Accelerating Secure Innovation at Defense and Intelligence Agencies

How Deep Observability Enables Agility, Reliability, and Zero Trust Capabilities

Executive Overview

Harnessing Deep Observability for Agility, Reliability, and Security

The U.S. Department of Defense (DoD) and intelligence community (IC) agencies face numerous pressures to deliver technology solutions that provide agile, reliable, and secure support for today's warfighter.

As outlined in "Fulcrum: The Department of Defense Information Technology Advancement Strategy" (June 2024), technological innovation plays an increasingly significant role in warfighting and intelligence-gathering missions. Agencies must find effective ways to fully leverage the power and versatility of commercial information technology and evolve from a network-centric to a data-centric, Zero Trust (ZT) model to modernize and meet information network, compute, and security needs (Fulcrum, LOE 2, p.7).

Building on existing DoD cloud strategies, Fulcrum aims to enable exponential growth, scale resources, address cybersecurity challenges, empower artificial intelligence (AI) and machine learning (ML), and extend tactical support for warfighters.

The strategy includes three lines of effort (LOE) that, among other strategic objectives, focus on:

- Treating and securing data as a strategic product (LOE 1.2)
- Optimizing the DoD information network (LOE 2.1)
- Implementing Zero Trust across DoD networks and compute (LOE 2.2)

The Gigamon Deep Observability Pipeline enables agencies to achieve these and many other objectives. Gigamon has been a trusted partner of the DoD for over a decade, with a proven track record of innovating and delivering mission-critical capabilities. Our collaborations with DoD agencies have led to advancements such as accelerating Zero Trust implementations and developing tactical, backpack-compatible versions of our solutions to support warfighters on the modern battlefield.

Packet-Level Visibility is Foundational to These Frameworks

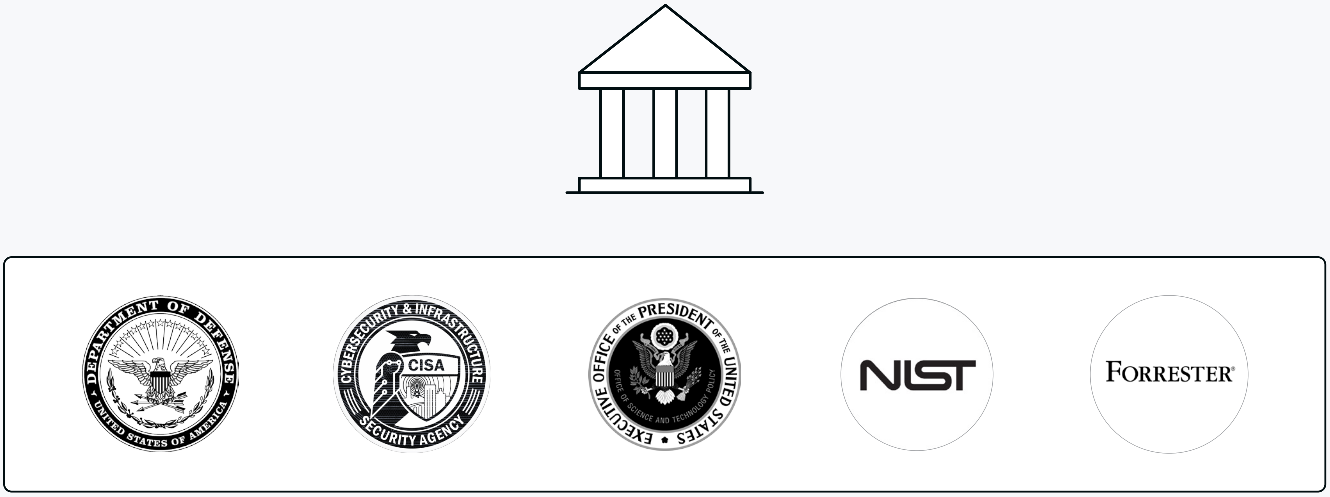

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
NIST
FORRESTER

Figure 1. Gigamon provides the packet-level visibility needed to meet compliance needs for a variety of Zero Trust frameworks.

© 2025 Gigamon. All rights reserved.

At a strategic level, the true value that Gigamon provides to the DoD and IC lies in the pervasive visibility of network transactions that Gigamon delivers to network, security, and operations teams and tools. This ensures powerful situational awareness even in the most dynamic tactical and strategic situations, as well as unprecedented visibility into the actions of adversaries targeting us and the posture and deployment of our own infrastructure.

Making Zero Trust Architecture a Reality

In the DoD Zero Trust Strategy released in 2022, the department established a minimum set of capability outcomes and activities necessary to secure the DoD information enterprise that the department and its components must achieve by 2027, which is referred to as Target Level ZT. Once this is achieved, the DoD will focus on achieving capability outcomes and activities supporting advanced ZT. The Gigamon Deep Observability Pipeline meets or enables 56 of the 152 capabilities and activities (37 percent), supporting all seven Zero Trust pillars (user, device, application and workload, data, network and environment, automation and orchestration, and visibility and analytics) described in the Zero Trust Strategy, as illustrated on the right.

How the Gigamon Deep Observability Pipeline Enables Zero Trust

The Gigamon Deep Observability Pipeline supports Zero Trust capabilities and activities in hybrid cloud network infrastructures by providing visibility into traffic within and between segmented environments, including:

- Physical networks from 10 Mbps to 400 Gbps
- Virtual networks like Broadcom/VMware, Nutanix, and OpenStack
- Public Cloud platforms, such as AWS, Azure, Google, and Oracle Cloud
- Containerized environments, including Kubernetes

U.S. Dept. of Defense Zero Trust Reference Architecture v2.0

- Considered the most mature Zero Trust model
- Gigamon addresses 56 activities

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

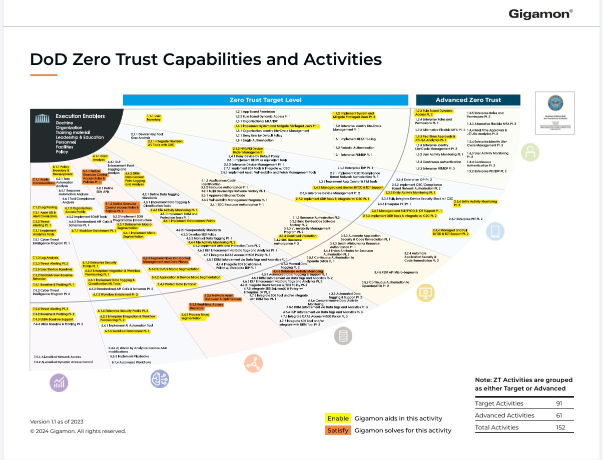


Figure 2. DoD Fan Chart with Gigamon Mapping. Available online.

- Cellular networks (5G, 4G/LTE), including private cellular networks
- Mobile, deployed, and tactical environments

Additionally, the Gigamon Deep Observability Pipeline offers visibility at every level of the Open Systems Interconnection (OSI) stack. It uses packet-level network telemetry to generate high-assurance network intelligence that provides detailed application-specific metadata from every network transaction. This telemetry enhances the efficiency and performance of security tools, validates and augments logs generated by network devices, ensures Zero Trust policy compliance, and trains AI or ML algorithms. Additionally, Gigamon has multiple solutions to deal with TLS, from full break and inspect to our innovative cloud-based Gigamon PrecryptionTM technology. Specifically, Gigamon enables the following DoD ZT Capabilities:

DoD ZT Capability 2.1

Continuous Hardware and Software Discovery

DoD ZT Capability 2.3

Enforce Endpoint Asset Compliance

DoD ZT Capability 2.7

Continuous Threat Detection and Response

DoD ZT Capability 5.1

Mature Segmentation to Lowest Level

DoD ZT Capability 5.2

Deploy SDPs as Close to Protected Resources as Possible

DoD ZT Capability 6.1

Policy Inventory and Development

DoD ZT Capability 7.1

Log Collection and Analysis

DoD ZT Capability 7.4

Identity and Entity Behavior Baselines

© 2025 Gigamon. All rights reserved.

Zero Trust in Hybrid and Multi-Cloud Environments

For Zero Trust deployments in hybrid or multi-cloud environments, Gigamon ensures consistent capture of network telemetry across cloud, on-premises, and virtual environments. This allows organizations to use existing security tools to quickly analyze and correlate threat activity in complex environments.

Because this telemetry is observed rather than generated by network devices, it provides a ground-truth view of network activity. If a transaction occurs, Gigamon will see it, record it, and provide context, offering higher assurance than device-generated logs, which are often targeted by adversaries.

In one of the original Zero Trust pilots sponsored by the Defense Information Systems Agency (DISA), United States Cyber Command (USCYBERCOM), and the National Security Agency (NSA), the Gigamon Deep Observability Pipeline was crucial. It provided visibility into red team activity within lateral (East-West) traffic between virtualized environments, which was quickly detected by the blue team once Gigamon was activated. This level of visibility and capability makes Gigamon essential for many Zero Trust projects.

M-21-31 and Beyond

For many federal agencies, meeting M-21-31 requirements remains a short-term priority and challenge. To accelerate M-21-31 compliance, Gigamon has produced a template and set of best practices that enable organizations to quickly meet M-21-31 logging requirements, which are necessary to support several Zero Trust capabilities necessary to achieve target and advanced ZT.

Event logging maturity model

- Collect, retain, and manage logs
- Centralized SOC access and visibility
- Three compliance levels

Common Challenges

- Encryption: Inconsistent or insufficient timestamping accross logging devices
- Virtual: Missing container visibility
- DNS: Burden on DNS sytems to perform their own logging
- Sequencing: Inconsistent or insufficient timestamping across logging devices
- Device: Network logs often don't report true MAC address

Level 1: Basic Logging

- ✓ Sequencing: common timestamp with PTP nanosecond resolution
- ✓ DNS: Passive DNS monitoring to offload DNS server reporting
- ✓ Device: True device identifier with reliable IP0to0MAC mapping
- ✓ Enables 72-hour full packet capture
- ✓ Provides the rquired network-derived syslog records to meet the level one data requirements
- ✓ Logs data for unmanaged devices through netwok-derived intelligence
- ✓ Forwards events for centralized storage

Level 2: Intermediate Logging

- ✓ Encryption: Gigamon provides decrypted or plaintext vixibility of encrypted traffic
- ✓ Decrypt once by policy: several modes available including inline, out-of-band, and PrecryptionTM

Level 3: Advanced Logging

- ✓ Virtual/Cloud: Gigamon provides East-West virtual visibility, even for containers
- ✓ Orchestrated solution to meet automation requirements

© 2025 Gigamon. All rights reserved.

Supporting Zero Trust with Comprehensive Decryption Capabilities

Encryption is a double-edged sword. While it protects data from adversaries, it also allows them to navigate networks undetected. Gigamon provides decryption solutions that work with existing security tools to selectively decrypt data, maintain privacy, optimize performance, and ensure compliance with Zero Trust security policies.

Gigamon supports a wide range of tactical approaches for TLS visibility, from full break and inspect to passive decryption to L3 decrypt to our ground-breaking Precryption technology, and we can combine them all into an interoperable and enterprise-scalable TLS visibility solution for TLS 1.3 down to SSLv3m, as well as passive TLS inspection for TLS 1.2 and below.

Gigamon can provide cloud and lateral traffic decryption using Gigamon Precryption technology, which eliminates blind spots within encrypted communications and eliminates the complexity and overhead of key-based decryption solutions. Precryption works by using eBPF functions to intercept application calls that would otherwise need to be encrypted, opening a secure tunnel between the source and target destinations and sending application data in clear text between these locations. The secure tunnel provides the same level of security as encryption with the complexity of key generation and management. The combination of Gigamon Decryption and Precryption solutions ensures effective and consistent decryption across even the most complex hybrid infrastructure for all forms of TLS without key management and enables a robust Zero Trust architecture (ZTA).

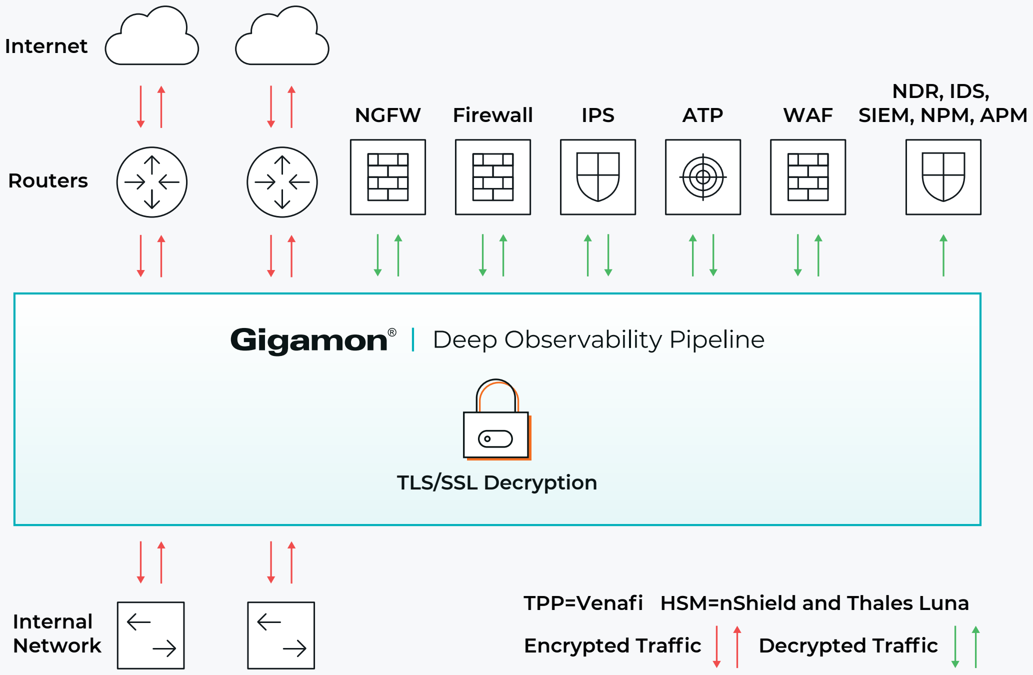


Figure 3. Gigamon centralizes and simplifies the handling of encrypted traffic including key management.

© 2025 Gigamon. All rights reserved.

Gigamon Precryption: Keyless Decryption for the Cloud and Lateral Traffic

Capability	Native Mirror + Out-of-Band Decryption	Inline Proxy Decryption	GigaVUE Cloud Suite™ with Precryption™
Plaintext visibility into TLS 1.2 encrypted traffic (non-PFS)	✓	✓	✓
Plaintext visibility into TLS 1.3 encrypted traffic (PFS)		✓	✓
Plaintext visibility without CPU impact from decryption			✓
No agents inside container workloads	✓	✓	✓
No complicated or special routing	✓		✓
No blind spots on lateral (East-West) cloud traffic			✓
No special key management libraries across all ciphers			✓
No hassle of constant key library updates			✓
No impact from cipher type, strength, and version			✓
Extension of Zero Trust architecture into the cloud			✓

Enhancing Logging and Security with Metadata

Gigamon Application Metadata Intelligence enhances the logging capabilities of existing security tools with network-derived intelligence delivered to these tools through highly efficient, context-rich metadata. Combined with the complete packet-level visibility Gigamon provides into all North-South and lateral East-West traffic, this metadata-level visibility provides a solid Zero Trust foundation by:

- Enhancing logging-based security tools (for example, SIEMs) with packet and metadata-level insights for faster, more precise threat detection and reduced MTTR
- Filtering and routing all network traffic to existing security tools, extending your security posture and maximizing the efficiency of these tools 3–5x
- Leveraging application metadata to gain context and insights to detect and respond to application-level threats
- Gaining more situational awareness with GigaVUE® Enriched Metadata for faster troubleshooting, threat detection, and incident response

> We ran a test and realized we couldn’t see certain events because we’re weren’t inspecting the packets going across the wire. At some point, phone calls were made, and we brought Gigamon on.

CHIEF ARCHITECT FOR ZERO TRUST
US Department of Defense

© 2025 Gigamon. All rights reserved.

Optimizing Observability and Security for Hybrid Cloud Deployments

The DoD is expanding its use of commercial enterprise software in hybrid cloud infrastructures. Gigamon helps defense and intelligence agencies realize cloud computing benefits while mitigating availability, performance, and security risks. The Gigamon Deep Observability Pipeline provides a unified view of activity across traditional data centers, private clouds, and multi-provider public cloud deployments, including visibility into service mesh architectures on Kubernetes-orchestrated containers.

Initially adopted by many DoD agencies as a network packet broker, Gigamon has evolved to support network traffic acquisition, aggregation, transformation, and enrichment across virtualized, private, and public cloud environments. Gigamon seamlessly integrates with existing tools and enhances their ability to detect, analyze, and respond to threats in real time, helping defense and intelligence agencies accelerate and reduce the cost of ZTA adoption.

The federal government's 2021 budget requeset focuses on IT modernization to improve mission delivery, productivity, and security using the following strategies:

- Cloud computing and shared services adoption
- Recruiting, retention and reskilling the workforce for IT and cybersecurity
- Reducing the federal cybersecurity risk
- Continued use of the Technology Modernization Fund

Gigamon Reduces Tools Traffic By Up To 78%

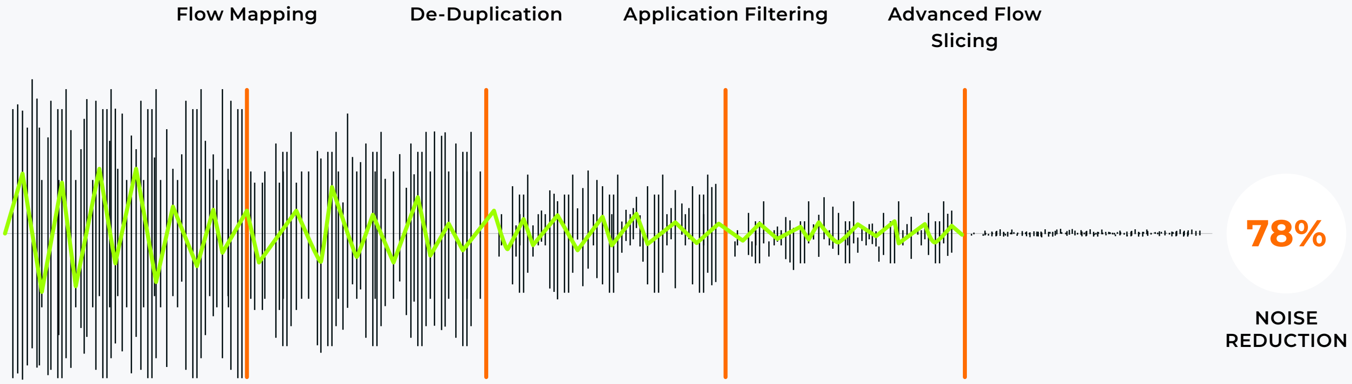


Figure 4. Advanced Gigamon functions such as Flow Mapping and De-Duplication optimize tools efficiency by eliminating irrelevant or duplicate traffic.

© 2025 Gigamon. All rights reserved.

Supporting the Need for Tactical Innovation

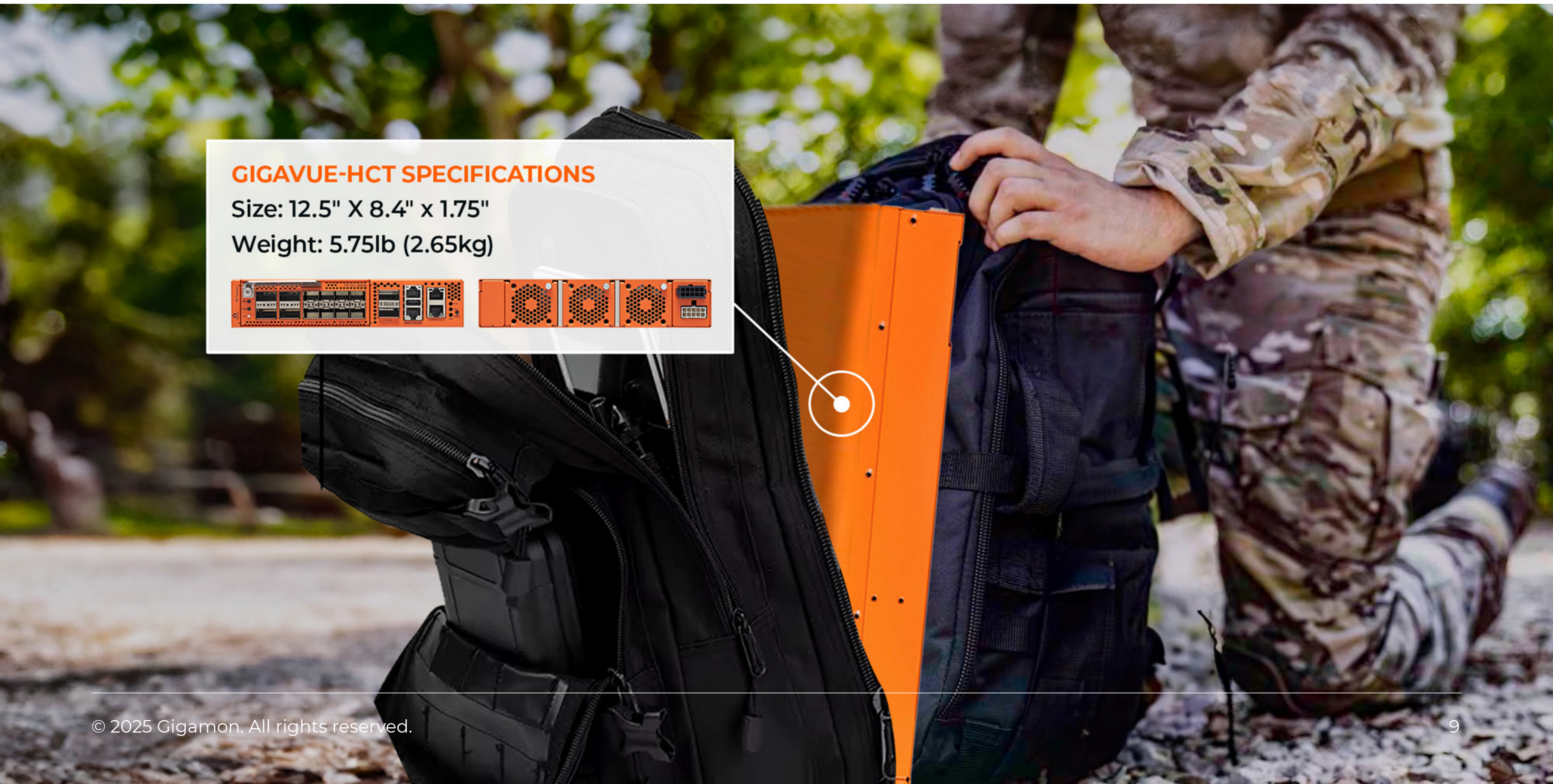
As all branches of the armed forces plan for operations in diverse tactical theaters, a key consideration is connectivity in contested, low-bandwidth, and disconnected, intermittent, and limited (DDIL) environments. To support warfighters in these conditions, Gigamon offers a range of deployment options for our software, suitable for data centers, public clouds, or individual warfighters. For instance, the GigaVUE HC-T device supports the full feature set of our widely deployed HC-Series appliances while meeting the connectivity needs of mobile, edge, and tactical units in a 5-pound SWaP form factor that fits in a backpack

Cost Efficiency in the Public Cloud

As DoD and IC organizations move workloads to the public cloud, Gigamon can reduce the cost of acquiring cloud traffic by up to 80 percent. This is achieved by eliminating the need for services like gateways and load balancers previously required by cloud service providers. This not only saves significant ongoing costs but also simplifies cloud infrastructure management, easing the burden on scarce cloud specialists.

Optimizing NDR Performance

Network detection and response (NDR) tools provide essential functionality that bridges potential gaps in hybrid cloud visibility. Gigamon extends this capability to provide total situational awareness, significantly increasing NDR detection rates by eliminating blind spots caused by encrypted, lateral (East-West), container, and operational technologies and (OT) Internet of Things (IoT) traffic. In addition, network intelligence generated by Gigamon reduces the amount of redundant or unnecessary traffic sent to NDR tools while maintaining fidelity, reducing data movement costs, and, most importantly, providing more precise, context-rich data to optimize mean time to detect and respond.



GIGAVUE-HCT SPECIFICATIONS
Size: 12.5" X 8.4" x 1.75"
Weight: 5.75lb (2.65kg)

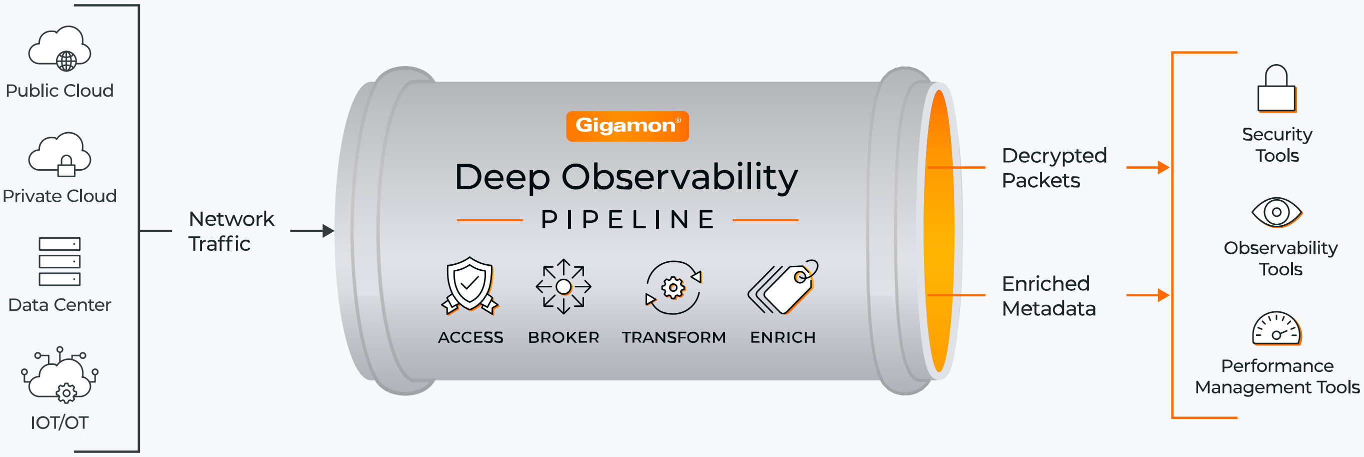


Figure 5. The Gigamon Deep Observability Pipeline powers security and network tools with both network packets and enriched metadata

Looking ahead, the importance of empowering NDR and other security tools with network intelligence derived from monitoring hybrid cloud network activity cannot be exaggerated. For example, according to the 2024 Gartner NDR Market Guide, the number of cloud security incidents discovered by NDR tools will increase five-fold by 2028.

Innovation with Operational and Tactical Technology

The DoD has long been a leader in deploying industrial control systems (ICS), OT, and IoT devices. However, this leadership has introduced challenges, as many of these are based on older hardware that cannot support local agents, making them vulnerable to cyber adversaries, with potentially catastrophic consequences.

The Gigamon Deep Observability Pipeline integrates with OT, ICS, supervisory control and data acquisition (SCADA), and IoT monitoring and security tools to provide comprehensive visibility across all assets, whether remote or local, in physical, hybrid, or cloud environments. Gigamon efficiently manages and delivers network traffic to tools in the required formats and proprietary protocols. It aggregates low-volume links, de-duplicates packets to reduce overhead, and controls asymmetric routing to ensure session information remains intact for security analysis.

Additionally, the Gigamon Deep Observability Pipeline offers load balancing, header stripping, and masking for security and compliance. It can be integrated into systems without introducing new mission risks by mirroring traffic through a one-way connection, capturing traffic details from ICS, OT, and IoT systems without using agents that could disrupt or compete for resources with mission-critical control systems.

© 2025 Gigamon. All rights reserved.

Accomplishing More at a Lower Cost

DoD and IC agencies face the dual challenge of delivering technology solutions that provide functional, rapid, and secure support for today's warfighter while maintaining critical existing systems on increasingly tight budgets.

Agency IT and security teams must work more efficiently and maximize the value of existing tool investments. Gigamon can be an invaluable ally in this effort. The Gigamon Network Efficiency Assessment and team can show you how Gigamon can typically reduce traffic to tools by over 50 percent, meaning agencies may need fewer tool instances to manage growing data and threat volumes. Savings from eliminating or deferring new tool purchases can be redirected to support new projects that advance the agency's mission.

The traffic management techniques provided by the Gigamon Deep Observability Pipeline, such as De-duplication, Advanced Flow Slicing, and Application Filtering Intelligence, can reduce "noise" or traffic to tools by 50–80 percent. This optimization enhances tool efficiency and potentially reduces the number of tool instances required. For organizations considering tool consolidation or rationalization, Gigamon offers proven and practical solutions to achieve these goals.

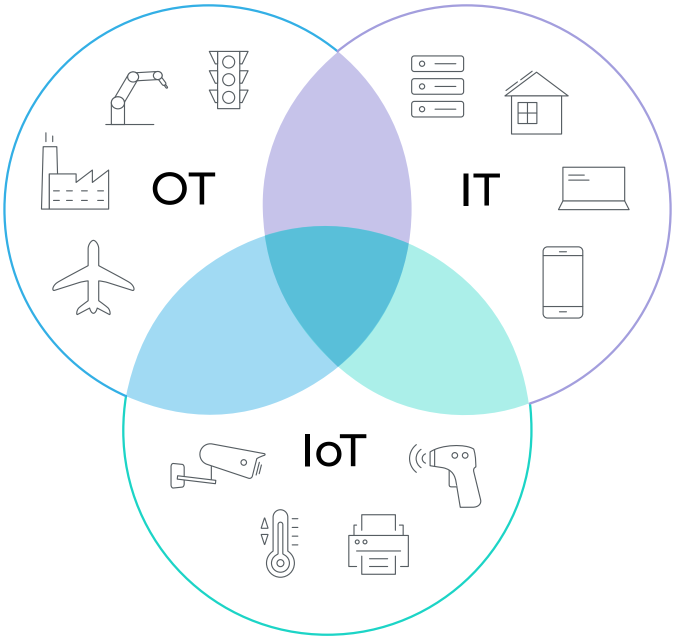


Figure 6.
Gigamon enables OT and IoT device traffic to be managed using existing security tools and best-practices.

© 2025 Gigamon. All rights reserved.

> The scope, complexity, and urgency of the foreign intelligence threats facing the United States necessitates that we engage partners and audiences across the whole of society to share information, identify and mitigate vulnerabilities, strengthen our defenses and build resilience, and work together to combat these threats and overcome challenges to protect our people, institutions, and strategic advantages.

NATIONAL COUNTERINTELLIGENCE STRATEGY
August 2024

Meeting the Challenges of Today and Tomorrow

For over a decade, Gigamon has partnered with DoD and IC agencies to face these intelligence and military threats by providing solutions that manage and secure the hybrid cloud networks essential to their mission's success. A key part of our commitment to working with these agencies is achieving and maintaining federal certifications, including Common Criteria, DoDIN APL, FIPS, USGv6r1, the M-22-18 Secure Supply Chain and Secure Software Development Practices mandate, and upcoming CMMC requirements.

The Gigamon Deep Observability Pipeline provides pervasive visibility of all hybrid network transactions that ensures powerful situational awareness even in the most dynamic tactical and strategic situations, as well as unprecedented visibility into the actions of adversaries targeting us and the posture and deployment of our own infrastructure. This enables the U.S. Department of Defense and intelligence community agencies to deliver technology solutions that provide agile, reliable, and secure support for today's intelligence communities and warfighters.

10/10

TOP U.S. FEDERAL AGENCIES
have deployed Gigamon solutions

FROST & SULLIVAN
#1 Market Share Leader
DEEP OBSERVABILITY
2024

61%

MARKET SHARE
for Deep Observability in 2024

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived telemetry 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.

Gigamon®

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

© 2025 Gigamon. All rights reserved. Gigamon and Gigamon logos are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.