Increasing Visibility and Security While Reducing Risk, Complexity, and Cost

Supporting State, Local, and Educational Institutions

> Today, we enjoy the peace of mind that the continuous uptime and reliability Gigamon delivers with a 100 percent ROI in less than 18 months.
>
> **ANTHONY H. CHOGYOJI**
> Chief Information Security Officer, Riverside County

The cybersecurity threat landscape combined with the growing cost and complexity of managing hybrid cloud infrastructure is evolving rapidly for state, local, and educational (SLED) institutions. These institutions face significant risk from security incidents and performance bottlenecks, which can expose them to substantial financial and reputational damage. The need for efficient and effective security measures has never been more critical to their success.

In recent years, numerous government entities and educational institutions have experienced damage due to security breaches and delayed responses due to network and application performance issues. This situation is compounded by evolving technologies, outdated systems, employee limitations, and budgetary restrictions, all of which challenge an institution's ability to deliver for students and communities. A key challenge facing these institutions is limited visibility into the network traffic traversing their hybrid cloud infrastructure.

More specifically, limited visibility into East-West traffic (lateral movement within the network) and the increasing volume of encrypted traffic creates blind spots where malware and malicious activity can go undetected. The expanded use of Internet of Things (IoT) devices and untrusted Bring Your Own Device (BYOD) systems further exacerbates these challenges.

It is therefore more important than ever for IT and security teams in government and education institutions to find ways to do more with less. For many, the only way to mitigate exposure to security risk is to increase the efficiency and effectiveness of their existing security measures and overall posture.

Key Cybersecurity Challenges for SLED

Limited Network And Cloud Visibility

Government agencies and educational institutions often struggle to collect and analyze data across hybrid cloud infrastructure that spans on-premises, virtual, container, and private and public cloud workloads, making it difficult for security operations teams to gain unobscured visibility into all data in motion.

Disruption To Critical Activities

When existing security tools are entangled with the underlying infrastructure, they can create blind spots and performance bottlenecks that require change management or result in downtime.

Limitations Of Existing Security Tools

While many government and education security teams have deployed a range of existing security tools, their effectiveness can be limited when they rely exclusively on metric, event, log, and trace data to detect threats and remediate accordingly. These limitations result in teams not being able to see the complete picture.

Growing Tool Complexity And Cost

Networks and cloud environments are becoming increasingly complex, leading to tool sprawl and higher management and security costs.

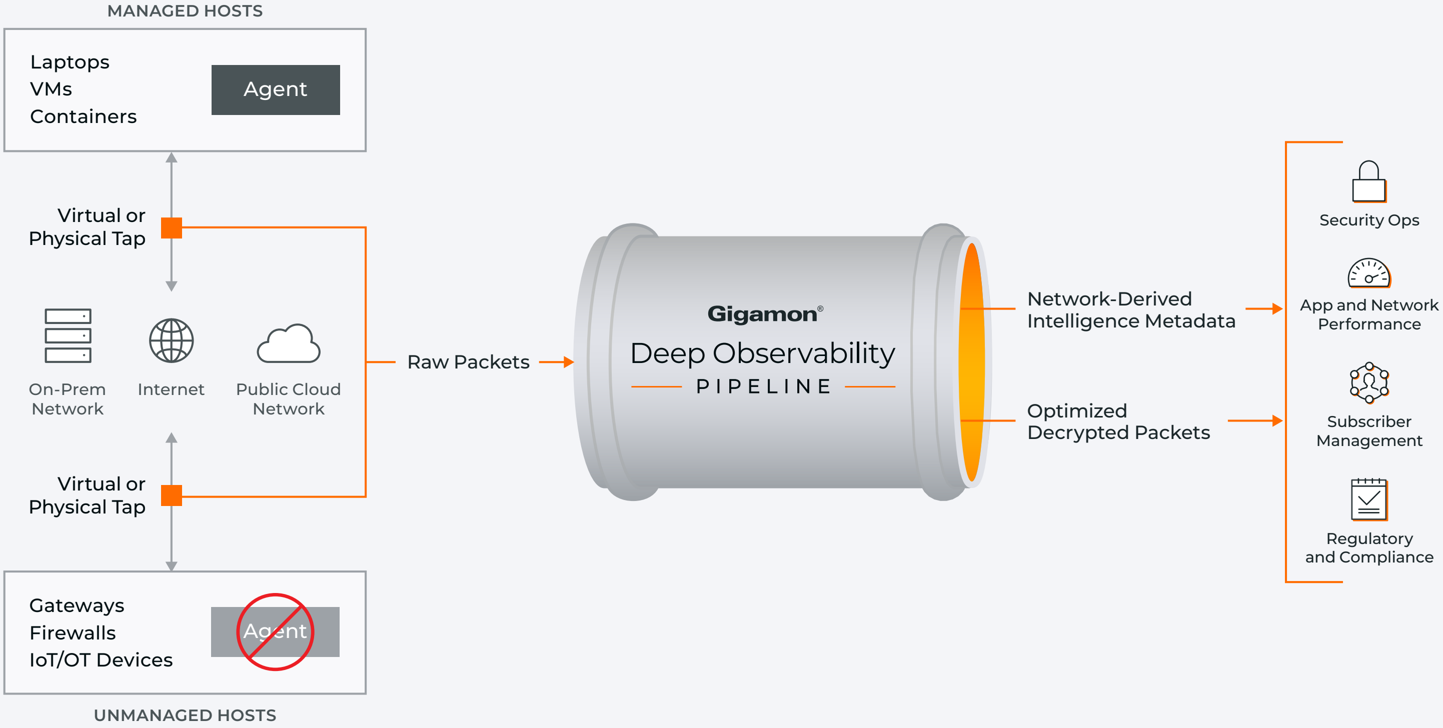

Figure 1. Gigamon accesses all network traffic and then delivers network-derived intelligence to security, network, and observability tools for further analysis.

How Can Gigamon Help?

Gigamon streamlines the process for state, local, and educational industries to secure and manage their hybrid cloud infrastructure in a more efficient and cost-effective manner. The Gigamon Deep Observability Pipeline captures and optimizes traffic as it crosses specific points in your network, then efficiently delivers network-derived intelligence and insights to critical security and performance monitoring tools to bring the complete picture into focus. Positioned between hybrid cloud infrastructure and security, monitoring, and management tools, Gigamon brings deep observability into all data in motion, eliminating security blind spots, optimizing network traffic and reduce the cost and complexity of securing and managing hybrid cloud infrastructure.

Eliminate Blind Spots

You can't secure what you can't see. Gigamon provides deep observability into physical, virtual, and cloud networks through physical and virtual taps. This spans on-premises, virtual, container, private and public cloud workloads.

Encrypted and lateral traffic present major security monitoring challenges, especially with the rise in VPN usage in educational environments, often deployed without split tunnels enabled to avoid unnecessary encryption. Gigamon addresses this challenge, offering centralized TLS/SSL Decryption to enable efficient and cost-effective inspection of encrypted traffic. By eliminating lateral (East-West) traffic blind spots, Gigamon enhances the effectiveness of security tools in detecting and mitigating threats, including ransomware.

Optimize Resource Utilization

As network traffic volumes grow, security and monitoring tools often become overwhelmed. This, combined with tool sprawl increases the cost and complexity teams face in securing and managing their infrastructure. In higher education campus environments, this problem is exacerbated by the large volume of traffic from streaming services such as Hulu, Netflix, and YouTube. These services generate significant traffic volumes but are often considered low-risk traffic that unnecessarily consumes security and performance monitoring tool resources. This forces a compromise between costly upgrades or acceptance of blind spots.

Gigamon features such as Application Filtering Intelligence identify and filter high volume, low-risk application traffic such as Hulu, Netflix, and YouTube, sending only relevant traffic to security tools, improving efficiency and capacity, lowering processing and storage requirements, and enhancing the detection and mitigation of high-risk traffic.

Enhance Network Agility

The Gigamon Deep Observability Pipeline helps institutions remain agile while maintaining effective security and performance monitoring postures. It aggregates traffic acquired by taps and SPAN ports across a hybrid network (including physical, virtual, public cloud, IoT/OT, mobile devices, and containers), delivering only relevant traffic streams and network-derived intelligence to your tools.

The deep observability pipeline acts as an abstraction layer between your infrastructure and tools allowing you to quickly absorb changes without impacting network availability or performance. This avoids painful network interruptions and eliminates single points of failure on the network.

Additionally, Gigamon helps to reduce the workload for IT teams by automating and streamlining network operations, enabling faster response to changing business requirements.

Reduce Cost And Complexity

Organizational growth and the need to respond to changing requirements can lead to unplanned network changes and the creation of an "accidental hybrid" infrastructure. As needs evolve, security and monitoring tools are frequently added on an ad hoc basis, creating environments that are complex to secure and manage.

Gigamon simplifies management by acquiring network traffic once and efficiently delivering optimized data to security, monitoring, and management tools, reducing operational complexity and cost. Gigamon network taps, integral to the Deep Observability Pipeline, provide access to 100 percent of network traffic required to secure, monitor, and manage hybrid cloud infrastructure. This ensures that tools have the data they need, avoiding the trouble of direct access and enabling better troubleshooting and management. By reducing the volume of traffic sent to tools and minimizing data movement costs, Gigamon helps lower cloud costs while maintaining security and performance.

> Gigamon [has] helped us move beyond playing whack-a-mole and chasing every vulnerability, toward a more strategic approach to cybersecurity. It gives us the data we need to build network resilience, reduce our attack surface, and make it harder for threat actors to impact our environment.
>
> **SUTHAGAR SEEVARATNAM**
> CISO of Australian National University

Gigamon complements log-based tools with network-derived intelligence to deliver deep observability across hybrid cloud infrastructure.

	Classic Network Logs	Netflow	Network-Derived Intelligence
Source IP	✓	✓	✓
Source Port	✓	✓	✓
Destination IP	✓	✓	✓
Destination Port	✓	✓	✓
Network Protocol Information	✓	✓	✓
Ingress Interface (if available via SNMP)		✓	✓
Flow start time, bytes		✓	✓
Mac Address, DHCP options			✓
L4-L7 Protocol Intelligence (buffer size, retransmits, errors)			✓
Encryption Levels			✓
Certificate Information			✓
Layer and Encoding			✓
Application Visibility and Metadata			✓

Use Cases

Security

Take control of decryption

- Monitor TLS/SSL versions to verify whether applications have expired certificates or weak ciphers

Gain visibility into all data-in-motion

- Identify compression algorithms used by each application, including endpoints
- Detect and remediate P2P applications, excessive usage of file-sharing services, and data exfiltration
- Identify remote desktop/remote control and non-standard port usage
- Traffic coming from adversarial countries/regions

Secure DNS traffic

- Monitor DNS traffic, identify rogue DNS servers, and assess external DNS server queries
- Analyze DNS transactions with details on DNS server IP, source and destination IP, and application info

Understand at a deeper level

- Investigate and remediate deprecated hash functions
- Visualize Message Authentication Codes (MAC)
- Monitor Perfect Forward Secrecy (PFS)
- Identify compression algorithms used by applications
- Identify unauthorized devices and track all devices on the network

Performance

Identify initial signs of bottlenecks

- Detect applications with long round-trip times
- Number of 404 errors per host
- Number of connections per TLS version across all environments
- Report on TCP and application round-trip-time
- Identify sessions with packet loss
- Identify session with CRC checksum failures
- Understand response times of various DNS servers

Quickly pinpoint the root cause of performance issues

- Understand whether an issue is because of a network issue, application issue, or both
- Pinpoint servers that are not performing as expected

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.

To learn more, please visit gigamon.com.

Gigamon®

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