Unified Data Management Leveraging Gigamon Network Telemetry and Splunk Federated Data Access

Delivering Complete Visibility and Control with Efficient, Compliant Data Access Across Hybrid and Multi-Cloud Environments

KEY BENEFITS

- End-to-End Data Control: Network-derived telemetry and processors for intelligent, location-optimized data preparation.
- Unified Data Access: Federated Search across all data sources and reduce the need for costly data duplication.
- Operational Efficiency: Process only what you need, where you need it to reduce ingestion costs and storage footprint.
- Strengthened Security Posture: Gain complete visibility into lateral and encrypted traffic, internal threats, and policy violations across environments.

The Gigamon Deep Observability Pipeline captures raw network traffic (north-south and East-West) and extracts rich L2–L7 metadata using deep packet inspection. This network-derived telemetry is then efficiently delivered to Splunk where it is enriched and correlated with logs, metrics, events and traces (MELT) data from other sources to form the foundation of a unified data management strategy:

Gigamon Visibility with Splunk Edge Processor

The Gigamon Deep Observability Pipeline efficiently delivers network-derived telemetry—including application metadata, threat indicators, and decrypted traffic—directly to the Splunk Edge Processor. This enables real-time filtering, masking, and enrichment at the source,

reducing unnecessary data volume, conserving bandwidth, and accelerating time-to-insight while strengthening compliance and data privacy.

Gigamon-Optimized Data with Splunk Ingest Processor

Traffic intelligence provided by Gigamon is aggregated, deduplicated, and optimized before reaching Splunk Cloud. This ensures the Ingest Processor receives only high-value, security- and performance-relevant data for dynamic routing, enrichment, and redaction. The result is lower ingestion costs and more actionable, compliant data for indexing and analytics.

Gigamon Telemetry with Splunk Federated Search

By integrating Gigamon metadata and traffic intelligence, Splunk Federated Search delivers broader visibility across distributed and siloed datasets without requiring centralized storage. This combination ensures secure, consistent access to complete, reliable network data across hybrid and multi-cloud environments—accelerating investigations and improving outcomes for security, compliance, and performance use cases.

1. Network Intelligence Extraction

Gigamon acquires and processes network traffic from on-prem, cloud, virtual, containers, and IoT sources, extracting application aware metadata that offers deep insights into application performance, user behavior, and potential security threats.

2. Distributed Pre-Ingest Processing

Organizations can choose their processing strategy:

- Splunk Edge Processor filters and enriches data onpremises at or near Gigamon collection points.
- Splunk Ingest Processor provides centralized cloud-based processing to standardize and optimize data before indexing.

3. Data Routing

Data processed by Splunk Edge/Ingest Processor can be routed to either Splunk Index or third-party storage solution provider like AWS S3 or Azure Blog Storage

4. Federated Access to All Data

With Splunk Federated Search, security, devops, and operations teams can query:

- Indexed Splunk data across different environments
- Supported third-party data sources

This delivers deep observability and a truly unified view across all relevant datasets for comprehensive threat hunting, compliance, and performance analysis, and forensic investigation.

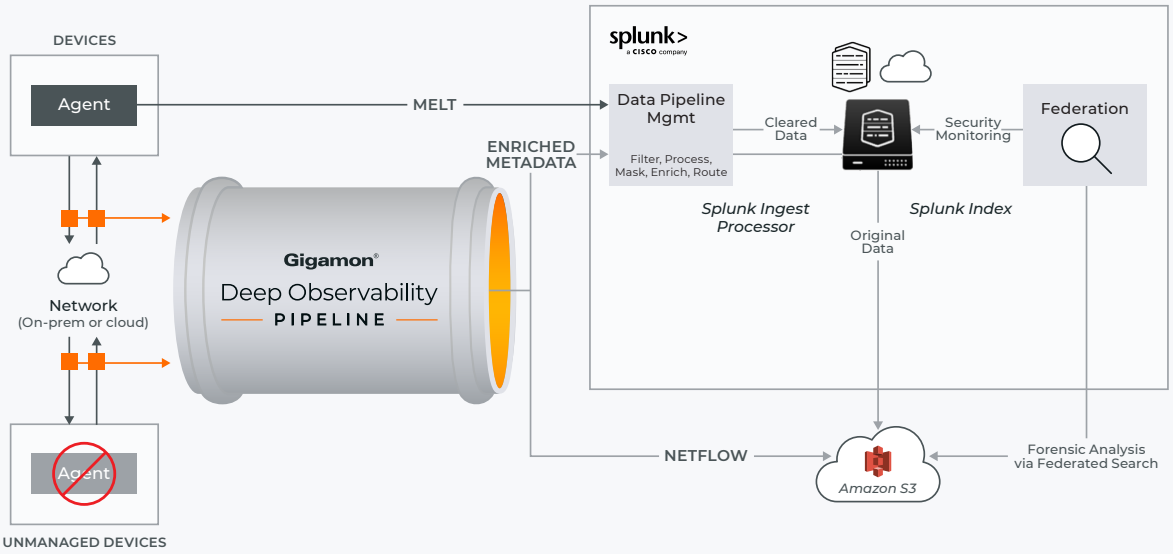

Figure 1. The Gigamon Deep Observability Pipeline efficiently delivers L2-L7 network-derived telemetry to the Splunk Ingest Processor.

Compliance: PCI DSS4.0

Integration with Splunk

R1: Network Traffic	R2: Default Configurations
Firewall Rule Activity	Default Account Access
Network Traffic Activity	Insecure Authentication Attempts
Prohibited Services	PCI System Inventory
• PCI–Non-PCI Network Communication	Primary Functions
• Monitor DNS	Prohibited Services
• Rogue DNS Servers	System Misconfigurations
• External DNS Server Query	Wireless Network Misconfigurations
• Monitor FTP	• Verify Separation of Network Services
• Monitor SMBv1	• Detect Unnecessary Services
• Monitor Traffic Between CDE and Non-CDE Network	• Verify unsecure Protocols and Services
• Monitor IoT and BYOD	• Verify Administrative Traffic is Encrypted at the Appropriate Level

• Additional visibility provided by Gigamon

Use Case	Data Required	Benefits
Compliance and Governance Strengthen regulatory reporting and audit readiness	• Gigamon TLS metadata • Endpoint/workload context • Splunk audit, cloud, and identity logs	Gigamon network-derived telemetry enriches Splunk dashboards for automated compliance reporting

Use Case	Data Required	Benefits
Security Posture Improve threat detection and hunting, and attack chain coverage.	• Gigamon provides insights into East-West lateral flows • TLS Fingerprints, DGA scores • Splunk SIEM events, identity data, threat intel	Gigamon endpoint/IP context boosts Splunk detections; actions automated via Splunk SOAR

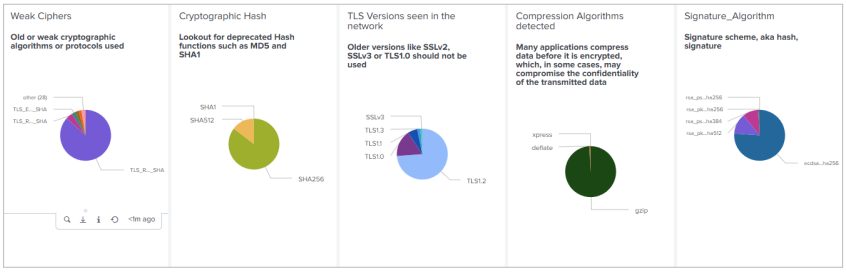

Figure 2. Boost detections and highlight operational risk.

Use Case	Data Required	Benefits
Operational Excellence Drive service reliability, MTTR reduction, and SLO tracking	• Gigamon network performance telemetry • Splunk observability and ITSI metrics	Performance insights from Gigamon network-derived telemetry accelerate Splunk playbooks to quickly isolate root cause

Figure 3. Quickly identify performance bottlenecks and isolate the root cause.

Support and Services

Gigamon offers a range of support and maintenance services. For details regarding the Gigamon Limited Warranty and its Product Support and Software Maintenance Programs, visit gigamon.com/support/support-and-services.

About Gigamon

Gigamon® delivers an AI-powered Deep Observability Pipeline that provides network-derived telemetry to cloud, security, and observability tools. With AI-driven insights across packets, flows, and application metadata, organizations gain complete visibility into all data in motion to detect threats concealed in encrypted and lateral traffic, resolve network and application performance issues, and validate compliance while reducing operational cost and complexity. Gigamon is trusted by 4,000+ organizations worldwide, including 83 of the Fortune 100. Learn more at gigamon.com.

Gigamon®

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