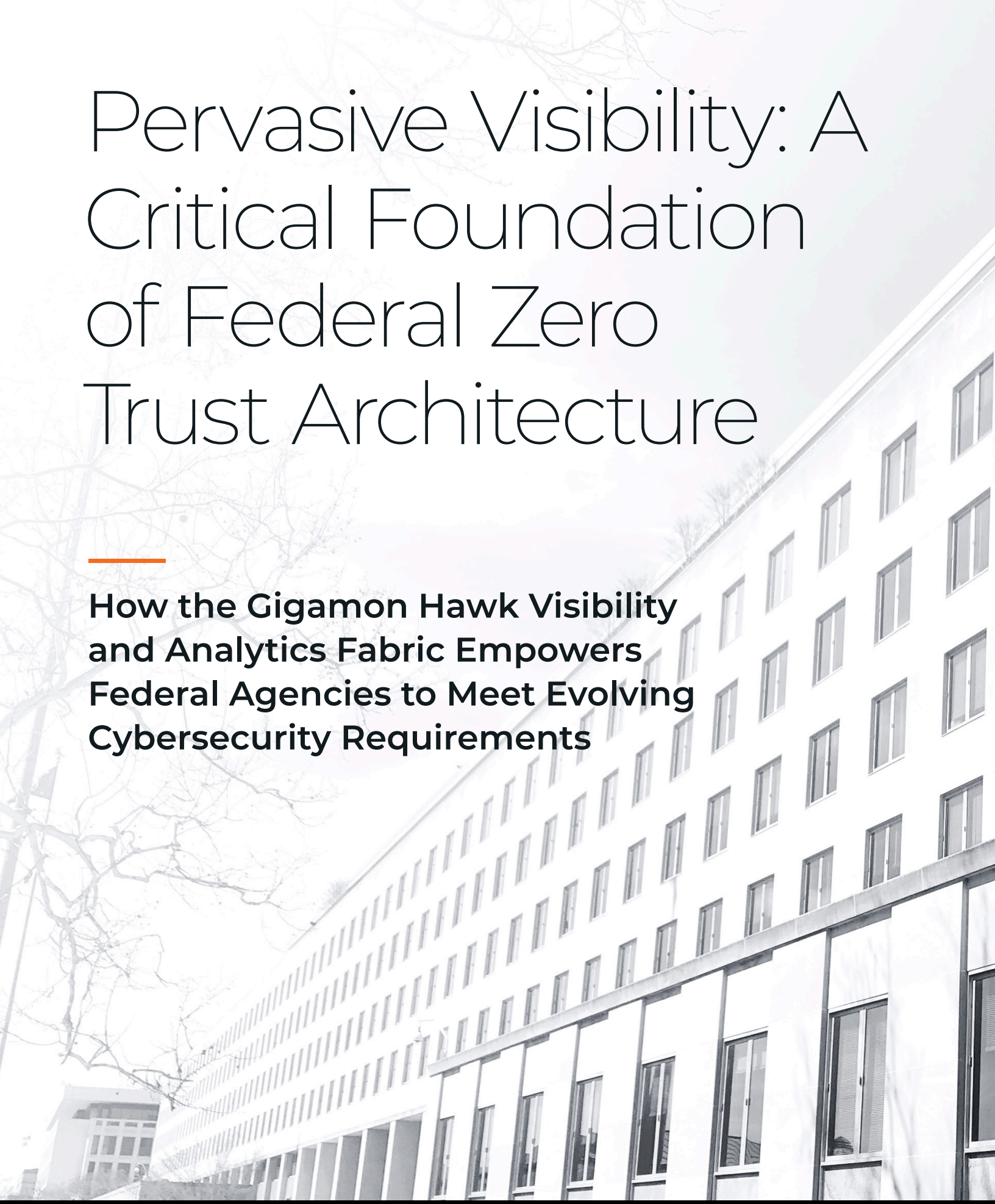
Pervasive Visibility: A Critical Foundation of Federal Zero Trust Architecture

How the Gigamon Hawk Visibility and Analytics Fabric Empowers Federal Agencies to Meet Evolving Cybersecurity Requirements



Gigamon®

SEC. 3. MODERNIZING FEDERAL GOVERNMENT CYBERSECURITY

The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

– WHITE HOUSE EXECUTIVE ORDER
MAY 12, 2021

Large-Scale Cybersecurity Incidents Are Driving an Urgent Federal Response

Rapid evolution and escalation of the security threat landscape, including the SolarWinds, Microsoft Exchange, and Colonial Pipeline security incidents, are driving an increased focus and investment in cybersecurity at the federal government level.

In May 2021, the White House issued an executive order calling for broad and bold improvements to the nation's cybersecurity infrastructure through partnership between the public and private sectors. One of the most ambitious requirements of the executive order calls for modernization of federal government cybersecurity through broader use of secure cloud services and adoption of Zero Trust Architecture.

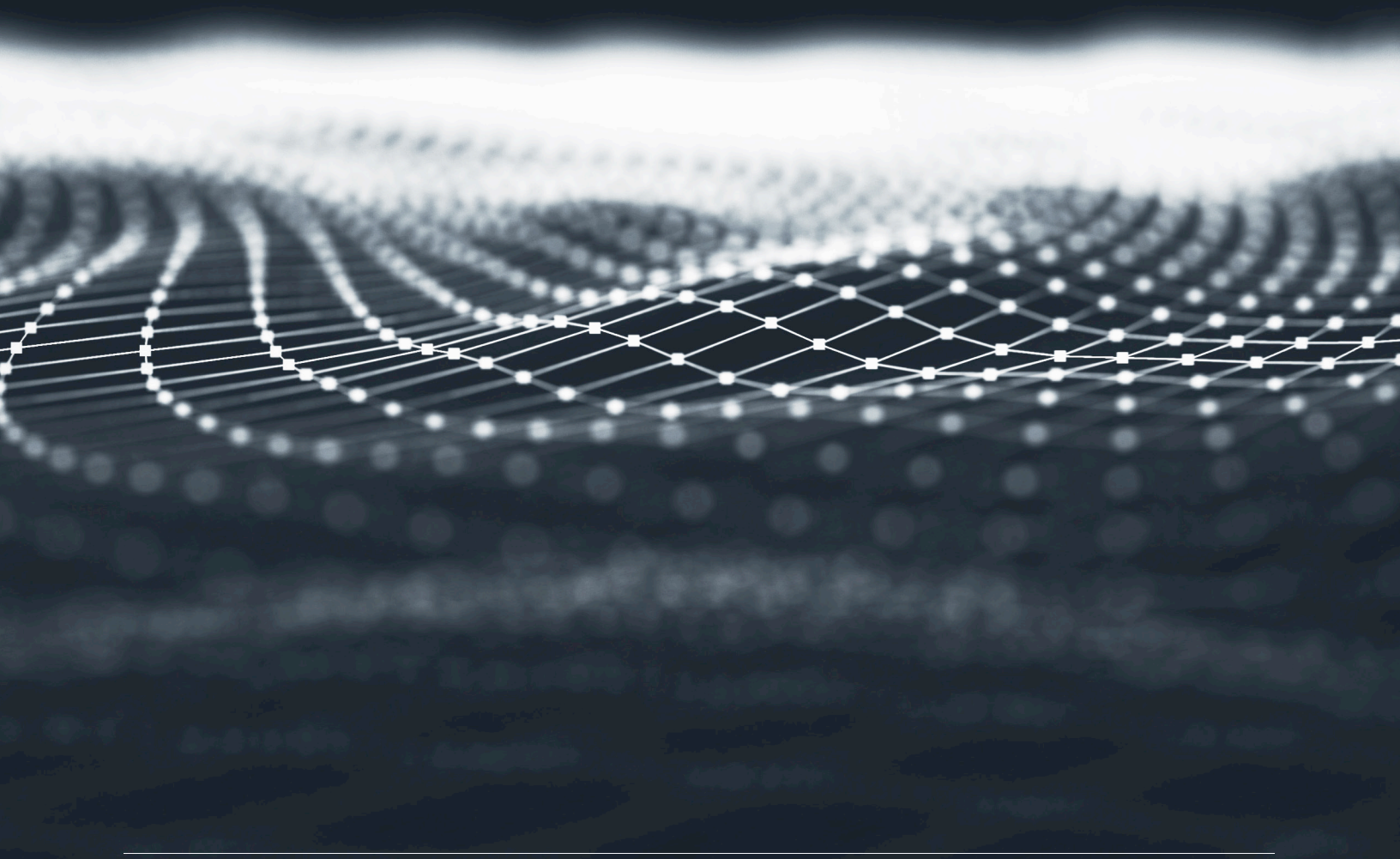
Even before the executive order, advancing towards a Zero Trust Architecture was a priority across the federal government, with the National Institute of Standards and Technology (NIST) and other agencies releasing specific guidance and, in some cases, developing reference architectures.

While agencies developing Zero Trust Architecture designs often begin with a search for new security tools, you can't secure what you can't see. Complex challenges such as data center and cloud blind spots, latency, and irrelevant traffic analysis can severely limit the effectiveness of Zero Trust Architecture policy evaluation and enforcement tools.

A clear strategy and technology foundation for pervasive visibility is the key to overcoming these challenges and implementing an effective Zero Trust Architecture.

Pervasive Visibility Explained

Pervasive visibility means being aware of all data in motion across your physical, virtual, and cloud networks with the help of network visibility tools. Visibility tools are used to keep a close and constant eye on network traffic, monitored applications, network performance, managed network resources, and security threat indicators. To be effective, a pervasive visibility approach must include scalable data collection and aggregation across all on-premises and cloud environments, along with mechanisms to deliver optimized data feeds to specialized performance management and security tools.



Zero Trust Architecture and Key Challenges That Agencies Will Encounter

According to NIST Special Publication 800-207 "Zero Trust Architecture," 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." Stated simply, Zero Trust Architecture assumes that breaches are inevitable and treats every user, device, workload, or dataflow as untrusted until it is explicitly verified.

An effective Zero Trust Architecture must bring many different security technologies together to perform granular, real-time decision-making about network, system, and data access. For this reason, the NIST guidance includes a specific requirement that the "enterprise can observe all network traffic" and extract metadata for use by the Zero Trust policy engine (PE).

Any gaps in network or cloud visibility will undermine the integrity of the Zero Trust Architecture.

Agencies may encounter numerous challenges when attempting to achieve complete visibility across all their environments. SPAN port limitations and contention in on-premises settings make it challenging to see the entire picture of all network activity. In addition, now that use of virtualization is prevalent in federal government data centers, it is increasingly difficult to gain visibility into East-West traffic that never reaches the physical network.

DEFINITION

East-West Traffic
East-West traffic consists of the data packets that move from server-to-server within a data center or cloud environment. Unlike North-South traffic, which generally flows to and from locations outside the network perimeter, East-West traffic may not pass through a network gateway or even reach a physical network in the case of virtualized data centers or cloud environments. As a result, it is more susceptible to monitoring gaps and blind spots.

> 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 as it evaluates access requests.
>
> – NIST SPECIAL PUBLICATION 800-207
> "ZERO TRUST ARCHITECTURE", AUGUST, 2020

Expanding the use of cloud services in accordance with White House and Office of Management and Budget (OMB) guidance increases the visibility challenge dramatically. Cloud services add even more East-West traffic, and the overall volume and complexity of traffic data that agencies must aggregate, harmonize, and distribute multiplies once cloud services are added alongside traditional on-premises infrastructure.

As agencies move to these more complex hybrid cloud architectures, there is much greater potential for blind spots, as depicted in Figure 1. Unless these blind spots are eliminated, any security strategy will not be as effective as it needs to be.

Another consideration that can help agencies achieve an efficient implementation is ensuring that only relevant traffic is flowing to each specific security tool. Overwhelming these tools with irrelevant traffic, such as duplicate packets, reduces tool effectiveness and drives up tool costs.

A final consideration is latency. Implementing a scalable and useable Zero Trust Architecture that supports rapid data delivery and analysis is challenging. Pervasive visibility helps organizations manage complexity and avoid delays or bottlenecks that undermine the user experience and potentially disrupt mission-critical agency activities.

Gigamon Provides the Pervasive Visibility Needed for an Effective and Scalable Zero Trust Architecture

The Gigamon Hawk Visibility and Analytics Fabric™ addresses all of the challenges highlighted below by providing:

+ Pervasive visibility across all on-premises and cloud environments, including East-West traffic visibility in virtualized data centers and cloud environments
+ Centralized, high-velocity data aggregation, analysis, and transformation
+ Near real-time delivery of optimized traffic data to other security technologies and tools deployed as part of a Zero Trust Architecture design

Figure 1. Lack of visibility across data center, cloud, and hybrid cloud environments is a significant obstacle to Zero Trust Architecture adoption.

As shown in Figure 2 below, the Gigamon Hawk Visibility and Analytics Fabric sits between an agency's on-premises and cloud infrastructure and security tools. From this central position, it collects all data in motion, preprocesses it, and delivers it to all Zero Trust Architecture policy decision and enforcement points, as depicted in Figure 3.

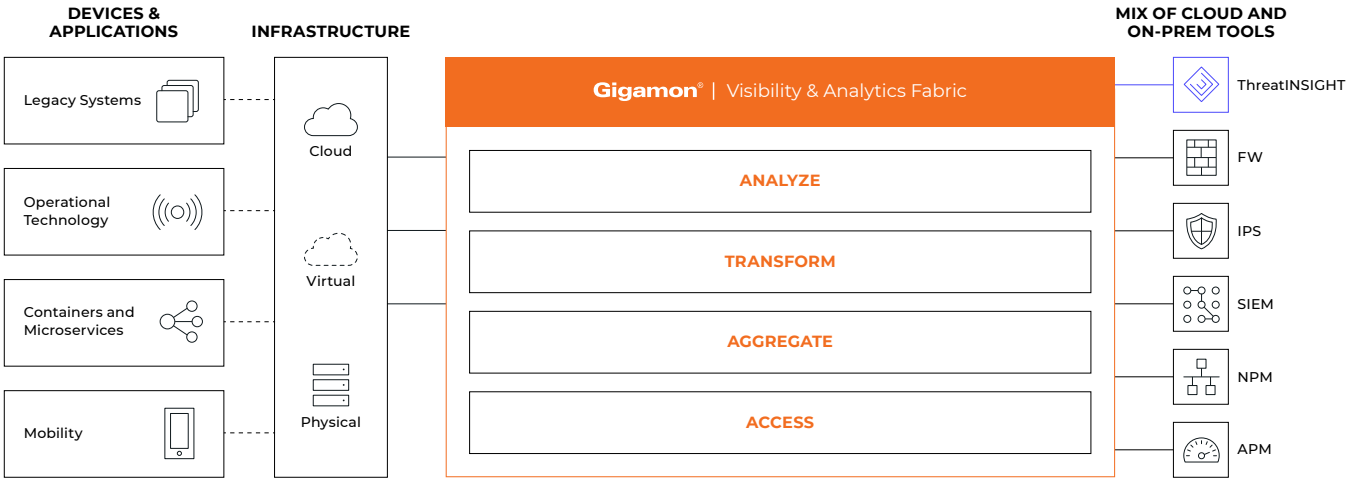


Figure 2. The Gigamon Hawk Visibility and Analytics Fabric enables pervasive visibility across all on-premises and cloud environments, delivering timely, consistent, and actionable data to all other elements of the Zero Trust Architecture.

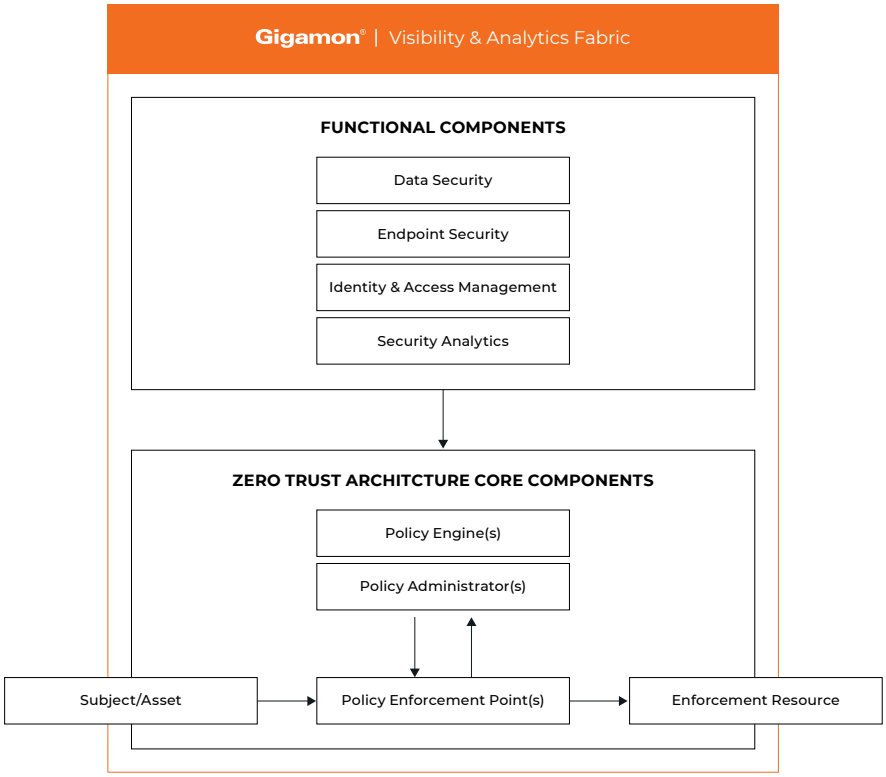


Figure 3. The Gigamon Hawk Visibility and Analytics Fabric brings functional security components together into a real-time data stream that is actionable by core components of the Zero Trust Architecture.

In addition to giving Zero Trust Architecture policy decision and enforcement points the visibility they need to perform their functions, the Gigamon Hawk Visibility and Analytics Fabric also optimizes the performance, scalability, and effectiveness of all core and functional Zero Trust Architecture components. For example, Gigamon can de-duplicate traffic before sending it to security tools, preventing information overload and delaying the need for costly upgrades to meet growing performance demands. Capabilities like Application Filtering Intelligence can also send selective subsets of relevant traffic, filtered with application (Layer 7) granularity, to specific tools when the situation requires it, further reducing unnecessary tool load.

Real-World Example: Zero Trust Architecture at DreamPort

One of the first federal government examples of Zero Trust Architecture deployment at scale is a joint initiative by the Defense Information Systems Agency (DISA), United States Cyber Command (USCYBERCOM) and the National Security Agency (NSA) to implement a live Zero Trust Architecture at DreamPort, the USCYBERCOM's open facility for innovation and collaboration with the private sector.

While the project was a major success, significant lessons were learned that can inform efforts by civilian agencies to design and implement Zero Trust Architectures.

As the team at DreamPort designed their Zero Trust Architecture, they encountered blind spots. For example, the team had limited visibility into the East-West traffic, where a large amount of unsanctioned activity appears, in their virtualized data center environment. As a result of these and other blind spots, the Red Team charged with security testing for the environment was able to access sensitive resources without triggering detection and alerts. Beyond visibility, there were also inefficiency and scalability challenges.

> We ran a test and realized we couldn't see certain events because we weren't inspecting the packets going across the wire. At that point, phone calls were made, and we brought Gigamon on."
>
> – DAVID JONES
> CHIEF ARCHITECT FOR ZERO TRUST CLOUD
> DEPARTMENT OF DEFENSE

Implementing the Gigamon Hawk Visibility and Analytics Fabric as part of the Zero Trust Architecture at DreamPort helped the team overcome the issues described above by:

+ Improving visibility through tapped data paths, SPAN ports, and granular traffic data collection, including for East-West traffic within the virtualized data center environment
+ Optimizing network traffic delivery to cybersecurity and network performance tools, eliminating information overload and making data streams more actionable for other Zero Trust Architecture components

Gigamon and the project team are now building on this initial success by extending visibility and single-pane-of-glass management to the cloud infrastructure with the Gigamon Hawk Visibility and Analytics Fabric and further enhancing visibility in the data center with inline TLS decryption.

Designing for Scalability and Effectiveness

Zero Trust cannot be realized overnight. It's a major shift in philosophy and technology architecture that must be implemented over time. Agencies moving to a Zero Trust Architecture often rush to invest in endpoint security, identity management, and policy enforcement technologies as the first step. These are, in fact, critical components of a mature Zero Trust Architecture, but their value cannot be realized without complete visibility across all on-premises and cloud environments.

This was proven out at DreamPort, and the importance of visibility as a foundation for Zero Trust Architecture is now featured prominently in early guidance provided by defense and intelligence agencies. For example, guidance released by the NSA in February 2021 highlights the need to "Inspect and log all traffic before acting – Establish full visibility of all activity across all layers from endpoints and the network to enable analytics that can detect suspicious activity."

Similarly, DISA's reference architecture, also released in February 2021, emphasizes that "a Zero Trust enterprise will capture and inspect traffic, looking beyond network telemetry and into the packets themselves to accurately discover traffic on the network and observe threats that are present and orient defenses more intelligently."

Civilian agencies that build on these lessons and make pervasive visibility an essential foundation of their Zero Trust Architecture will be well-positioned to avoid protection gaps and achieve success at scale.

Learn How Gigamon Is Driving Zero Trust Deployment Success at Federal Agencies

To learn more about how Gigamon is accelerating and optimizing Zero Trust Architecture at federal agencies today, download the following supporting materials:

Case Study: "Gigamon Adds Crucial Network Visibility to Zero Trust at the Department of Defense"

Whitepaper: "Enabling Secure Innovation at Defense and Intelligence Agencies"

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[1]

50 percent decrease in costs associated with security efforts[1]

58 percent market share in the government sector, nearly four times the nearest competitor[2]

#1 market leader with 38 percent market share, twice the market share of the nearest competitor[2]

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

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

About Gigamon

Gigamon provides network visibility and analytics on all traffic across your physical, virtual, and cloud networks to solve critical security, performance, and business continuity needs. The Gigamon Visibility and Analytics Fabric™ delivers optimized network and security performance, simplified management, and accelerated troubleshooting while increasing your tools' return on investment. Our comprehensive solutions accelerate your organization's ability to detect and respond to security threats, including those hidden in encrypted traffic. Trusted by 83 percent of the Fortune 100 and 4,000 organizations worldwide, Gigamon ensures that your business can run fast and stay secure in The New Tomorrow.

Gigamon®

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

06.21_01