Enabling Secure Innovation at Defense and Intelligence Agencies

How Deep Observability Accelerates IT Modernization and New Security Capabilities While Reducing Cost

Gigamon®

Contents

Overview

U.S. Department of Defense (DoD) and Intelligence Community (IC) agencies face a number of competing pressures. As technology innovation assumes a more significant role in both warfighting and intelligence gathering missions, agencies must find effective ways to migrate or evolve rapidly while maintaining legacy infrastructure and ensuring that security practices and capabilities keep pace. They must accomplish these objectives while facing unrelenting budget pressures and constraints.

The federal government's 2021 budget request 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[1]

With these challenges in mind, the DoD and IC are pursuing several strategic technology initiatives, including:

+ Enhancing security through the use of Zero Trust Architecture (ZTA) concepts
+ Expanding the use of more agile and scalable cloud infrastructure
+ Mitigating security risks with existing mission systems and operational technology (OT) networks
+ Finding innovative ways to apply and secure emerging 5G technology

Deep Observability Explained

Deep observability empowers IT to proactively mitigate security and compliance risk, deliver a superior user experience, and contain the cost and operational complexity of managing hybrid and multi-cloud IT infrastructures. It lets you harness actionable network-derived intelligence and insights to amplify the power of your cloud, security, and observability tools and processes you've already invested in.

Deep observability enables organizations to realize the full transformational promise of the cloud, and set the stage for delivering significant value.

Read more at gigamon.com

Making Zero Trust Architecture a Reality

As defense and intelligence agencies consider how to enhance the security of existing IT infrastructure and enable secure adoption of public cloud infrastructure, the urgency to adopt Zero Trust Architecture models is increasing. According to NIST Special Publication 800-207 "Zero Trust Architecture,"[2] Zero Trust security models "assume that an attacker is present in the environment and that an enterprise-owned environment is no different — or no more trustworthy — than any non-enterprise-owned environment."

A cybersecurity architecture based on ZTA principles moves your defensive perimeter from the edge of the network to assets within the network. Zero Trust continuously evaluates trust on a per-transaction basis to ensure the right people are accessing the right systems. This makes ZTA particularly well-suited for defense and intelligence applications as users become more geographically distributed and as public cloud usage grows. As a result, the National Security Agency (NSA), Defense Information Systems Agency (DISA), U.S. Cyber Command (USCYBERCOM) and DoD Office of the CTO are collaborating on a ZTA pilot program and deployment strategy.[3] These efforts will likely advance from pilot to implementation at scale across several military branches in 2021.

Success Story

GIGAMON PLAYS CENTRAL ROLE IN ZERO TRUST CLOUD PILOT

In 2019, the NSA, DISA and U.S. Cyber Command began a multi-phase Zero Trust reference architecture project. The top objectives of the project were to apply ZTA concepts to:

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

During the initial planning and design process at DreamPort, the 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 the inclusion of the Gigamon Deep Observability Pipeline in the team's first ZTA implementation at a pilot site in a DoD production 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.

A second project phase, which is now underway at DreamPort, will build on the DoD production deployment's success by extending the reference architecture to cloud platforms, which will support the next generation of DoD IT initiatives. Gigamon is playing a central role in this phase through its ability to support both physical and cloud networks with a unified deep observability pipeline.

See the associated success story for more.

To be effective, a ZTA deployment must continuously evaluate every user or device seeking access to network resources and data. This introduces significant complexity for network architects. Furthermore, it is critical for ZTA deployments to avoid introducing network latency that can disrupt mission-critical activities. Implementing ZTA at scale requires an integrated architecture that brings many disparate security technologies together.

The Gigamon Deep Observability Pipeline gives agencies adopting ZTA a single pane of glass to collect, process and forward data to the policy engine supporting their implementation, as depicted in Figure 1.

In essence, the deep observability provided by Gigamon acts as the glue that ties all ZTA functional components together. It enables agencies to access and collect all data in transit across physical, hybrid or cloud infrastructure, aggregate and process the data in real time (including the generation of flow data and Layer 5–7 metadata), and forward custom sets of data to the necessary components of the ZTA policy engine.

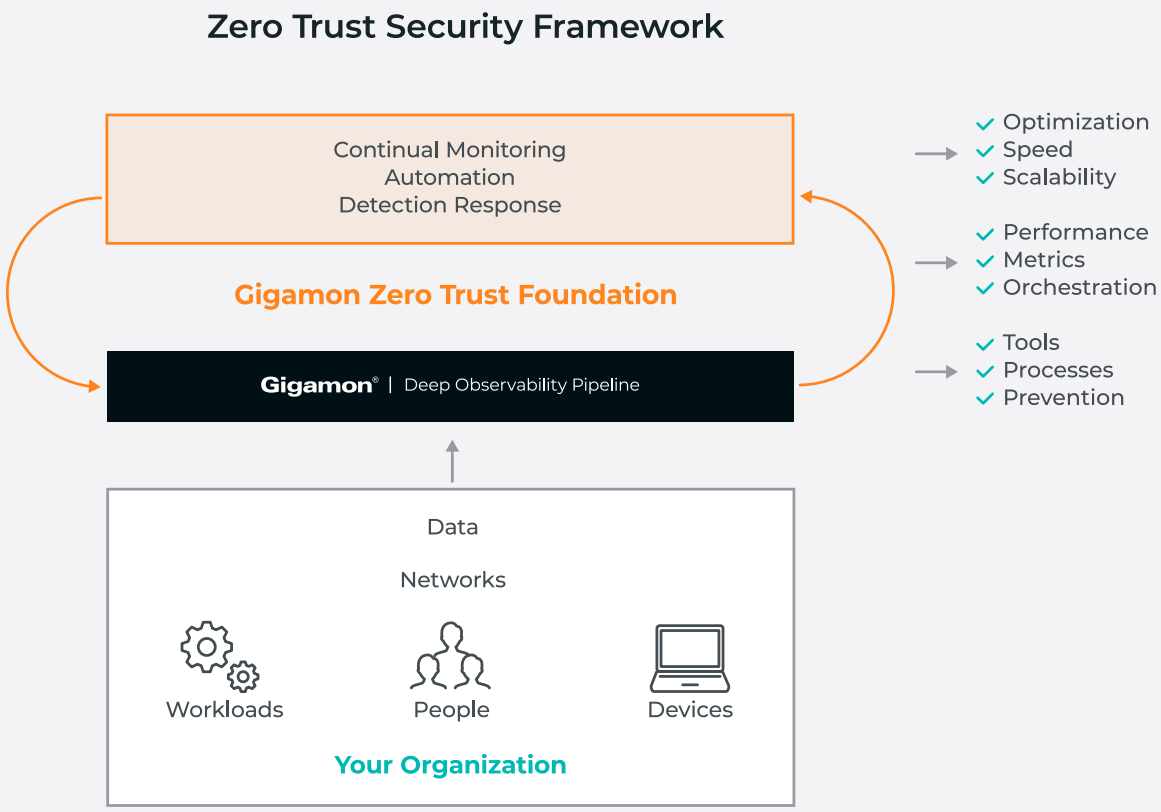

Figure 1. Gigamon Zero Trust foundation.

Success Story

GIGAMON HELPS GOVERNMENT ORGANIZATIONS ENHANCE SECURITY AND GAIN EFFICIENCY

After deploying the Gigamon Deep Observability Pipeline, a well-known government organization reported that it:

+ Accelerated threat prevention, detection and response time
+ Optimized tool utilization through the use of Flow Mapping
+ Reduced storage costs with better management of traffic volume
+ Enhanced staff efficiency by reducing manual tasks

Another government entity reported that Gigamon increased network-security visibility by 50 percent, significantly improving its ability to detect advanced persistent threat malware and malicious communications while decreasing the utilization load on security tools.

The Gigamon approach aligns with the ZTA guidance provided in NIST SP 800-207. For example, it helps achieve tenet 7, which recommends that an enterprise implementing a ZTA "collects as much information as possible about the current state of assets, network infrastructure and communications and use it to improve its security posture." Gigamon also satisfies one of the fundamental "Network Requirements to Support ZTA" as articulated at paragraph 3.4.1 (3) of SP 800-207:

The enterprise can observe all network traffic. The enterprise records packets seen on the data plane, even if it is not able to perform application layer inspection (i.e., OSI layer 7) on all packets. The enterprise filters out metadata about the connection (e.g., destination, time, device identity) to dynamically update policies and inform the PE [policy engine] as it evaluates access requests.

By implementing the Gigamon Deep Observability Pipeline as a centralized framework for collecting network traffic data from across all on-premises and cloud environments, optimizing it through techniques such as de-duplication and intelligently routing it to the tools that need it to enforce ZTA policies, defense and intelligence agencies can reduce the cost and complexity of ZTA adoption substantially.

Migrating to the Cloud — DoD and IC Considerations

> **"DoD appears to be firming up its commitment to commercial cloud, estimating $299M of its planned FY 2021 cloud budget will be spent with commercial providers."** [4]

Public cloud initiatives are gaining significant momentum across the defense and intelligence agencies. Increasing cloud adoption is being driven by several strategic objectives as outlined in the DoD's cloud strategy,[5] including:

+ Enabling exponential growth
+ Gaining the ability to scale resources up or down based on mission requirements
+ Proactively addressing cybersecurity challenges through modernization
+ Enabling new AI and machine learning (ML) applications
+ Extending capabilities and support for warfighters operating at the tactical edge
+ Enhancing IT infrastructure resiliency
+ Realizing IT efficiencies

The IC published its own cloud strategy[6] in 2019 that expresses a similar urgency for expanding the public cloud's use to improve intelligence gathering capabilities. However, given the sensitive nature of many defense and intelligence missions, the benefits of expanded cloud usage can only be achieved with appropriate security measures that match or exceed those in on-premises environments.

The DoD and IC both have active cloud deployments with major new phases on the near-term horizon. For example, DISA currently operates milCloud 2.0, a private cloud platform designed to streamline access to IT resources. The DoD is now taking additional steps toward the public cloud with its $727 million U.S. Air Force Cloud One contract and forthcoming $10 billion Joint Enterprise Defense Infrastructure (JEDI) contract.

The IC is even further along with its use of the cloud. It has been collaborating with Amazon Web Services (AWS) on a Commercial Cloud Services (C2S) platform with top-secret, secret and unclassified elements since 2013. It is now moving forward with a multi-cloud successor, Commercial Cloud Enterprise (C2E), which will incorporate cloud services from AWS, Microsoft, Oracle, IBM and Google.

As the DoD and IC infrastructure evolves into a heterogeneous blend of legacy on-premises infrastructure, private cloud infrastructure and multiple public cloud providers, it will be increasingly challenging to manage performance and security holistically. New approaches such as ZTA will help mitigate new risks presented by the public cloud if visibility across all on-premises and cloud infrastructure is provided. In addition, future security strategies must include protection models for physical servers connected to traditional networks, virtual machines running in private and public cloud environments, and emerging application deployment models such as containers and micro-services. This includes new visibility and security techniques for the infrastructure itself, as well as the DevSecOps skills and practices necessary to protect a fast-evolving IT infrastructure.

Gigamon helps defense and intelligence agencies realize the benefits of cloud computing while mitigating infrastructure availability, performance and security risks. The Gigamon Deep Observability Pipeline provides a unified view of activity across traditional data centers, private cloud environments and multi-provider public cloud deployments as shown in Figure 2. This approach aligns well with broader DoD and IC security requirements, including those outlined in the "DoD Cloud Computing Security Requirements Guide" (SRG).[7]

Gigamon provides visibility into traditional network traffic and enables the creation of sophisticated cloud sensor frameworks to monitor activity in the public cloud, as shown in Figure 3. This includes visibility into modern service mesh architectures running on Kubernetes-orchestrated containers.

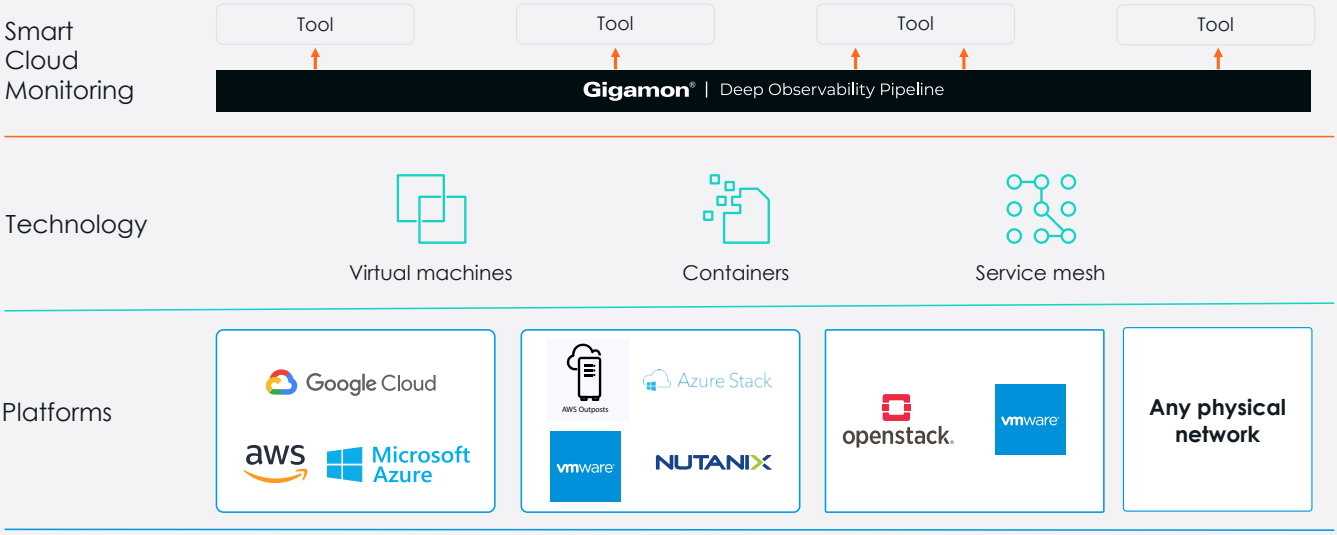

Figure 2. Gigamon technology and platform coverage.

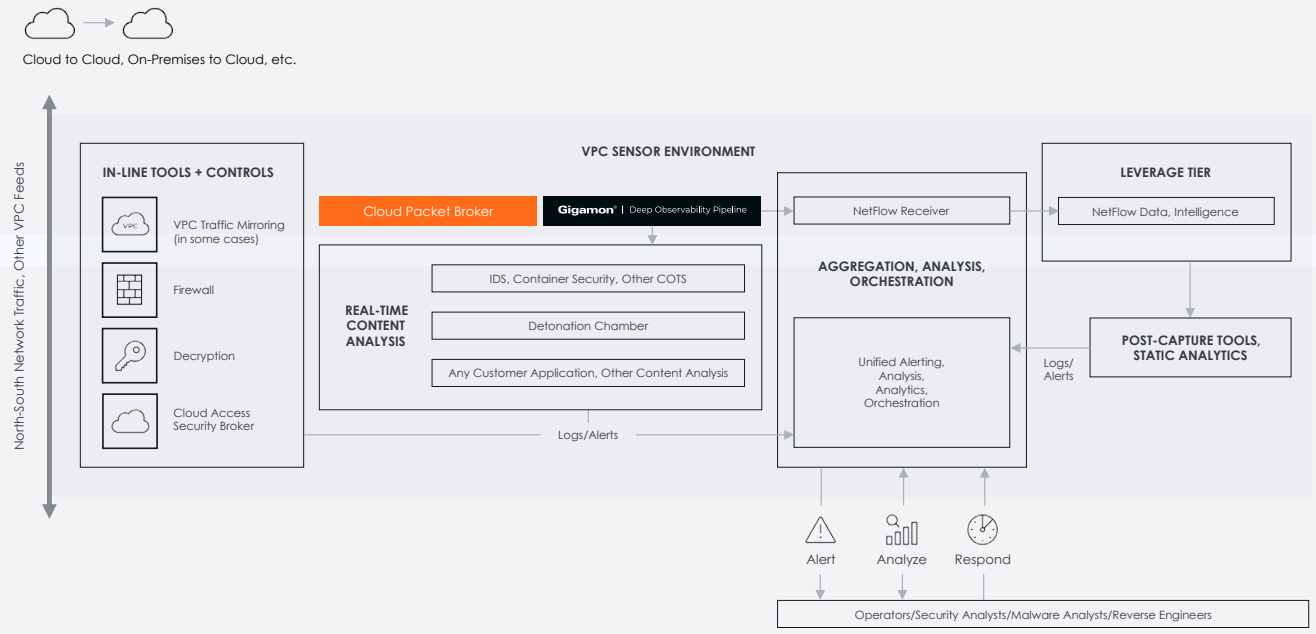

Figure 3. Gigamon private cloud sensor environment.

Dynamic application deployment models like containers bring tremendous flexibility, but because they change frequently, gaining and maintaining visibility is challenging. As agencies deploy these types of architectures, the Gigamon Deep Observability Pipeline can be extended into these environments through the use of specialized G-vTAP Containers. G-vTAP Containers are deployed within each worker node automatically and send traffic as required to Gigamon nodes running in the cloud or on-premises. This approach ensures that visibility adapts along with the containerized infrastructure and makes it possible to view service mesh activity alongside activity in more traditional cloud and data center infrastructure.

This model supports continuous integration/ continuous delivery (CI/CD) pipelines, where application development moves through different, siloed stages (dev, staging, QA, etc.) before finally being deployed into a production environment for customer usage. The Gigamon non-intrusive container visibility solution can reach into the different phases of the application development, as shown in Figure 4, to extract the right information for the tools to perform their inspection or to further extend the ZTA framework in real time as applications are being created.

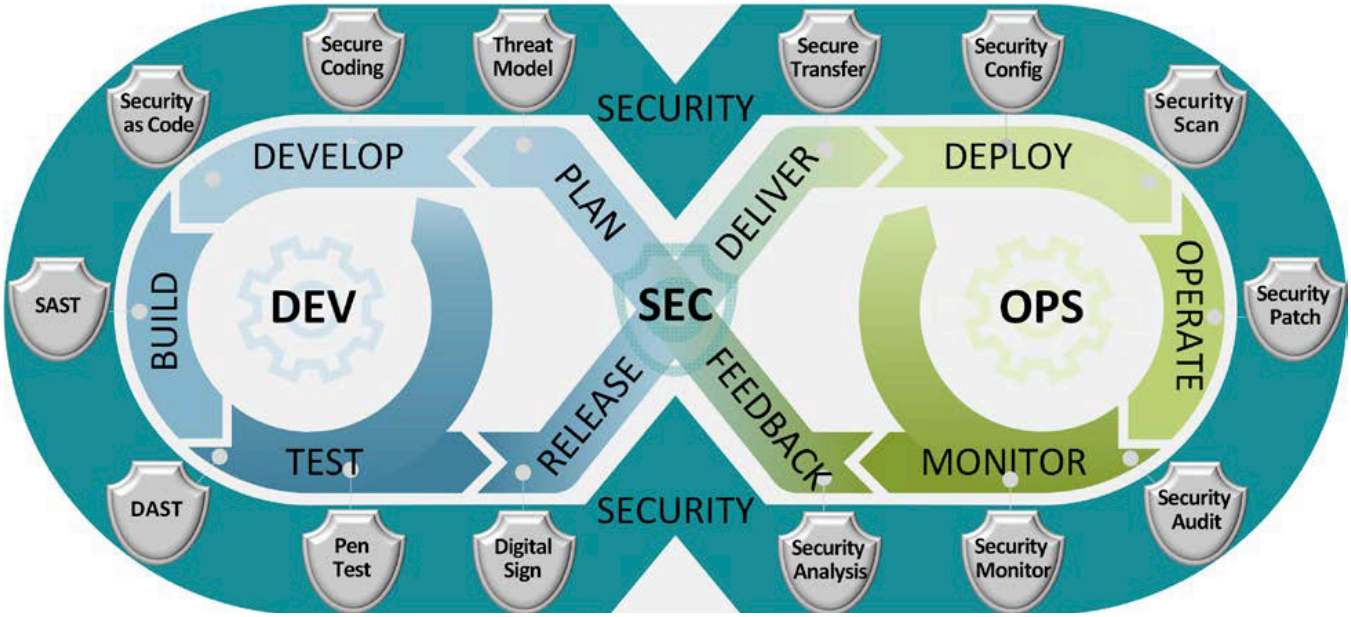

Figure 4. DevSecOps development cycle for DoD.[8]

Securing Operational Technology and Mission Systems

Even as the DoD and IC embrace new technologies such as 5G and the public cloud, they face the parallel challenge of modernizing existing systems that perform mission-critical functions. The computing resources, software and industrial control systems (ICS) and OT networks used to operate mission systems and other critical infrastructure are notable examples.

The hardware and software used to operate mission systems require active protection. This is only possible through visibility that spans across both modern and legacy networks. This is an ongoing challenge in all networks, including IT defense networks. This is especially true with ICS and OT networks, which are often comprised of aging distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems that weren't designed with the modern security threat landscape in mind. These systems were not originally intended to be connected to IT networks, so remote access security, visibility and threat analysis were not design priorities.

These technologies are central to the operation of many sensitive mission systems and their supporting infrastructure, including high-value targets such as utilities, dams, interconnected aircraft systems, navigational systems, power control systems, embedded ground systems, access controls systems, and hull, mechanical and electrical (HM&E) systems. As such, safety and availability, including 100 percent uptime requirements in many cases, are top priorities. With the convergence of OT controls with IT networks, there is greater exposure to cyberattacks. Attackers are targeting ICS and OT with greater frequency, and any security compromise could have catastrophic consequences. Therefore, incorporating these systems into a holistic security strategy that is capable of providing secure visibility into remote locations without on-site personnel is essential.

ICS and OT Security Are a Growing Priority

"By 2021, 25 percent of asset-centric enterprises will adopt a hybrid model to secure operational technology (OT) environments with traditional security deployed alongside specialist OT security technology, up from 10 percent in 2018."[9]

The Gigamon Deep Observability Pipeline integrates with OT, ICS or SCADA tools to offer comprehensive and integrated visibility across all remote and local assets in physical, hybrid or cloud deployments. Gigamon enables traffic from across the network to be managed and delivered to tools efficiently and in the format (including proprietary protocols) they need, aggregates low-volume links together before forwarding them, de-duplicates packets to avoid unnecessary overhead and offers easier control of asymmetric routing to ensure that session information is kept together for security tools to analyze.

The Gigamon Deep Observability Pipeline also provides load balancing, header stripping and masking for security and compliance. Gigamon can be integrated into these systems without introducing new mission risks by mirroring traffic through a one-way connection that passively captures network traffic details from active mission, ICS and OT systems for out-of-band analysis without intruding on sensitive communication activity and without using agents that could potentially disrupt or compete for resources of critical control systems. This provides tools with the required visibility to ensure Security Operations teams can protect the systems, software and networks relied upon by mission systems and OT.

Innovating with 5G Technologies Securely

The high-bandwidth and low-latency characteristics of 5G technologies offer tremendous potential across a wide range of defense and intelligence, tactical and enterprise activities, including logistics, training, warfighting and intelligence gathering missions. As a result, the DoD and IC have active initiatives to apply 5G technologies for purposes far beyond traditional voice and data communication. The strategic importance of 5G is also driving a proactive focus on security. The DoD 5G Strategy,[10] published in May 2020, establishes three key objectives:

+ Advance U.S. and partner 5G capabilities
+ Promote awareness of 5G risks to national security
+ Develop approaches to protect 5G infrastructure and technologies

Active research and testing projects are already underway in each of these areas. For example, in October 2020, the DoD awarded $600 million in contracts[11] to grow the number of military installations performing 5G testing and experimentation from 12 to 17. Each site will focus on specialized areas of 5G innovation, such as:

+ 5G-enabled smart warehouses
+ Military ship and aircraft connectivity and readiness
+ Connectivity for Forward Operating Bases (FoBs) and Tactical Operations Centers (ToCs)
+ Augmented reality (AR) support for maintenance and training
+ 5G core security
+ Strategies for wireless-spectrum sharing by DoD and commercial entities

In addition to 5G technology experimentation and testing, DoD agencies such as the Air Force and Army are collaborating on the use of 5G to modernize the Joint All-Domain Command and Control (JADC2), the DoD's warfighting network of networks.[12] The 5G networks of the future will extend well beyond mobile phones and PCs to include networked cavalries of Humvees, fleets of ships and squadrons of aircraft that are capable of delivering greater value at the tactical edge.

While 5G holds tremendous promise, it introduces new management and security challenges. As the number and types of connected devices multiplies, the size and complexity of the security attack surface that must be protected grows as well. Security threats that are of concern for 5G networks are shown in Figure 5. By default, the security tools used to detect threats and attacks on traditional networks will likely lack visibility into 5G networks. Even when visibility is possible, the large quantities of data generated by 5G networks, including significant amounts of duplicate data, may have adverse effects on security tool performance and effectiveness.

Gigamon helps defense and intelligence agencies overcome these challenges by establishing a deep observability pipeline that can be used to monitor and secure both traditional network infrastructure and 5G network deployments, as shown in Figure 6. This includes the ability to decrypt SSL/TLS-encrypted 5G user plane traffic, which is where malware often hides itself, in a centralized and controlled manner for more complete visibility into possible threats. Gigamon makes scaling 5G network security easier by giving security teams the ability to manage traffic flow to specific tools, including de-duplication, application detection and load sharing across multiple tool instances, while keeping individual user sessions together. As user plane traffic grows over time, the Gigamon Deep Observability Pipeline provides the ability to correlate the user plane traffic with the actual user, network or priority identifiers (contained in the 5G core network control plane communication), which allows isolated or targeted monitoring of specific user traffic and load balancing the traffic across multiple instances of each monitoring tool type.

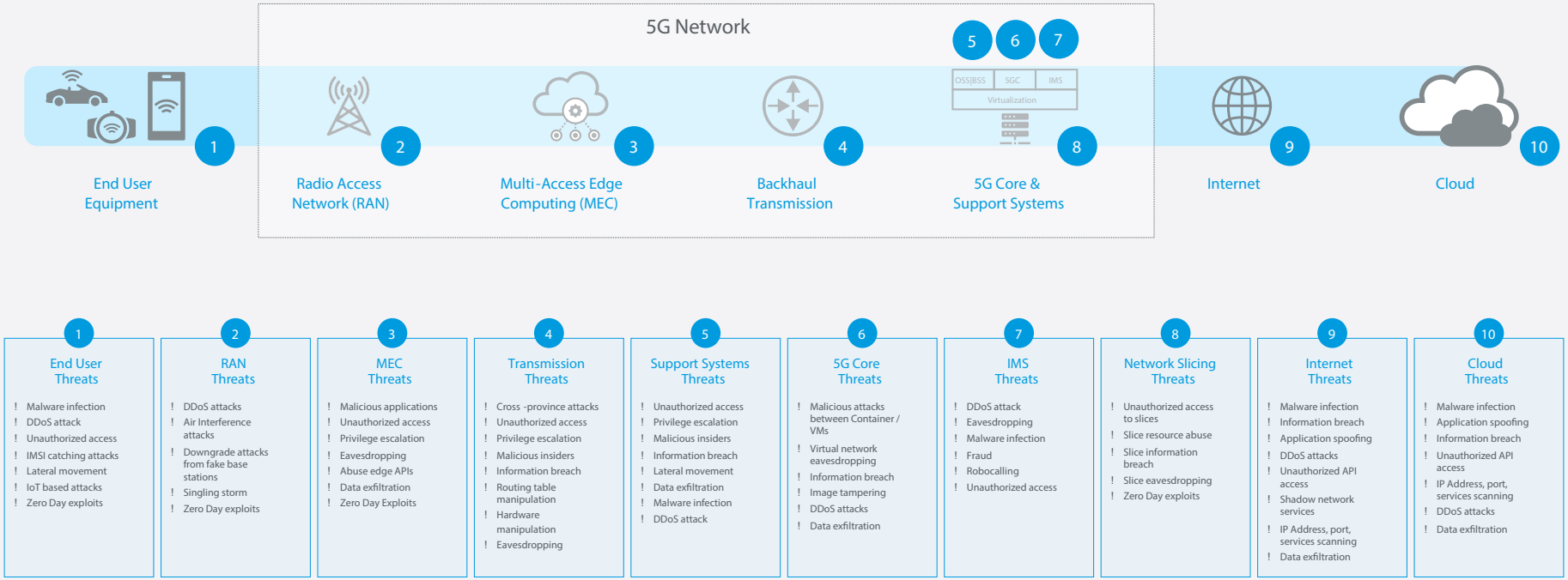

Figure 5. Security concerns for 5G networks.

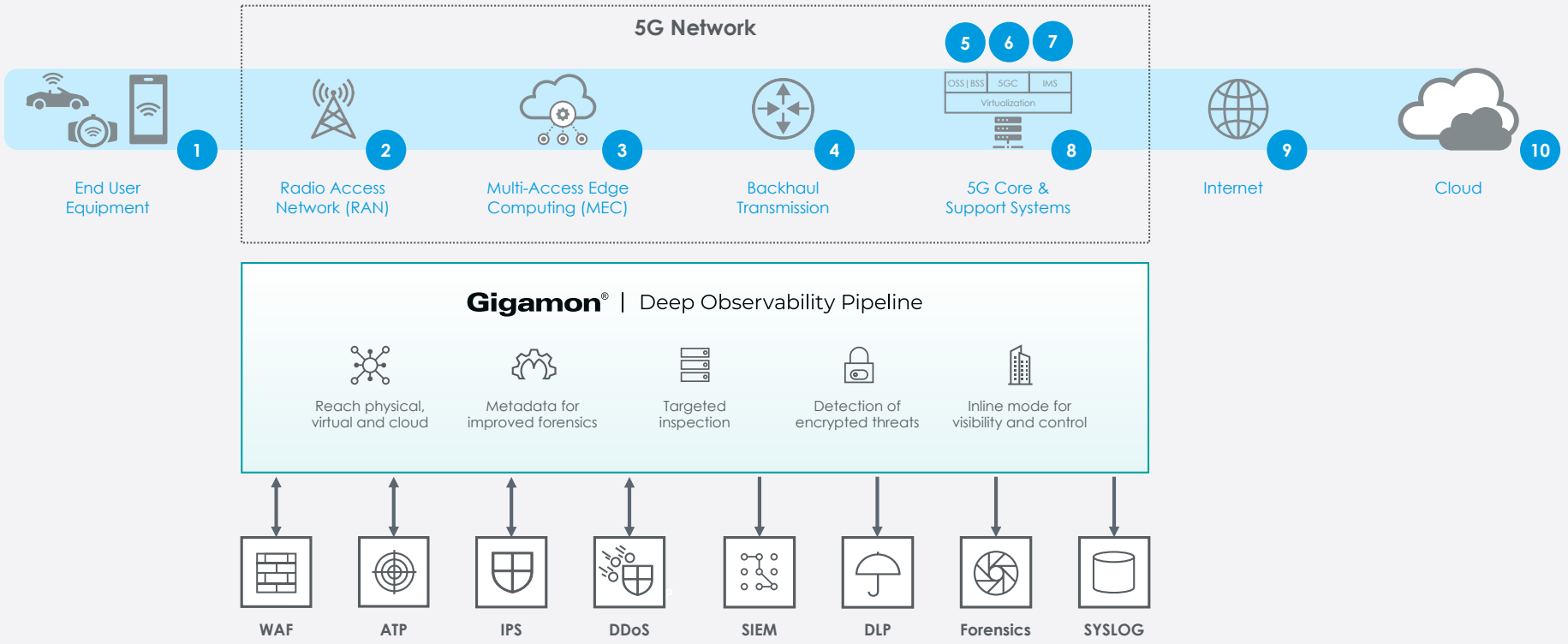

Figure 6. The Gigamon Deep Observability Pipeline to address 5G security concerns.

Accomplishing More at Lower Cost

As DoD and IC infrastructure evolves with the addition of public cloud platforms and new deployment models like containers, agencies gain much greater ability to innovate and scale IT resources dynamically based on mission requirements. While this brings potential operational costs savings and agility advantages, it places tremendous pressure on security teams to accomplish more with less.

Each new technology implemented represents a potential increase in the size of the overall security attack surface. Meanwhile, adversarial nation-states, cybercriminals, disgruntled employees or contractors can put unrelenting pressure on all aspects of the DoD and IC technology infrastructure.

Agency security teams often don't have the luxury of adding expensive incremental tools and specialized personnel as new technologies and threats emerge. They must find ways to work more efficiently and extract every possible bit of value from existing security tool investments.

By reducing the load on security tools by offloading resource-intensive operations such as SSL/TLS decryption and optimizing the flow of traffic data to monitoring tools, Gigamon helps security teams keep pace with the rapidly evolving threat landscape while reducing cost.

U.S. Government Agency Saves Over $1 Million with Gigamon

Faced with growing infrastructure utilization and rising tool vendors costs, a U.S. government agency was able to realize over $1 million in cost savings with Gigamon solutions by:

+ Maximizing network visibility and performance monitoring
+ Optimizing tool utilization by traffic filtering
+ Reducing storage costs
+ Lowering escalating costs with other vendors and tools

Our [costs have] been significantly reduced upon deploying Gigamon solutions. Thanks to Gigamon, considerably less time is now needed to develop new tools — or to augment current tools — in order to handle increasing data volume. Historically, in order to accommodate high data volumes, hundreds or thousands of hours were spent developing or changing current data processing software tools. The Gigamon appliances enabled us to spend resources on software feature enhancements versus baseline maintenance."

– MAGNIHIL DLEET, DoD IT ARCHITECT

Conclusion: Future-Proofing DoD and IC Infrastructure with Gigamon

As we've explored, the pervasive visibility enabled by Gigamon simplifies and accelerates many different types of strategic IT and security initiatives. This includes today's most pressing DoD and IC priorities, such as ZTA, cloud adoption, ICS/OT security and 5G. However, the essential value that Gigamon provides is flexibility in the face of change.

When today's key defense and intelligence initiatives are completed, a new wave of IT and security priorities will take their place. Similarly, today's budget pressures will certainly not be the last. Making Gigamon technology a key component of the IT infrastructure at DoD and IC agencies will ensure that these environments are scalable, adaptable and cost-effective as new technology requirements emerge. Accomplishing this does not require a complex and costly one-time project. It can start with focused applications of Gigamon modular architecture to address tactical, regional or mission-specific challenges. Over time, these efforts can be woven together into a broader deep observability pipeline that delivers strategic value across geographic and organizational boundaries.

RELATED RESOURCES

+ For civilian federal agencies: "Ensuring Continuity, Effectiveness and Security During Uncertain Times"
+ For government contractors: "Reduce the Cost and Complexity of CMMC Compliance"

A top 10 defense systems integrator confirmed the following results with Gigamon solutions:

+ Centralized traffic decryption (FIPS 140-2 Level 2 certified)
+ Maximized network visibility
+ Optimized tool utilization by traffic filtering
+ Lowered escalating tool cost
+ Enhanced staff efficiency by reducing manual tasks

GIGAMON CERTIFICATIONS AND AUTHORITY TO OPERATE (ATO)

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

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

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

CAGE: 4XKN9
DUNS: 362737251

Gigamon is trusted by 10 of the top 10 U.S. federal agencies, leading DoD contractors and vendors.

10 out of the top 10 U.S. federal agencies have deployed Gigamon solutions

153 percent ROI improvement of the security stack[13]

50 percent decrease in costs associated with security efforts[13]

58 percent market share in the government sector, nearly four times the nearest competitor[14]

40 percent market share for deep observability in 2022[15]

About Gigamon

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

Gigamon®

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

06.23_03

References

[1] "Federal Cloud Computing Market 2020–2022" (Report). GovWin by Deltek. August 27, 2020. https://iq.govwin.com/neo/marketAnalysis/view/Federal-Cloud-Computing-Market--2020-2022-/46722?researchTypeId=2&researchMarket=.

[2] Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly. "NIST Special Publication 800-207 Revision 5 – Zero Trust Architecture." National Institute of Standards and Technology. August 2020. https://doi.org/10.6028/NIST.SP.800-207.

[3] "Zero Trust Becoming Cyber Strategy of Choice Across Defense Department." MeriTalk. October 8, 2020. https://www.meritalk.com/articles/zero-trust-becoming-cyber-strategy-of-choice-across-defense-department.

[4] "Federal Cloud Computing Market 2020–2022" (Report). GovWin by Deltek. August 27, 2020.

[5] "DoD Cloud Strategy." U.S. Department of Defense. December 2018. https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF.

[6] "Strategic Plan to Advance Cloud Computing in the Intelligence Community." U.S. Intelligence Community. June 26, 2019. https://www.dni.gov/files/documents/CIO/Cloud_Computing_Strategy.pdf.

[7] "DoD Cloud Computing SRG." Department of Defense. March 6, 2017. https://dl.dod.cyber.mil/wp-content/uploads/cloud/pdf/Cloud_Computing_SRG_v1r3.pdf.

[8] "DoD Enterprise DevSecOps Reference Design V1.0." Department of Defense. August 12, 2019. https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf.

[9] "OT Security Best Practices" Gartner, September 2018

[10] "Department of Defense (DoD) 5G Strategy (Unclassified)." Department of Defense. May 2, 2020. https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf

[11] Scott Maucione. "DoD Puts Down Serious Money on 5G Experimentation." Federal News Network. October 13, 2020. https://federalnewsnetwork.com/dod-reporters-notebook-jared-serbu/2020/10/dod-puts-down-serious-money-on-5g-experimentation

[12] Jackson Barnett. "The Army Says It's Working with the Air Force on JADC2." FedScoop. October 7, 2020. https://www.fedscoop.com/army-jadc2-air-force-collaboration.

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

[14] Network Monitoring Equipment Annual Market Report: Omdia, June 2020.

[15] "Observability Quarterly Market & Long-Term Forecast Report." 650 Group, April 5, 2023. https://650group.com/reports/observability/