# Maximizing the Benefits of CDM DEFEND for Your Agency with Gigamon

## Optimize Solution Performance to Lower CAPEX & OPEX


Achieve 50% reductions in cyber monitoring costs with an ROI exceeding 150%.[1]

### Key Benefits

- Traffic visibility across public (AWS, Azure, OpenStack), private and hybrid cloud deployments
- Decryption of SSL/TLS-encrypted Application Data-in-Transit at the boundary and across the network interior.
- Cybersecurity tools optimized for effectiveness and cost with visibility into network traffic across all IT operations
- Application Intelligence for application discovery and classification, with generation of Application Metadata and Internet IP Metadata including NetFlow

[1]The Total Economic Impact™ of Gigamon, a commissioned study conducted by Forrester Consulting on behalf of Gigamon, April 2016

CDM DEFEND provides Federal Agencies with a unique opportunity to partner with DHS and industry-best vendors to economically and continuously improve cybersecurity.

**Gigamon adds an essential element to CDM DEFEND solution deployments, enabling a rationalized approach to cybersecurity solutions deployments that can generate reductions in monitoring costs of 50% with a 3-year return on investment exceeding 150%.** The Gigamon Security Delivery Platform optimizes CDM DEFEND solution coverage and performance, lowers solution CAPEX & OPEX and drives measurable improvements in key cybersecurity metrics.

## The Gigamon Security Delivery Platform for CDM DEFEND

The Gigamon Security Delivery Platform provides network and security teams with broad access to and control over “data-in-transit” across all IT operations. Gigamon can be configured to decrypt select network and boundary traffic, detect and identify applications, isolate specific application sessions and generate application metadata. The Gigamon architecture allows cyber tool deployments using both out-of-band and in-line bypass configurations, optimizing cyber tool coverage, effectiveness and ROI while maintaining network throughput. Gigamon enables measurable improvements in key visibility-dependent cybersecurity metrics.

## What Agencies Have Discovered When Deploying Gigamon for CDM DEFEND

1. **Phase 1 Solutions are Optimized:** When Gigamon is architected into the CDM DEFEND Phase 1 HWAM or Phase 1 Gap Fill deployment, the solutions are optimized for cost, coverage and effectiveness.
2. **Phase 3 and Phase 4 Solutions are Optimized:** The pervasive visibility established for Phase 1 creates a foundation for subsequent CDM DEFEND solution deployments, reducing the associated CAPEX and OPEX, and maximizing the effectiveness of Network Access Control (NAC), Cloud/Mobile Security, Boundary Security/Discovery, etc.
3. **The Network is Optimized to Support Cybersecurity and Ongoing Authorization:** By utilizing Gigamon to optimize the performance of CDM DEFEND Phase 1, Phase 3 and Phase 4 solutions, the Agency is cumulatively deploying elements of a Network Security Architecture (also called a Visibility Fabric) that will support the effective and efficient deployment of cyber tools in accordance with the Cyber Risk Management Framework.
4. **CDM DEFEND Benefits are Immediate:** This network security architecture is created without the need for a major upgrade or overhaul of existing network infrastructure. Your agency does not need to wait on an expensive and disruptive six-year network infrastructure upgrade cycle before optimizing the effectiveness of CDM solutions.

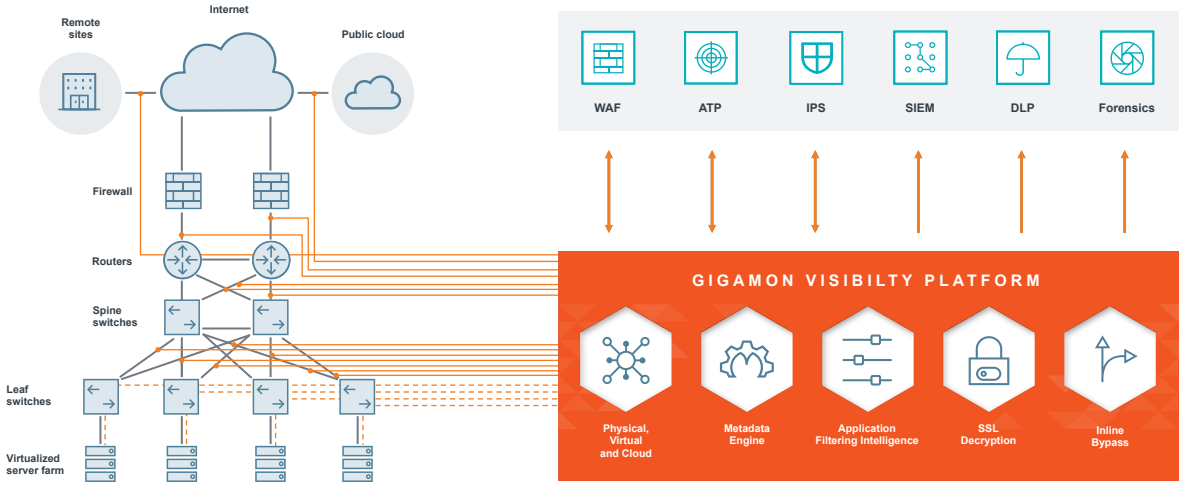


*Figure 1: The Gigamon Security Delivery Platform Establishes Network Traffic Visibility Across All IT Operations*

## Gigamon Security Delivery Platform and Group F

The Gigamon Security Delivery Platform is the Relay/Aggregator needed to supply the hosted continuous monitoring tools with desired monitoring data, tagged to provide for multi-tenant support.

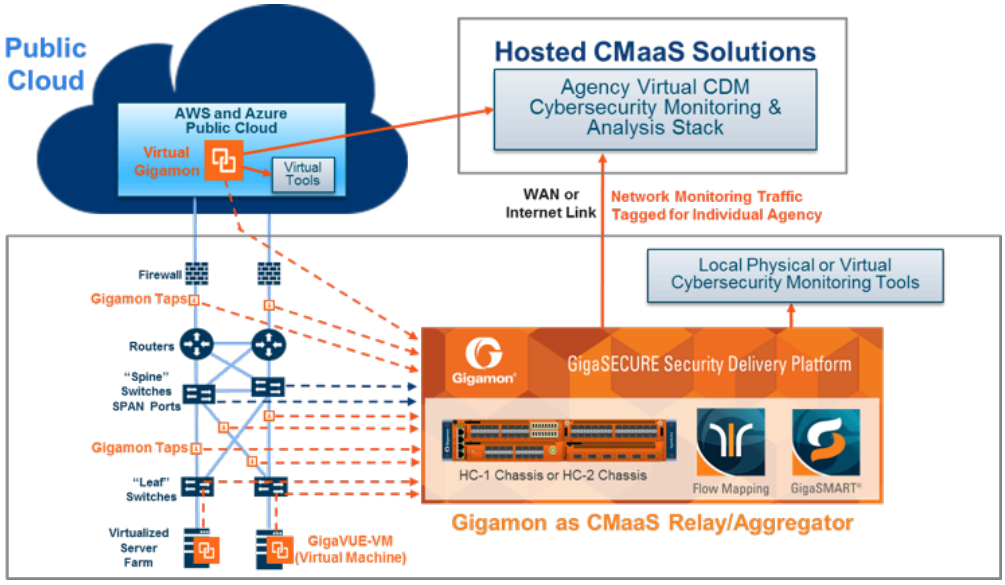


*Figure 2: Gigamon Security Delivery Platform*

## Gigamon Drives Measurable Improvement in Key Cybersecurity Metrics

The Gigamon Security Deliver Platform enables maximum event detection on the network, optimizing the ability of cyber tools to rapidly identify and correlate related events across all IT operations.

These capabilities drive immediate and measurable improvements to following key metrics:

- Mean Time To Detect (MTTD)
- Mean Time To Identify (MTTI)
- Mean Time To Respond (MTTR)

## Gigamon is an Approved Solution for Multiple CDM DEFEND Categories

The Gigamon Security Delivery Platform maps to 10 out of the 16 defined requirements for CDM DEFEND. Gigamon is on the CDM APL for the following solution deployments:

- Manage “What is on the Network?”
- Manage “How is the Network Protected?”
- Manage “What is Happening on the Network?”
- Manage “How is the Data Protected?” and Future Capabilities

## The Gigamon Investment Extends to Other Federal Cybersecurity Initiatives

Investment in the Gigamon Security Delivery Platform positions the Agency to meet the requirements of the following additional Federal Cybersecurity Initiatives and Programs:

- **Cybersecurity Framework Adoption from Executive Order 13800** – Optimization of the Agency cyber suite allows re-deployment of resources for High Value Asset protection.
- **Federal IT Modernization Implementation from Executive Order 13800**
  1. Gigamon decryption of data-in-transit enables monitoring at the application and data levels, while Gigamon NetFlow and Application Metadata augment “enhanced server logging” for more effective Event Detection & Correlation by the SIEM.
  2. Gigamon enables cloud migrations by optimizing TIC cybersecurity and throughput.
  3. Gigamon improves systemic Performance Monitoring to support deployment and oversight of Managed Services.
- **SOC Consolidation and SOCaaS from Executive Order 13800** – Gigamon provides multi-tenant collection of monitoring data from across multiple agencies.
- **.govCAR from Executive Order 13800** – Gigamon systemic visibility enables effective implementation of .govCAR for system-wide detection of threat actor actions.
- **DCOI** – Gigamon extends cybersecurity monitoring across virtualized environments.
- **FY 2019 CIO FISMA Metrics** – Gigamon enables improvements to multiple DETECT Metric Scores and to the RESPOND MTTD Metric Score. Gigamon Public Cloud solutions enable CIOs/CISOs to maintain FISMA scores as operations are migrated to the Cloud.


*Figure 3: Gigamon CDM DEFEND Investment Enables Agencies to Meet Additional Cyber Requirements*

## Leverage the Power of the Gigamon Ecosystem

GigaSECURE empowers the inline security tools – such as the Cisco FirePOWER Intrusion Prevention System (IPS), the FireEye Network Security Advanced Threat Prevention (ATP) solution and the Imperva SecureSphere Web Application Firewall (WAF) – to see, secure and prevent intrusions within growing network traffic and during software upgrades. By bringing threat traffic to the front of the line, offloading SSL decryption and boosting resiliency, Gigamon along with its ecosystem partners make your network more accurate and efficient.

### Gigamon Ecosystem Partners

Security and Vulnerability Management

algosec, AWAKE, bivio networks, BLUVECTOR, CENTRIPETAL NETWORKS, Check Point SOFTWARE TECHNOLOGIES LTD., CISCO, Cyber Test Systems, aws, CYPHORT, DAMBALLA, vmware, ExtraHop, Fidelis Cybersecurity, Flowmon, FLOWTRAQ, FORCEPOINT, ForeScout, FORTINET, FireEye, GuardiCore, IBM, iboss CYBERSECURITY, IMPERVA, LogRhythm The Security Intelligence Company, niara, NIKSUN, NexDefense, Lumeta, ManagedMethods, MICRO FOCUS, napatech, nectar, NETFORT know your network, paloalto, Phantom, pindrop security, PROTECTWISE Security Enlightened, REDSEAL, TREND MICRO, SENTINEL, SentryWire PACKET CAPTURE PLATFORM, SPIRENT, splunk>, StealthSecurity, tenable network security, RSA, Trustwave, VECTRA, VERSIVE, WHEEL, Microsoft

## For More Information

To find out how the Gigamon Security Delivery Platform can help you improve security and reduce costs, visit www.gigamon.com.



Gigamon®

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