

2.2 Device Detection and Compliance

2.3 Device Authorization with Real-Time Inspection

2.4 Remote Access

2.5 Partially & Fully Automated Asset, Vulnerability, and Patch Management

2.6 Unified Endpoint Management & Mobile Device Management

2.7 Endpoint & Extended Detection & Response

Application & Workload

3.1 Application Inventory

3.2 Secure Software Development & Integration

3.3 Software Risk Management

3.4 Resource Authorization & Integration

3.5 Continuous Monitoring and Ongoing Authorizations

Data

4.1 Data Catalog Risk Assessment

4.2 DoD Enterprise Data Governance

4.3 Data Labeling and Tagging

4.4 Data Monitoring and Sensing

4.5 Data Encryption & Rights Management

4.6 Data Loss Prevention

4.7 Data Access Control

Network & Environment

5.1 Data Flow Mapping

5.2 Software Defined Networking

5.3 Macro Segmentation

5.4 Micro Segmentation

Automation & Orchestration

6.1 Policy Decision Point & Policy Orchestration

6.2 Critical Process Automation

6.3 Machine Learning

6.4 Artificial Intelligence

6.5 Security Orchestration, Automation & Response

6.6 API Standardization

6.7 Security Operations Center & Incident Response

Visibility & Analytics

7.1 Log All Traffic (Network, Data, Apps, Users)

7.2 Security Information and Event Management

7.3 Common Security and Risk Analytics

7.4 User and Entity Behavior Analytics

7.5 Threat Intelligence Integration

7.6 Automated Dynamic Policies

EXECUTION ENABLERS:
Doctrine • Organization • Training • Material • Leadership & Education • Personal • Facilities • Policy

Figure 2. DoD Zero Trust Capabilities.

- Activities Gigamon aids.
- Activities Gigamon solves for.

Gigamon Support	ID#	Activity Name	Associated Capability
DoD ZERO TRUST STRATEGY FOR THE USER PILLAR			
	1.1	User Inventory	1 - User
●	1.1.1	Inventory User	1.1 User Inventory
	1.2	Conditional User Access	1 - User
●	1.2.3	Rule Based Dynamic Access Pt. 2	1.2 Conditional User Access
	1.3	Multi-Factor Authentication (MFA)	1 - User
	1.4	Privileged Access Management (PAM)	1 - User
●	1.4.1	Implement System and Migrate Privileged Users Pt. 1	1.4 Privileged Access Management (PAM)
●	1.4.2	Implement System and Migrate Privileged Users Pt. 2	1.4 Privileged Access Management (PAM)
●	1.4.3	Real time Approvals and JIT/JEA Analytics Pt. 1	1.4 Privileged Access Management (PAM)
	1.5	Identity Federation and User Credentialing	1 - User
	1.6	Behavioral, Contextual ID, and Biometrics	1 - User
●	1.6.1	Implement User and Entity Behavior Activity (UEBA) Tooling	1.6 Behavioral, Contextual ID, and Biometrics
●	1.6.2	User Activity Monitoring Pt. 1	1.6 Behavioral, Contextual ID, and Biometrics
●	1.6.3	User Activity Monitoring Pt. 2	1.6 Behavioral, Contextual ID, and Biometrics
	1.7	Least Privileged Access	1 - User
	1.8	Continuous Authentication	1 - User
	1.9	Integrated ICAM Platform	1 - User

Gigamon Support	ID#	Activity Name	Associated Capability
DoD ZERO TRUST STRATEGY FOR THE DEVICE PILLAR			
	2.1	Device Inventory	2 - Device
●	2.1.2	NPE/PKI, Device under Management	2.1 Device Inventory
	2.2	Device Detection and Compliance	2 - Device
	2.3	Device Authorization w/ Real Time Inspection	2 - Device
●	2.3.1	Entity Activity Monitoring Pt. 1	2.3 Device Authorization w/ Real Time Inspection
●	2.3.2	Entity Activity Monitoring Pt. 2	2.3 Device Authorization w/ Real Time Inspection
●	2.3.4	Integrate NextGen AV Tools with C2C	2.3 Device Authorization w/ Real Time Inspection
	2.4	Remote Access	2 - Device
●	2.4.2	Managed and Limited BYOD and IOT Support	2.4 Remote Access
●	2.4.3	Managed and Full BYOD and IOT Support Pt. 1	2.4 Remote Access
●	2.4.4	Managed and Full BYOD and IOT Support Pt. 2	2.4 Remote Access
	2.5	Partially and Fully Automated Asset, Vulnerability and Patch Management	2 - Device
	2.6	Unified Endpoint Management (UEM) and Mobile Device Management (MDM)	2 - Device
	2.7	Endpoint and Extended Detection and Response (EDR and XDR)	2 - Device
●	2.7.2	Implement Extended Detection and Response (XDR) Tools and Integrate with C2C Pt. 1	2.7 Endpoint and Extended Detection and Response (EDR and XDR)
●	2.7.3	Implement Extended Detection and Response (XDR) Tools and Integrate with C2C Pt. 2	2.7 Endpoint and Extended Detection and Response (EDR and XDR)

Gigamon Support	ID#	Activity Name	Associated Capability
DoD ZERO TRUST STRATEGY FOR THE APPLICATION & WORKLOAD PILLAR			
	3.1	Application Inventory	3 - Applications and Workloads
●	3.1.1	Application/Code Identification	3.1 Application Inventory
●	3.1.3	Resource Authorization Pt. 1	3.4 Resource Authorization and Integration
●	3.1.4	Resource Authorization Pt. 2	3.4 Resource Authorization and Integration
	3.2	Secure Software Development and Integration	3 - Applications and Workloads
	3.3	Software Risk Management	3 - Applications and Workloads
●	3.3.4	Continual Validation	3.3 Software Risk Management
	3.4	Resource Authorization and Integration	3 - Applications and Workloads
	3.5	Continuous Monitoring and Ongoing Authorizations	3 - Applications and Workloads

Gigamon Support	ID#	Activity Name	Associated Capability
DoD ZERO TRUST STRATEGY FOR THE DATA PILLAR			
	4.1	Data Catalog Risk Alignment	4 - Data
🟡	4.1.1	Data Analysis	4.1 Data Catalog Risk Alignment
	4.2	DoD Enterprise Data Governance	4 - Data
	4.3	Data Labeling and Tagging	4 - Data
	4.4	Data Monitoring and Sensing	4 - Data
🟡	4.4.2	File Activity Monitoring Pt. 1	4.4 Data Monitoring and Sensing
🟡	4.4.3	File Activity Monitoring Pt. 2	4.4 Data Monitoring and Sensing
🟡	4.4.4	Database Activity Monitoring	4.4 Data Monitoring and Sensing
🟠	4.4.5	Comprehensive Data Activity Monitoring	4.4 Data Monitoring and Sensing
	4.5	Data Encryption and Rights Management	4 - Data
	4.6	Data Loss Prevention (DLP)	4 - Data
🟡	4.6.1	Implement Enforcement Points	4.6 Data Loss Prevention (DLP)
	4.7	Data Access Control	4 - Data

Gigamon Support	ID#	Activity Name	Associated Capability
DoD ZERO TRUST STRATEGY FOR THE NETWORK & ENVIRONMENT PILLAR			
	5.1	Data Flow Mapping	5 - Network and Environment
●	5.1.1	Define Granular Control Access Rules and Policies Pt. 1	5.1 Data Flow Mapping
●	5.1.2	Define Granular Control Access Rules and Policies Pt. 2	5.1 Data Flow Mapping
	5.2	Software Defined Networking (SDN)	5 - Network and Environment
●	5.2.3	Segment Flows into Control, Management, and Data Planes	5.2 Software Defined Networking (SDN)
●	5.2.4	Network Asset Discovery and Optimization	5.2 Software Defined Networking (SDN)
●	5.2.5	Real-Time Access Decisions	5.2 Software Defined Networking (SDN)
	5.3	Macro Segmentation	5 - Network and Environment
●	5.3.1	Datacenter Macrosegmentation	5.3 Macro Segmentation
●	5.3.2	B/C/P/S Macrosegmentation	5.3 Macro Segmentation
	5.4	Micro Segmentation	5 - Network and Environment
●	5.4.1	Implement Microsegmentation	5.4 Micro Segmentation
●	5.4.2	Application and Device Microsegmentation	5.4 Micro Segmentation
●	5.4.3	Process Microsegmentation	5.4 Micro Segmentation
●	5.4.4	Protect Data In Transit	5.4 Micro Segmentation

Gigamon Support	ID#	Activity Name	Associated Capability
DoD ZERO TRUST STRATEGY FOR THE AUTOMATION & ORCHESTRATION PILLAR			
	6.1	Policy Decision Point (PDP) and Policy Orchestration	6 - Automation and Orchestration
●	6.1.1	Policy Inventory and Development	6.1 Policy Decision Point (PDP) and Policy Orchestration
●	6.1.2	Organization Access Profile	6.1 Policy Decision Point (PDP) and Policy Orchestration
●	6.1.3	Enterprise Security Profile Pt. 1	6.1 Policy Decision Point (PDP) and Policy Orchestration
●	6.1.4	Enterprise Security Profile Pt. 2	6.1 Policy Decision Point (PDP) and Policy Orchestration
	6.2	Critical Process Automation	6 - Automation and Orchestration
●	6.2.2	Enterprise Integration and Workflow Provisioning Pt. 1	6.2 Critical Process Automation
●	6.2.3	Enterprise Integration and Workflow Provisioning Pt. 2	6.2 Critical Process Automation
	6.3	Machine Learning	6 - Automation and Orchestration
●	6.3.1	Implement Data Tagging and Classification ML Tools	6.3 Machine Learning
	6.4	Artificial Intelligence	6 - Automation and Orchestration
	6.5	Security Orchestration, Automation and Response (SOAR)	6 - Automation and Orchestration
	6.6	API Standardization	6 - Automation and Orchestration
	6.7	Security Operations Center (SOC) and Incident Response (IR)	6 - Automation and Orchestration
●	6.7.1	Workflow Enrichment Pt. 1	6.7 Security Operations Center (SOC) and Incident Response (IR)
●	6.7.2	Workflow Enrichment Pt. 2	6.7 Security Operations Center (SOC) and Incident Response (IR)
●	6.7.3	Workflow Enrichment Pt. 3	6.7 Security Operations Center (SOC) and Incident Response (IR)

Gigamon Support	ID#	Activity Name	Associated Capability
DoD ZERO TRUST STRATEGY FOR THE VISIBILITY & ANALYTICS PILLAR			
	7.1	Log All Traffic (Network, Data, Apps, Users)	7 - Visibility and Analytics
●	7.1.1	Scale Considerations	7.1 Log All Traffic (Network, Data, Apps, Users)
●	7.1.2	Log Parsing	7.1 Log All Traffic (Network, Data, Apps, Users)
●	7.1.3	Log Analysis	7.1 Log All Traffic (Network, Data, Apps, Users)
	7.2	Security Information and Event Management (SIEM)	7 - Visibility and Analytics
●	7.2.1	Threat Alerting Pt. 1	7.2 Security Information and Event Management (SIEM)
●	7.2.2	Threat Alerting Pt. 2	7.2 Security Information and Event Management (SIEM)
●	7.2.3	Threat Alerting Pt. 3	7.2 Security Information and Event Management (SIEM)
●	7.2.4	Asset ID and Alert Correlation	7.2 Security Information and Event Management (SIEM)
●	7.2.5	User/Device Baselines	7.2 Security Information and Event Management (SIEM)
	7.3	Common Security and Risk Analytics	7 - Visibility and Analytics
●	7.3.1	Implement Analytics Tools	7.3 Common Security and Risk Analytics
●	7.3.2	Establish User Baseline Behavior	7.3 Common Security and Risk Analytics
	7.4	User and Entity Behavior Analytics	7 - Visibility and Analytics
●	7.4.1	Baseline and Profiling Pt. 1	7.4 User and Entity Behavior Analytics
●	7.4.2	Baseline and Profiling Pt. 2	7.4 User and Entity Behavior Analytics
●	7.4.3	UEBA Baseline Support Pt. 1	7.4 User and Entity Behavior Analytics
●	7.4.4	UEBA Baseline Support Pt. 2	7.4 User and Entity Behavior Analytics
	7.5	Threat Intelligence Integration	7 - Visibility and Analytics
	7.6	Automated Dynamic Policies	7 - Visibility and Analytics

Conclusion

Zero Trust is challenging. It is important to have a guiding framework and then understand which solutions map to which activities. There is a gap in operationalizing such a broad and complex framework. Architects should have other vendors map their solutions to a common framework such as this one so there can be better understanding of where orgs have existing solutions and where there are gaps that need to be addressed. Having a unifying framework is also important, as no one group will have diverse enough domain knowledge to understand every aspect of the activities. As this risk framework matures, it will naturally influence future compliance frameworks. This is a pioneering effort in terms of size, scope, and ambition.

If an organization is struggling with getting started with Zero Trust, narrow down a sample size for initial testing. Select some data from within your company and designate it as special. See who and what can access that data, see who needs access, and start to limit and protect access to it. Apply these rules to that subnet of special data and slowly work your way across the enterprise.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived intelligence to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations.

To learn more, please visit gigamon.com.

Appendix

Description of Solutions

This section will go deeper into the solutions. The solutions will have a DoD description of the activity and a second entry on how Gigamon either aids or solves for the activity.

All pillars are referenced here. However only sub activities (for example 1.1.1) are listed if Gigamon has a compensating aid or solves for an activity in that area. The source of these activity descriptions can be found here: DoD Zero Trust Capability Execution Roadmap (COA 1).

The descriptions are repeated here for ease of reference.

1 User

1.1 USER INVENTORY

Description
Regular and Privileged users are identified and integrated into an inventory supporting regular modifications. Applications, software and services that have local users are all part of the inventory and highlighted.

Outcome
System owners have control (visibility and administrative rights) of all authorized and authenticated users on the network. Users not authorized will be denied access.

1.1.1 User Inventory
Identified Managed Regular Users; Identified Managed Privileged Users; Identified applications using their own user account management for non-administrative and administrative accounts

How Gigamon Helps
Most user inventory approaches will start from the source-of-truth directory service, such as Active Directory. An important check on the directory service is to complement the inventory with a summary of which users are communicating over the network (identified by SRC/DST IP address mapped back to directory service). It is likely there will be many users in the directory service who are not actually present on the network, and there could also be some communications from hosts that are not known to the directory service but nonetheless allowed to communicate, hence could be missed without the network intelligence check. The Gigamon Deep Observability Pipeline provides exactly this actionable network intelligence, across hybrid cloud and multi-public cloud, even if different directory services are used for different platforms.

1.2 CONDITIONAL ACCESS

Description
Through maturity levels Conditional Access works to create a dynamic level of access for users in the environment. This starts with traditional role-based access controls across a federated ICAM, expands to be application focused roles and ultimately utilizes enterprise attributes to provide dynamic access rules.

Outcome
Eventually, organizations control user, device, and non-user entity DAAS access through dynamically changing user risk profiles and fine-grained access control to include the use of user risk assessment

Users not known to the system and users who present an unacceptable degree of risk will be denied access with greater accuracy

1.2.3 Rule Based Dynamic Access (part 2)
Components and services are fully utilizing rules to enable dynamic access to applications and services; technology utilized for Rule Based Dynamic Access supports integration with AI/ML tooling

How Gigamon Helps
In a more advanced implementation of Conditional User Access, IoT devices would be profiled by an IoT security/profiling service that requires network telemetry to be complete and accurate across the enterprise, otherwise devices will be missed. The activity itself does not require complete visibility, but correctness and completeness of conditional user ("user" = IoT device category) access would require network visibility via the Deep Observability Pipeline. Also, visibility from high-fidelity telemetry into cloud platform, instance, VM, container, and user attributes across all network traffic would enhance the dynamic access controls to applications and services.

1.4 - PRIVILEGED ACCESS MANAGEMENT (PAM)

Description
The capability focuses on removal of permanent administrator/elevated privileges by first creating a Privileged Account Management (PAM) system and migrating privileged users to it. The capability is then expanded upon by using automation with privilege escalation approvals and feeding analytics into the system for anomaly detection.

Outcome
DoD organizations control, monitor, secure, and audit privileged identities (e.g., through password vaulting, JIT/JEA with PAWS) across their IT environments. Critical assets and applications secured, controlled, monitored and managed through limits on admin access

1.4.1 - Privileged Access Management (PAM)
Privilege Access Management (PAM) tooling is implemented; identified applications that support and do not support PAM tools; applications that support PAM, now use PAM for controlling emergency/built-in accounts

How Gigamon Helps
Visibility into user attributes, cloud resource access and utilization reduce the attack surface, ensuring users have only the necessary privileges. To enable more automated discovery of privilege escalation situations, network-level intelligence, in combination with cluster analysis and role classification, can be used to identify individual users who typically act like one kind of user but have privileges that are out of sync with those users. This analysis can be done in a static/theoretical way as a strong start, but network intelligence will inform an analysis based on actual user behavior.

1.4.2 - Implement System and Migrate Privileged Users Pt2
Privileged activities are migrated to PAM and access is fully managed

How Gigamon Helps
To enable more automated discovery of Privilege Escalation situations, visibility into user attributes, cloud resources access and utilization, and network-level intelligence, in combination with cluster analysis, can be used to identify individual users who typically act like one kind of user but have privileges that are out of sync with those users. This analysis can be done in a static/theoretical way as a strong start, but network intelligence will inform an analysis based on actual user behavior.

1.4.3 - Real time Approvals and JIT/JEA Analytics Pt1
Identified accounts, applications, and data of concern (of greatest risk to DoD mission); using PAM tools, applied JIT/JEA access to high-risk accounts; privileged access requests are automated as appropriate

How Gigamon Helps
To enable more automated discovery of privilege escalation situations, network-level intelligence in combination with cluster analysis and role classification can be used to identify individual users who typically act like one kind of user but have privileges that are out of sync with those users. This analysis can be done in a static/theoretical way as a strong start, but network intelligence with user attribution and cloud resources usage will inform an analysis based on actual user behavior.

1.6 - BEHAVIORAL, CONTEXTUAL ID, AND BIOMETRICS

Description
Utilizing the Enterprise IDP, user and entity behavioral analytics (UEBA) are enabled with basic user attributes. Once completed this is expanded into Organizational specific attributes using Organizational IDPs as available. Finally, UEBA are integrated with the PAM and JIT/JEA systems to better detect anomalous and malicious activities.

Outcome
DoD organizations utilize behavioral, contextual, and biometric telemetry to enhance risk-based authentication and access controls. Behavioral, contextual, and biometric telemetry enhances MFA with user activity monitoring.

1.6.1 - Implement User and Entity Behavior Activity (UEBA) Tooling
UEBA functionality is implemented for Enterprise IDP

How Gigamon Helps
The Gigamon Deep Observability Pipeline is the most efficient way to provide network intelligence on all users and entities, across all domains, into a centralized UEBA system. Roles and permissions must be determined by the business, but should not be done in a vacuum, i.e., without knowledge of actual patterns of user behavior, such as which users access which resources and applications with what frequency. Network intelligence, visualized in various tools, can provide a baseline of actual communications which can inform cluster analysis to suggest useful role groupings and can validate whether suggested role-permission combinations are in fact utilized.

1.6.2 - User Activity Monitoring Pt1
UEBA is integrated with Org IDPs as appropriate; UEBA is integrated with JIT/JEA for critical services

How Gigamon Helps
The Gigamon Deep Observability Pipeline is the most efficient way to provide network intelligence on all users and entities, across all domains, into a centralized UEBA system. Roles and permissions must be determined by the business, but should not be done in a vacuum, i.e., without knowledge of actual patterns of user behavior, such as which users access which resources and applications with what frequency. Network intelligence, visualized in various tools, can provide a baseline of actual communications which can inform cluster analysis to suggest useful role groupings and can validate whether suggested role-permission combinations are in fact utilized.

1.6.3 - User Activity Monitoring Pt2
UEBA/Entity Monitoring is integrated with JIT/JEA for all services

How Gigamon Helps
The Gigamon Deep Observability Pipeline is the most efficient way to provide network intelligence on all users and entities, across all domains, into a centralized UEBA system. Roles and permissions must be determined by the business, but should not be done in a vacuum, i.e., without knowledge of actual patterns of user behavior, such as which users access which resources and applications with what frequency. Network intelligence, visualized in various tools, can provide a baseline of actual communications which can inform cluster analysis to suggest useful role groupings, and can validate whether suggested role-permission combinations are in fact utilized.

2 Device

2.1 - DEVICE INVENTORY

Description
DoD organizations establish and maintain an approved inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection. Device attributes will include technical details such as the PKI (802.1x) machine certificate, device object, patch/vulnerability status and others to enable successor activities.

Outcome
DoD organizations establish and maintain a trusted inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection. By default policy, devices will be denied network access; the only devices permitted access to the network shall be known, authorized, and listed in the device inventory.

2.1.2 - NPE/PKI, Device under Management

How Gigamon Helps
This is supported in part by the deep observability of network traffic that Gigamon provides. By collecting network information, a dataset can be collected and made to compare to device management tools and logs, particularly for NPEs at scale.

2.3 - Device Authorization w/ Real Time Inspection

Description
DoD Organizations conduct foundational and extended device tooling (NextGen AV, AppControl, File Integrity Monitoring (FIM), etc.) integration to better understand the risk posture. Organizational PKI systems are integrated to expand the existing Enterprise PKI to devices as well. Lastly Entity Activity Monitoring is also integrated to identify anomalous activities.

Outcome
DoD organizations establish processes (e.g., Enterprise PKI) and utilize tools to identify any device (including unmanaged devices, infrastructure devices, and endpoint devices) attempting to access the network, and make a determination if the device should be authorized to access the network. Maturation of this capability monitoring and detection of this activity on endpoints and IT infrastructure in real time. Components can use policies to deny devices by

default and explicitly allow access to DAAS resources only by devices that meet mandated configuration standards. Unknown devices and security threats are detected faster through continuous traffic monitoring, which enables quicker remediation.

2.3.1 Entity Activity Monitoring Pt1
UEBA attributes are integrated for device baselining; UEBA attributes are available for usage with device access

How Gigamon Helps
This is supported in part by the deep observability Gigamon provides into network traffic. By collecting network information, a dataset can be collected and analyzed in a SIEM tool, revealing all the users/entities in the network, both managed and unmanaged, including OT. Real-time UEBA attributes may be collected from deep packet inspection. Entity Activity Monitoring should include the network view, in addition to any endpoint-provided view such as from an EDR-type agent. The network view provides the "ground truth" of the entity's actual activity in terms of communication with other entities and resources. The Deep Observability Pipeline provides visibility not just on the immediate network, e.g., within a given public cloud platform, but also across multiple public clouds and between public cloud and private cloud or traditional on-prem.

2.3.2 Entity Activity Monitoring Pt2
UEBA attributes are mandated for device access

How Gigamon Helps
This is supported in part by deep observability Gigamon provides into network traffic. By collecting network information, a dataset can be collected and analyzed in a SIEM tool, revealing all the users/entities in the network, both managed and unmanaged, including OT. Real-time UEBA attributes may be collected from deep packet inspection. The AI-enabled dynamic access control would depend on the tool used to analyze the network traffic.

2.3.4 Integrate NextGen AV Tools with C2C
Critical NextGen AV data is being sent to C2C for checks; NextGen AV tooling is implemented on all critical services/applications

How Gigamon Helps
Entity Activity Monitoring should include the network view, in addition to any endpoint-provided view such as from an EDR-type agent. The network view provides the "ground truth" of the entity's actual activity in terms of communication with other entities and resources. The Deep Observability Pipeline provides visibility not just on the immediate network, e.g., within a given public cloud platform, but also across multiple public clouds and between public cloud and private cloud or traditional on-prem.

2.4 - REMOTE ACCESS

Description
DoD organizations audit existing device access processes and tooling to set a least privilege baseline. In phase 2 this access is expanded to cover basic BYOD and IOT support using the Enterprise IDP for approved applications. The final phases expand coverage to include all BYOD and IOT devices for services using the approved set of device attributes.

Outcome
DoD organizations establish policies to allow authorized users and devices access to the network or a device from a geographical distance through a network connection. Enables properly authorized and authenticated users and NPEs to access DAAS from remote locations

2.4.2 - Managed and Limited BYOD and IOT Support
All applications require dynamic permissions access for devices; BYOD and IOT device permissions are baselined and integrated with Enterprise IDP

How Gigamon Helps
Network visibility is essential for any IOT support at scale. Zero Trust principles require that IOT devices are appropriately authorized to the correct IOT-relevant resources, which depends on visibility in to what they are. The Deep Observability Pipeline ensures no devices are missed, enabling full IOT support with the same security posture as managed devices.

2.4.3 - Managed and Full BYOD and IOT Support Pt1
Only BYOD and IOT devices that meet mandated configuration standards allowed to access resources; Critical Services require dynamic access for devices

How Gigamon Helps
Network visibility is essential for any IOT support at scale. Zero Trust principles require that IOT devices are appropriately authorized to the correct IOT-relevant resources, which depends on visibility in to what they are. The Deep Observability Pipeline ensures no devices are missed, enabling full IOT support with the same security posture as managed devices. The metadata Gigamon generates can observe BYOD and IOT behaviors.

2.4.4 - Managed and Full BYOD and IOT Support Pt2
All possible services require dynamic access for devices

How Gigamon Helps
Network visibility is essential for any IOT support at scale. Zero Trust principles require that IOT devices are appropriately authorized to the correct IOT-relevant resources, which depends on visibility to what they are. The Deep Observability Pipeline ensures no devices are missed, enabling full IOT support with the same security posture as managed devices.

2.7 - Endpoint and Extended Detection and Response (EDR and XDR)

Description
DoD organizations use endpoint detection and response (EDR) tooling to monitor, detect, and remediate malicious activity on endpoints. Expanding the capability to include XDR tooling allows organizations to account for activity beyond the endpoints such as cloud and network as well.

Outcome
DoD organizations use EDR tools to monitor, detect, and remediate malicious activity on endpoints as a baseline. Upgrading to XDR tools allows organizations to account for activity beyond the endpoints. Threats originating from network-connected endpoints are initially reduced through active investigation and response. Maturation focuses on forensics and faster threat detection and remediation are enabled by correlating data across multiple security layers (e.g., email, cloud, endpoint)

2.7.2 Implement Extended Detection and Response (XDR) Tools and Integrate with C2C Pt1
Integration Points have been identified per Capability; riskiest integration points have been integrated w/ XDR; basic alerting is in place with SIEM and/or other mechanisms

How Gigamon Helps
Extended detection and response tools require network-based visibility alongside endpoint-based visibility and possibly log analysis for the complete view. The Gigamon Deep Observability Pipeline provides complete network intelligence for all workloads in all environments, making a given XDR tool extensible across the entire organization and IT estate versus just within a specific siloed domain or cloud platform.

2.7.3 Implement Extended Detection and Response (XDR) Tools and Integrate with C2C Pt2
Remaining integration points have been integrated as appropriate; extended alerting and response is enabled with other Analytics tools at least using SIEM

How Gigamon Helps
Extended detection and response tools require network-based visibility alongside endpoint-based visibility and possibly log analysis for the complete view. The Gigamon Deep Observability Pipeline provides complete network intelligence for all workloads in all environments, making a given XDR tool extensible across the entire organization and IT estate versus just within a specific siloed domain or cloud platform.

3 Application and Workload

3.1 - APPLICATION INVENTORY

Description
System owners ensure that all applications and application components are identified and inventoried; only applications and application components that have been authorized by the appropriate authorizing official/CISO/CIO shall be utilized within the system owner's purview

Outcome
System owners ensure that all applications and application components are identified and inventoried; only applications and application components that have been authorized by the appropriate authorizing official/CISO/CIO shall be utilized within the system owner's purview. Unauthorized applications and application components are not used on or within the system

3.1.1 - Application/Code Identification
Component has identified applications and classified as either legacy, virtualized on-premises, and cloud hosted

How Gigamon Helps
Deep observability into network traffic and AMI capabilities provide visibility and metadata about applications communicating on the network, SDNs or in containers.

3.2.3 - Resource Authorization Pt1
Resource Authorization Gateway is in place for external facing applications; Resource Authorization policy integrated with identity and device; Enterprise-wide Guidance on conversion standards are communicated to stakeholders

How Gigamon Helps
Deep observability into network traffic and AMI capabilities provide visibility and metadata about applications communicating on the network, SDNs, or in containers.

3.1.4 - Resource Authorization Pt2
Resource Authorization gateway is utilized for all applications; Resource Authorization is integrated with DevSecOps and CI/CD for automated functions

How Gigamon Helps
Deep observability into network traffic and AMI capabilities provide visibility and metadata about applications communicating on the network, SDNs, or in containers.

3.3 - SOFTWARE RISK MANAGEMENT

Description
DoD organizations establish software/application risk management programs. Foundational controls include Bill of Materials risk management, Supplier Risk Management, approved repositories and update channels, and vulnerability management program. Additional controls include Continual validation within the CI/CD pipelines and vulnerability maturation with external sources.

Outcome
DoD establishes policies and procedures to secure supply chain cybersecurity for code components within DoD and DIB systems by evaluating and identifying supplier sourcing risk for approved sources, creating repositories and update channels for use by development teams, creating Bill of Materials for applications to identify source, supportability and risk posture, and establishing industry standard (DIB) and approved vulnerability databases for use in DevSecOps. Code used in DAAS and associated components of the supply chain is secure, vulnerabilities are reduced, and DoD is aware of potential risks

3.3.4 - Continual Validation
Updated Applications are deployed in a live and/or production environment; Applications that were marked for retirement and transition are decommissioned; Continual validation tools are implemented and applied to code in the CI/CD pipeline; Code requiring continuous validation is identified and validation criteria are established

How Gigamon Helps
Deep observability into network traffic and AMI capabilities provide visibility and metadata about applications communicating on the network, SDNs, or in containers. This metadata can be sent to a SIEM for continuous monitoring of systems and identify vulnerable protocols and applications communicating.

4 Data

4.1 - DATA CATALOG RISK ALIGNMENT

Description
Data owners ensure that data is identified and inventoried and any changes to the data landscape are automatically detected and included within the catalog. The data landscape must then be reviewed to identify potential risks related to data loss, attack, or any other unauthorized alteration and/or access

Outcome
Data owners ensure that data is identified and inventoried and any changes to the data landscape are automatically detected and included within the catalog. The data landscape must then be reviewed to identify potential risks related to data loss, attack, or any other unauthorized alteration and/or access. Data assets are known and can therefore be collected, tagged, and protected according to risk levels in alignment with a prioritization framework, and encrypted for protection

4.1.1 - Data Analysis
The service catalog is updated with data types for each application and service based on data classification levels

How Gigamon Helps
Deep observability into network traffic and AMI capabilities provide continuous visibility and metadata generation for application and system communication about applications communicating on the network, SDNs, or in containers. This metadata can be sent to a SIEM for continuous monitoring of systems and identify vulnerable protocols and applications communicating that can be used in continuous ATOs. Gigamon can assist with detecting changes in the landscape, specifically the network, by allowing users to identify potential risks to data loss, attacks, or unauthorized alterations and/or access as the data is in transit across the network. Data owners ensure that data is identified and inventoried and any changes to the data landscape are automatically detected and included within the catalog. The data landscape must then be reviewed to identify potential risks related to data loss, attack, or any other unauthorized alteration and/or access.

4.4 - DATA MONITORING AND SENSING

Description
Data owners will capture active metadata that includes information about the access, sharing, transformation, and use of their data assets. Data Loss Prevention (DLP) and Data Rights Management (DRM) enforcement point analysis is conducted to determine where tooling will be deployed. Data outside of DLP and DRM scope such as File Shares and Databases is actively monitored for anomalous and malicious activity using alternative tooling.

Outcome
Data owners will capture active metadata that includes information about the access, sharing, transformation, and use of their data assets. Data in all states are detectable and observable

4.4.2 - File Activity Monitoring Pt1
Data and files of critical classification are actively being monitored; Basic Integration is in place with monitoring system such as the SIEM

How Gigamon Helps
Deep Observability into network traffic and AMI capabilities provide continuous visibility and metadata generation for application and system communication about applications communicating on the network, SDNs, or in containers. This metadata can be sent to a SIEM for continuous monitoring of systems and identify vulnerable protocols and applications communicating that can be used in Continuous ATOs. Gigamon can assist with detecting changes in the landscape, specifically the network, by allowing users to identify potential risks to data loss, attacks, or unauthorized alterations and/or access as the data is in transit across the network.

4.4.3 - File Activity Monitoring Pt2
Data and files of all regulated classifications are actively being monitored; Extended integrations are in place as appropriate to further manage risk

How Gigamon Helps
Deep observability into network traffic and AMI capabilities provide continuous visibility and metadata generation for application and system communication about applications communicating on the network, SDNs, or in containers. This metadata can be sent to a SIEM for continuous monitoring of systems and identify vulnerable protocols and applications communicating that can be used in Continuous ATOs. Gigamon can assist with detecting changes in the landscape, specifically the network, by allowing users to identify potential risks to data loss, attacks, or unauthorized alterations and/or access as the data is in transit across the network.

4.4.4 - Database Activity Monitoring
Appropriate Database are being actively monitored; Monitoring technology is integrated with solutions such as SIEM, PDP and Dynamic Access Control mechanisms

How Gigamon Helps
Deep observability into network traffic and AMI capabilities provide continuous visibility and metadata generation for application and system communication about applications communicating on the network, SDNs, or in containers. This metadata can be sent to a SIEM for continuous monitoring of systems and identify vulnerable protocols and applications communicating that can be used in Continuous ATOs. Gigamon

can assist with detecting changes in the landscape, specifically the network, by allowing users to identify potential risks to data loss, attacks, or unauthorized alterations and/or access as the data is in transit across the network.

4.4.5 - Comprehensive Data Activity Monitoring
Data Activity monitoring mechanisms are integrated to provide a unified view of monitoring across data repositories; Appropriate integrations exist with solutions such as SIEM and PDP

How Gigamon Helps
Deep observability into network traffic and AMI capabilities provide continuous visibility and metadata generation for application and system communication about applications communicating on the network, SDNs, or in containers. This metadata can be sent to a SIEM for continuous monitoring of systems and identify vulnerable protocols and applications communicating that can be used in Continuous ATOs. Gigamon can assist with detecting changes in the landscape, specifically the network, by allowing users to identify potential risks to data loss, attacks, or unauthorized alterations and/or access as the data is in transit across the network.

4.6 - DATA LOSS PREVENTION (DLP)

Description
DoD organizations utilize the identified enforcement points to deploy approved DLP tools and integrate tagged data attributes with DLP. Initially the DLP solution is put into a “monitor-only” mode to limit business impact and later using analytics is put into a “prevent” mode. Extended data tag attributes are used to feed the DLP solution and lastly integrate with ML and AI.

Outcome
DoD organizations have identified enforcement points, deployed approved DLP tools at those enforcement points, and integrate tagged data attributes with DLP. Data breaches and data exfiltration transmissions are detected and mitigated

4.6.1 - Implement Enforcement Points
Identified enforcement points have DLP tool deployed and set to monitor mode with standardized logging

How Gigamon Helps
Deep observability network traffic and AMI capabilities provide continuous visibility and metadata generation for application and system communication about applications communicating on the network, SDNs, or in containers. This metadata can be sent to a SIEM for continuous monitoring of systems and identify vulnerable protocols and applications communicating that can be used in Continuous ATOs. This can be deployed across a micro segmented network and can continue to scale with the growth of the network. Gigamon can use out-of-band network traffic collection, which passively monitors the network and sends packet data over to logging tools in a standardized fashion.

5 Network and Environment

5.1 - DATA FLOW MAPPING

Description
DoD organizations reconcile data flows by gathering, mapping, and visualizing network traffic data flows and patterns to ensure authorized access and protection for network and DAAS resources specifically tagging programmatic (e.g., API) access when possible.

Outcome
DoD organizations reconcile data flows by gathering, mapping, and visualizing network traffic data flows and patterns to ensure authorized access and protection for network and DAAS resources. Sets the foundation for network segmentation and tighter access control by understanding data traffic on the network

5.1.1 - Define Granular Control Access Rules and Policies Pt1
Provide Technical Standards; Develop Concept of Operations; Identify Communities of Interest

How Gigamon Helps
Gigamon observes traffic in motion and helps identify communication patterns which can be used for developing rules. Gigamon observes applications and traffic usage patterns to help define access control rules.

5.1.2 - Define Granular Control Access Rules and Policies Pt2
Define Data Tagging Filters for API Infrastructure

How Gigamon Helps
Gigamon observes traffic in motion and helps identify communication patterns which can be used for developing rules. Gigamon observes apps and traffic usage patterns to help define access control rules.

5.2 - Software Defined Networking (SDN)

Description
DoD organizations define API decision points and implement SDN programmable infrastructure to separate the control and data planes and centrally manage and control the elements in the data plane. Integrations are conducted with decision points and segmentation gateway to accomplish the plane separation. Analytics are then integrated to real time decision making for access to resources.

Outcome
DoD organizations define API decision points and implement SDN programmable infrastructure to separate the control and data planes and centrally manage and control the elements in the data plane. Enables the control of packets to a centralized server, provides additional visibility into the network, and enables integration requirements

5.2.3 - Segment Flows into Control, Management, and Data Planes
IPv6 Segmentation; Enable Automated NetOps Information Reporting; Ensure Configuration Control Across Enterprise; Integrated with SOAR

How Gigamon Helps
Gigamon can observe all traffic/apps in flight from source/destination across administrative boundaries. Gigamon can help with establishing visibility to assist in segmentation planning and then provide continuous visibility to verify guard rails are in place and working.

5.2.4 - Network Asset Discovery and Optimization
Technical Refreshment/Technology Evolution; Provide Optimization/Performance Controls

How Gigamon Helps
The Gigamon Deep Observability Pipeline is the most efficient way to acquire and aggregate the network visibility across hybrid cloud and multi-cloud domains for a complete network asset discovery. Gigamon observes network traffic in motion. This give a unique perspective on performance as low-level physical and protocols errors can be observed. Additionally, adding application visibility to flows can help identify if the network or workload is slow. This visibility can span beyond administrative and technical boundaries. i.e., outside the network.

5.2.5 - Real-Time Access Decisions
Analyze SIEM Logs with Analytics Engine to Provide Real-Time Policy Access Decisions; Support Sending Captured Packets, Data/Network Flows, and other Specific Logs for Analytics; Segment End-to-End Transport Network Flows; Audit Security Policies for Consistency across Enterprise; Protect Data-in-Transit During Coalition Information Sharing

How Gigamon Helps
The Gigamon Deep Observability Pipeline is the most efficient way to acquire and aggregate the network visibility across hybrid cloud and multi-cloud domains for a complete network asset discovery. Gigamon can make network logs application aware. This increases the depth of visibility SIEMS have to enrich decision-making

5.3 - MACRO SEGMENTATION

Description
DoD organizations establish network boundaries and provide security against networked assets located within an environment by validating the device, user, or NPE on each attempt of accessing a remote resource prior to connection.

Outcome
DoD organizations establish network perimeters and provide security against devices located within an environment by validating the device, user, or NPE on each attempt of accessing a remote resource prior to connection. Network segmentation is defined by a large perimeter to enable resource segmentation by function and user type

5.3.1 - Datacenter Macrosegmentation
Log Actions to SIEM; Establish Proxy/Enforcement Checks of Device Attributes, Behavior, and other Data; Analyze Activities with Analytics Engine

How Gigamon Helps
Macro- and micro-segmentation strategies are around network structure, facilitated by traditional methods (e.g., VLAN for macro-segmentation) or more modern methods (e.g., role-based policies enforced independently of VLAN). These different types of segmentations can inadvertently create challenges for security monitoring. The Gigamon Deep Observability Pipeline overcomes these challenges by bringing end-to-end consistent telemetry across all segments into a centralized security tools stack, such that the benefits of segmentation (minimize blast radius, reduce lateral movement risk, etc.) do not conflict with the benefits of comprehensive security monitoring (complete view of the enterprise). Gigamon can help with establishing visibility to assist in segmentation planning and then provide continuous visibility to verify guard rails are in place and working.

5.3.2 - B/C/P/S Macrosegmentation
Establish Proxy/Enforcement Checks of Device Attributes, Behavior, and other Data; Log Actions to SIEM; Analyze Activities with Analytics Engine; Leverage SOAR to Provide RT Policy Access Decisions

How Gigamon Helps
Macro- and micro-segmentation strategies are around network structure, facilitated by traditional methods (e.g., VLAN for macro-segmentation) or more modern methods (e.g., role-based policies enforced independently of VLAN). These different types of segmentations can inadvertently create challenges for security monitoring. The Gigamon Deep Observability Pipeline overcomes these challenges by bringing end-to-end consistent telemetry across all segments into a centralized security tools stack, such that the benefits of segmentation (minimize blast radius, reduce lateral movement risk, etc.) do not conflict with the benefits of comprehensive security monitoring (complete view of the enterprise). Gigamon can help with establishing visibility to assist in segmentation planning and then provide continuous visibility to verify guard rails are in place and working.

5.4 - MICRO SEGMENTATION

Description
DoD organizations define and document network segmentation based on identity and / or application access in their virtualized and/or cloud environments. Automation is used to apply policy changes through programmatic (e.g., API) approaches. Lastly where possible organizations will utilize host-level process microsegmentation.

Outcome
DoD organizations define and document network segmentation based on identity and / or application access in their virtualized cloud environments. Network segmentation enabled by narrower and specific segmentation in a virtualized environment via identity and / or application access, allowing for improved protection of data in transit as it crosses system boundaries (e.g., in a coalition environment, system high boundaries) and supported dynamic, real-time access decisions and policy changes

5.4.1 - Implement Microsegmentation
Accept Automated Policy Changes; Implement API Decision Points; Implement NGF/Micro FW/Endpoint Agent in Virtual Hosting Environment

How Gigamon Helps
Macro- and micro-segmentation strategies are around network structure, facilitated by traditional methods (e.g., VLAN for macro-segmentation) or more modern methods (e.g., role-based policies enforced independently of VLAN). These different types of segmentations can inadvertently create challenges for security monitoring. The Gigamon Deep Observability Pipeline overcomes these challenges by bringing end-to-end consistent telemetry across all segments into a centralized security tools stack, such that the benefits of segmentation (minimize blast radius, reduce lateral movement risk, etc.) do not conflict with the benefits of comprehensive security monitoring (complete view of the enterprise). Gigamon can help with establishing visibility to assist in micro-segmentation planning and then provide continuous visibility to verify guard rails are in place and working.

5.4.2 - Application and Device Microsegmentation
Assign Role, Attribute, and Condition Based Access Control to User and Devices; Provide Privileged Access Management Services; Limit Access on Per Identity Basis for User and Device; Create Logical Network Zones; Support Policy Control via REST API

How Gigamon Helps
Macro- and micro-segmentation strategies are around network structure, facilitated by traditional methods (e.g., VLAN for macro-segmentation) or more modern methods (e.g., role-based policies enforced independently of VLAN). These different types of segmentations can inadvertently create challenges for security monitoring. The Gigamon Deep Observability Pipeline overcomes these challenges by bringing end-to-end consistent telemetry across all segments into a centralized security tools stack, such that the benefits of segmentation (minimize blast radius, reduce lateral movement risk, etc.) do not conflict with the benefits of comprehensive security monitoring (complete view of the enterprise) Gigamon can help with establishing visibility to assist in micro-segmentation planning and then provide continuous visibility to verify guard rails are in place and working.

5.4.3 - Process Microsegmentation
Segment Host-Level Processes for Security Policies; Support Real-Time Access Decisions and Policy Changes; Support Offload of Logs for Analytics and Automation; Support Dynamic Deployment of Segmentation Policy

How Gigamon Helps
Macro- and micro-segmentation strategies are around network structure, facilitated by traditional methods (e.g., VLAN for macro-segmentation) or more modern methods (e.g., role-based policies enforced independently of VLAN). These different types of segmentations can inadvertently create challenges for security monitoring. The Gigamon Deep Observability Pipeline overcomes these challenges by bringing end-to-end consistent telemetry across all segments into a centralized security tools stack, such that the benefits of segmentation (minimize blast radius, reduce lateral movement risk, etc.) do not conflict with the benefits of comprehensive security monitoring (complete view of the enterprise). Gigamon can help with establishing visibility to assist in micro-segmentation planning and then provide continuous visibility to verify guard rails are in place and working

5.4.4 - Protect Data In Transit
Protect Data In Transit During Coalition Information Sharing; Protect Data in Transit Across System High Boundaries; Integrate Data In Transit Protection Across Architecture Components

How Gigamon Helps
We verify data is encrypted in transit. Gigamon directly secures data-in-transit by providing SSL/TLS decryption for data-in-transit, providing visibility for full security analytics. Gigamon also enables security for data-in-transit overall by providing efficient, optimized, enriched, complete visibility to all data in transit from Layer 2/3 to Layer 4 to Layer 7. Encryption ciphers can also be detected to ensure modern encryption is in use.

6 Automation and Orchestration

6.1 - POLICY DECISION POINT (PDP) AND POLICY ORCHESTRATION

Description
DoD organizations initially collect and document all rule-based policies to orchestrate across the security stack for effective automation; DAAS access procedures and policies will be defined, implemented, and updated. Organizations mature this capability by establishing PDPs and PEPs (including the Next Generation Firewall) to make DAAS resource determinations and enable, monitor, and terminate connections between a user/device and DAAS resources according to predefined policy.

Outcome
DoD organizations initially collect and document all rule-based policies to orchestrate across the security stack for effective automation; DAAS access procedures and policies will be defined, implemented, and updated. Organizations mature this capability by establishing PDPs and PEPs (including the Next Generation Firewall) to make DAAS resource determinations and enable, monitor, and terminate connections between a user/device and DAAS resources according to predefined policy. PDPs and PEPs ensure proper implementation of DAAS access policies to users or endpoints that are properly connected (or denied access) to requested resources

6.1.1 - Policy Inventory and Development
Policies have been collected in reference to applicable compliance and risk (e.g. RMF, NIST); Policies have been reviewed for missing Pillars and Capabilities per the ZTRA; Missing areas of policies are updated to meet the capabilities per ZTRA

How Gigamon Helps
Gigamon observes and reports on network-wide East-West movement of known and unknown applications and protocols to help facilitate policy development, verification, and enforcement. Gigamon has NGFW application and protocol visibility in a much broader scope.

6.1.2 - Organization Access Profile
Organization scoped profile(s) are created to determine access to DAAS using capabilities from User, Data, Network, and Device pillars; Initial enterprise profile access standard is developed for access to DAAS; When possible, the organization profile(s) utilizes enterprise available services in the User, Data, Network and Device pillars; Organization Mission/Task critical profile(s) are created.

How Gigamon Helps
Gigamon observes and reports on network-wide East-West movement of known and unknown applications and protocols to help facilitate policy development, verification, and enforcement. Gigamon has NGFW application and protocol visibility in a much broader scope.

6.1.3 - Enterprise Security Profile Pt1
Enterprise Profile(s) are created to access DAAS using capabilities from User, Data, Network and Device Pillars; Non-mission/task critical organization profile(s) are integrated with the enterprise profile(s) using a standardized approach.

How Gigamon Helps
Gigamon observes and reports on network-wide East-West movement of known and unknown applications and protocols to help facilitate policy development, verification, and enforcement. Gigamon has NGFW application and protocol visibility in a much broader scope.

6.1.4 - Enterprise Security Profile Pt2
Enterprise Profile(s) have been reduced and simplified to support widest array of access to DAAS; Where appropriate Mission/Task Critical profile(s) have been integrated and supported Organization profiles are considered the exception

How Gigamon Helps
Gigamon observes and reports on network-wide East-West movement of known and unknown applications and protocols to help facilitate policy development, verification, and enforcement. Gigamon has NGFW application and protocol visibility in a much broader scope.

6.2 - CRITICAL PROCESS AUTOMATION

Description
DoD organizations employ automation methods, such as RPA, to address repetitive, predictable tasks for critical functions such as data enrichment, security controls, and incident response workflows according to system security engineering principles.

Outcome
DoD organizations employ automation methods, such as RPA, to address repetitive, predictable tasks for critical functions such as data enrichment, security controls, and incident response workflows according to system security engineering principles. Response time and capability is increased with orchestrated workflows and risk management processes

6.2.2 - Enterprise Integration and Workflow Provisioning Pt1
Implement full enterprise integration; Identify key integrations; Identify recovery and protection requirements

How Gigamon Helps
Gigamon observes and reports on network-wide East-West movement of known and unknown applications and protocols to help facilitate policy development, verification, and enforcement. Gigamon can make logs application aware via metadata and can solve for the nonstandard port use case

6.2.3 - Enterprise Integration and Workflow Provisioning Pt2
Services identified; Service provisioning is implemented

How Gigamon Helps
Gigamon observes and reports on network-wide East-West movement of known and unknown applications and protocols to help facilitate policy development, verification, and enforcement. Gigamon can make logs application aware via metadata and can solve for the nonstandard port use case.

6.3 - MACHINE LEARNING

Description
DoD organizations employ ML to execute (and enhance execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging.

Outcome
DoD organizations employ ML to execute (and enhance execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging. Response time and capability is increased with orchestrated workflows and risk management processes

6.3.1 - Implement Data Tagging and Classification ML Tools
Implemented data tagging and classification tools are integrated with ML tools

How Gigamon Helps
ML-based data classification requires a real-life dataset of what is being transferred and communicated, not just a static classification. The ML will be more effective including broader context, allowing unsupervised as well as supervised learning. Gigamon observes and reports on network-wide East-West movement of known and unknown applications and protocols to help facilitate policy development, verification, and enforcement.

6.7 – SECURITY OPERATIONS CENTER (SOC) AND INCIDENT RESPONSE (IR)

Description
In the event a computer network defense service provider (CNDSP) does not exist, DoD organizations define and stand-up security operations centers (SOC) to deploy, operate, and maintain security monitoring, protections and response for DAAS; SOCs provide security management visibility for status (upward visibility) and tactical implementation (downward visibility). Workflows within the SOC are automated using automation tooling and enrichment occurs between service providers and technologies.

Outcome
In the event a CNDSP does not exist, DoD organizations define and stand up SOCs to deploy, operate, and maintain security monitoring, protections and response for DAAS; SOCs provide security management visibility for status (upward visibility) and tactical implementation (downward visibility)

6.7.1 - Workflow Enrichment Pt1
Threat events are identified; Workflows for threat events are developed

How Gigamon Helps
Gigamon observes and reports on East-West movement of known and unknown applications and protocols to help facilitate better forensic capabilities for developing and executing workflows. Gigamon can make logs application aware via metadata and can solve for the nonstandard port use case.

6.7.2 - Workflow Enrichment Pt2
Workflows for Advanced threat events are developed; Advanced Threat events are identified

How Gigamon Helps
Gigamon observes and reports on East-West movement of known and unknown applications and protocols to help facilitate better forensic capabilities for developing and executing workflows. Gigamon can make logs application aware via metadata and can solve for the nonstandard port use case.

6.7.3 - Workflow Enrichment Pt3
Enrichment data has been identified; Enrichment data is integrated into workflows

How Gigamon Helps
Gigamon observes and reports on East-West movement of known and unknown applications and protocols to help facilitate better forensic capabilities for developing and executing workflows. Gigamon can make logs application aware via metadata and can solve for the nonstandard port use case.

7 Visibility and Analytics

7.1 – LOG ALL TRAFFIC (NETWORK, DATA, APPS, USERS)

Description
DoD organizations collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or security operations center (SOC). Logs and events follow a standardized format, and rules/analytics are developed as needed.

Outcome
DoD organizations collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or SOC

7.1.1 - Scale Considerations
Sufficient infrastructure in place; Distributed environment established; Sufficient bandwidth for network traffic

How Gigamon Helps
Gigamon can log in parallel or offload logging from network devices with Layer 2–7 visibility. This includes protocol information, protocol errors, encryption types, performance, round trip time, DNS information, plus much more. This visibility through external observation of traffic can span administrative and technical boundaries to enable broad East-West visibility into on-prem, private, public, and multi-cloud environments.

7.1.2 - Log Parsing
Standardized log formats; Rules developed for each log format

How Gigamon Helps
Gigamon can provide standard network, application, protocol, and performance logging across on-prem, private, public, and multi-cloud in standard log formats. Logging generated from hybrid environments will be in a unified format as well.

7.1.3 - Log Analysis
Develop analytics per activity; Identify activities to analyze

How Gigamon Helps
Rather than analyzing only logs from network devices, “logging” should include records of network-based metadata, which gives a true record of actual communications between entities and resources across all types of environments and networks, including on-prem, private cloud, and public cloud.

7.2 – SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Description
Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) monitor, detect, and analyze data logged into a security information and event management (SIEM) tool. User and device baselines are created using security controls and integrated with the SIEM. Alerting within the SIEM is matured over the phases to support more advanced data points (e.g., Cyber Threat Intel, Baselines, etc.)

Outcome
CNDSPs/SOCs monitor, detect, and analyze data logged into a security information and event management (SIEM) tool

7.2.1 - Threat Alerting Pt1
Rules developed for threat correlation

How Gigamon Helps
Gigamon makes classic network logging application aware by adding Layer 2–7 visibility and context. Many network threats use misconfigured apps and protocols, which Gigamon can make visible in lateral movement in on-prem, private, public, and multi-cloud scenarios.

7.2.2 - Threat Alerting Pt2
Develop analytics to detect deviations

How Gigamon Helps
Many network threats use standard applications and protocols that could be misconfigured, which Gigamon can detect with its Layer 2–7 visibility for on-prem, private, public, and multi-cloud (port spoofing, vulnerable protocols). Network detection and response is an essential element of threat alerting, for defense-in-depth. Log-based threat alerting is necessary but not sufficient, and in particular EDR agents can be bypassed, and logging can be disabled or even manipulated. Endpoint agents do not cover IoT or rogue compute. Network-based intelligence

is “true” in that it is taken off the wire from actual communications, i.e., observability with network depth.

7.2.3 - Threat Alerting Pt3
Identify Triggering Anomalous Events; Implement Triggering Policy

How Gigamon Helps
Many network threats use standard applications and protocols that could be misconfigured which Gigamon can detect with its Layer 2–7 visibility for on prem, private, public, and multi-cloud (port spoofing, vulnerable protocols). Network detection and response is an essential element of threat alerting, for defense-in-depth. Log-based threat alerting is necessary but not sufficient, and in particular EDR agents can be bypassed, and logging can be disabled or even manipulated. Endpoint agents do not cover IoT or rogue compute. Network-based intelligence is “true” in that it is taken off the wire from actual communications, i.e., observability with network depth.

7.2.4 - Asset ID and Alert Correlation
Rules developed for asset ID based responses

How Gigamon Helps
The ability to see devices come online by seeing their MAC address and DHCP requests/options offers unparallel visibility and discovery into known and unknown compute/IoT. This can help identify known and unknown assets. Being able to identify assets is foundational to any kind of correlation. Network-based intelligence is “true” in that it is taken off the wire from actual communications, i.e., observability with network depth.

7.2.5 - User/Device Baselines
Identify user and device baselines

How Gigamon Helps
Gigamon has external observability into device behavior regardless of its internal state. This can be used to establish device base lines which can then be correlated to known user information. Gigamon can provide continuous reporting and visibility into network level traffic East-West of apps and protocols to help establish and report on behavior deltas.

7.3 – COMMON SECURITY AND RISK ANALYTICS

Description
Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) employ data tools across their enterprises for multiple data types to unify data collection and examine events, activities, and behaviors.

Outcome
CNDSPs/SOCs employ big data tools across their enterprises for multiple data types to unify data collection and examine events, activities, and behaviors

7.3.1 - Implement Analytics Tools
Develop requirements for analytic environment; Procure and implement analytic tools

How Gigamon Helps
Gigamon can provide network logging in a standard format that is M-21-31 compliant across different administrative/technical domains/hybrid cloud and provide visibility to what analytic tools need to see.

7.3.2 - Establish User Baseline Behavior
Identify users for baseline; Establish ML-based baselines

How Gigamon Helps
AI and ML are only as good as what you feed them. You can’t baseline what you can’t see. Gigamon can provide continuous reporting and visibility into network-level traffic East-West of apps and protocols to help establish and report on behavior deltas. Additional Gigamon can observe any anomalous traffic, apps, protocols, configurations laterally or in multicloud environments.

7.4 – USER AND ENTITY BEHAVIOR ANALYTICS

Description
DoD organizations initially employ analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors and detect anomalies. Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) mature this capability through the employment of advanced analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors and detect anomalies.

Outcome
DoD organizations initially employ analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors and detect anomalies. CNDSPs/SOCs mature this capability through the employment of advanced analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors, and detect anomalies

7.4.1 - Baseline and Profiling Pt1Develop analytics to detect changing threat conditions; Identify user and device threat profiles

How Gigamon Helps
You can't baseline what you can't see. Gigamon can observe Layers 2–7 and makes network logs application aware. This visibility can detect MAC addresses, DHCP options, and Layer 2 traffic that often is not seen by classic methods. Additional Gigamon can observe any anomalous traffic, apps, protocols, and configurations laterally or in multi-cloud environments. This visibility is needed to help establish and report on behavior deltas.

7.4.2 - Baseline and Profiling Pt2
Add threat profiles for IoT and OT devices; Develop and extend analytics; Extend threat profiles to individual users and devices

How Gigamon Helps
Gigamon can observe Layers 2–7 and makes network logs application aware. This visibility can detect MAC addresses, DHCP options, and Layer 2 traffic that often is not seen by classic methods. This Layer 2 visibility and lateral visibility is critically important to see IoT traffic. Additional Gigamon can observe any anomalous traffic, apps, protocols, and configurations laterally or in multi-cloud environments.

7.4.3 - UEBA Baseline Support Pt1
Implement ML-based Analytics to detect anomalies

How Gigamon Helps
AI and ML are only as good as what you feed them. Gigamon can observe Layers 2–7 and makes network logs application aware. This visibility can detect MAC addresses, DHCP options, and Layer 2 traffic that often is not seen by classic methods. Additional Gigamon can observe any anomalous traffic, apps, protocols, and configurations laterally or in multi-cloud environments.

7.4.4 - UEBA Baseline Support Pt2
Implement ML-based Analytics to detect anomalies

How Gigamon Helps
AI and ML are only as good as what you feed them. Gigamon can observe Layers 2–7 and makes network logs application aware. This visibility can detect MAC addresses, DHCP options, and Layer 2 traffic that often is not seen by classic methods. Additional Gigamon can observe any anomalous traffic, apps, protocols, configurations laterally or in multi-cloud environments.

Gigamon®

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

10.24_01