Gigamon® | splunk> a CISCO company

How Gigamon and Splunk Reduce Premium Data Movement While Preserving Investigation Context

As a Splunk Data Federation alpha participant and launch partner, Gigamon is helping shape a new approach for customers that need deeper visibility without the cost and complexity of centralizing every dataset. By combining Gigamon Application Metadata Intelligence (AMI) and the Gigamon Deep Observability Pipeline with Splunk Data Federation, joint customers can access high-value network-derived telemetry where it resides, support investigations across distributed environments, and create a more efficient path to security, operations, and compliance outcomes.

In a joint validation scenario, the combined solution processed 299K total events while routing only 6.04K events to the Splunk index and retaining the full dataset in Amazon S3 for lower-cost retention and extended investigation workflows.

This case study outlines the customer challenge, the joint solution approach, and the operational and cost-efficiency outcomes demonstrated during validation testing.

THE CHALLENGE

Security and operations teams increasingly struggle to balance visibility, investigation depth, and data management cost across hybrid and multi-cloud environments.

Customers want to:

- **Maintain** visibility across distributed datasets
- **Reduce** unnecessary premium ingestion and storage costs
- **Accelerate** investigations and operational workflows
- **Preserve** access to telemetry needed for security, compliance, and audit use cases

This challenge becomes more important as data volumes grow and teams are asked to do more with tighter budgets and more distributed infrastructure.

The Gigamon and Splunk Solution

Gigamon extends the value of Splunk Federated Search by making high-fidelity network-derived telemetry available for distributed access and analysis.

With the Gigamon Deep Observability Pipeline, customers can extract rich application and network metadata from traffic across hybrid environments. The telemetry can be routed in a search-ready format to Splunk indexes and lower-cost storage tiers such as Amazon S3, allowing organization to access and analyze distributed data without relying solely on centralized ingestion.

Together, Gigamon and Splunk help customers move toward a more practical data strategy:

- **Gigamon** delivers relevant, structured network intelligence
- **Splunk Data Federation** enables access to distributed data where it resides

The combined approach improves visibility while reducing unnecessary data movement.

How the Joint Approach Works

The joint workflow enables organization to selectively index high-value telemetry while preserving broder datasets for federated investigation and long-term retention. This enables teams to:

1. Capture and enrich network traffic with Gigamon AMI
2. Route high-value telemetry to Splunk indexes while retaining broader datasets in lower-cost storage tiers
3. Use Splunk Data Federation to query relevant datasets directly
4. Investigate and analyze distributed data through a more unified view

This model helps customers preserve access to valuable telemetry while being more selective about what they ingest into premium analytics tiers.

Operational and Business Impact

BETTER VISIBILITY ACROSS DISTRIBUTED ENVIRONMENTS

Gigamon provides deep observability into data in motion, helping customers see network activity that may otherwise be difficult to access through logs alone. With Splunk Data Federation, that visibility can be extended across distributed datasets without adding more data sprawl.

MORE COST-EFFECTIVE DATA ACCESS

Instead of centralizing every dataset in premium analytics tiers, organizations can retain more telemetry in cost-efficient storage while still querying it when needed through federated search workflows. This creates a more balanced model for data retention, access, and investigation.

FASTER INVESTIGATIONS AND OPERATIONAL INSIGHT

By combining federated access with network-derived telemetry, teams can investigate issues with more context and reduce the time spent pivoting between disconnected data sources.

SUPPORT FOR SECURITY, OPERATIONS, AND COMPLIANCE USE CASES

The joint approach can support use cases such as:

- Security investigations across hybrid environments
- Operational troubleshooting and workflow analysis
- Compliance reporting and audit support
- Broader access to telemetry for cross-team analysis

Why Gigamon

Gigamon helps organizations transform raw network traffic into high-fidelity actionable telemetry that supports security, observability, and operational workflows. For Splunk customers, this creates:

- **Richer context** for distributed investigations
- **Greater flexibility** in telemetry routing and retention
- **Improved efficiency** for federated search workflows
- **Stronger readiness** for AI-driven analytics and security operations

Launch Partner Perspective

Gigamon participation in the Splunk Federated Search alpha program reflects a shared focus on helping customers modernize how they manage telemetry. The validation reinforced a clear customer need: organizations want access to better telemetry and investigation context without forcing all data into centralized premium analytics tiers.

Testing Results

Testing validated the joint data path across ingest, indexing, and federated access.

In this testing scenario, 299K total events were processed through the pipeline. The pipeline was configured to forward only ssl_cipher_suite_id, ssl_protocol_version, and 5-tuple fields to the Splunk index, while retaining the full 299K-event dataset in Amazon S3 for lower-cost retention and compliance workflows.

Only 6.04K events were routed to the Splunk index, confirming that the indexed tier can stay intentionally small while the broader dataset remains available for deeper analysis. This creates a more efficient workflow for rapid triage in Splunk while preserving access to full-fidelity records for deeper investigation and compliance use cases.

- **Search workflow observations:** The indexed dataset exposed the core fields most useful for rapid filtering and triage, including app_name, source and destination IP, destination port, ssl_cipher_suite_id, and ssl_protocol_version.
- **Schema and dataset findings:** The federated dataset preserved the full raw event structure, including certificate, byte, packet, timing, and flow metadata, showing that selective indexing does not require sacrificing investigative depth.
- **Operational benefits observed:** The validation demonstrated a practical split between premium analytics and lower-cost retention. Analysts can search a smaller indexed footprint for everyday workflows and pivot to S3-backed data when they need full event detail for compliance or deeper forensics.

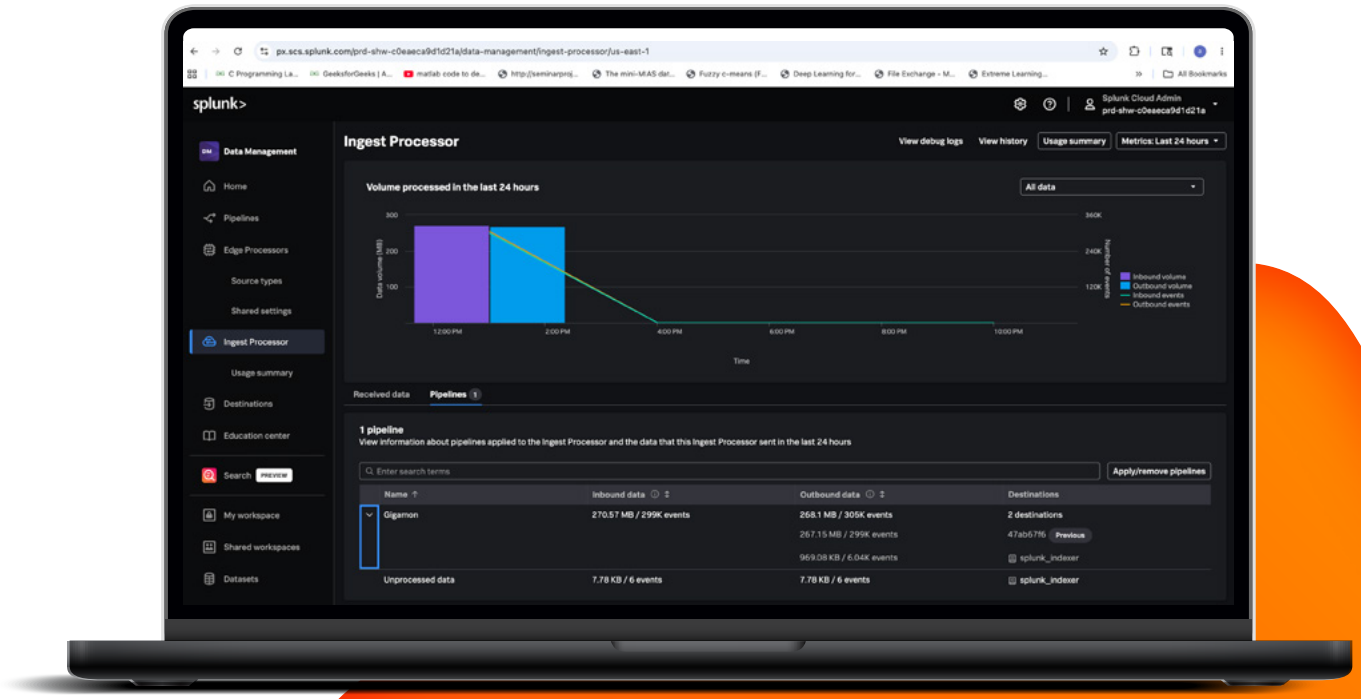

Figure 1. Splunk Ingest Processor usage summary showing 299K inbound events and selective routing to two destinations.

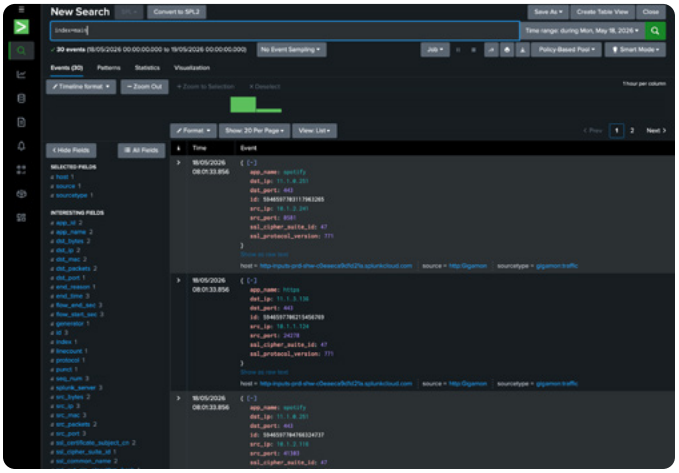

Figure 2. Splunk index search returning the reduced indexed record set with search-optimized fields.

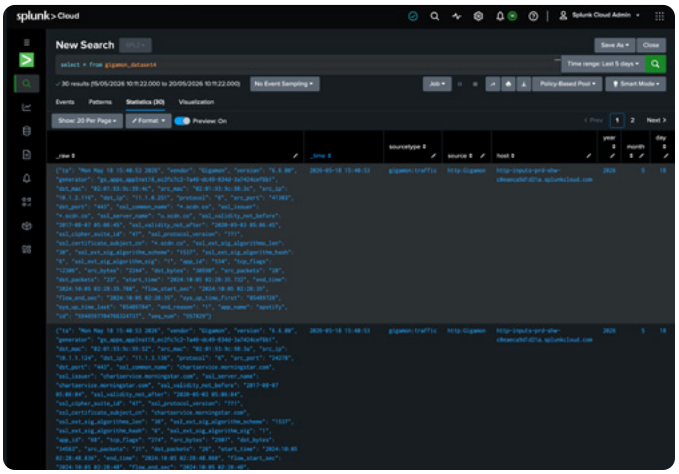

Figure 3. Federated dataset query showing the full raw event schema retained in the lower-cost data tier.

ROI and Business Impact

This validation demonstrates how organizations can reduce premium indexed volume while preserving access to full-fidelity telemetry for investigation, compliance, and long-term retention. In this specific test case, routing 6.04K of 299K total events to the Splunk index demonstrated the potential to materially reduce premium indexed event volume while still preserving access to the full dataset through Splunk Data Federation.

Actual results will vary based on each customer's environment, data mix, and filtering policies, so this outcome should be viewed as directional rather than prescriptive. For most customer planning scenarios, a more realistic expectation is a 50 to 70 percent reduction in premium indexed volume, depending on deployment design and the specific telemetry selected for indexing.

- In this validation scenario, approximately 50x fewer events were routed to the premium indexed tier.
- By data volume, the indexed output shown in testing was under 1 MB, compared with roughly 267 MB retained in the lower-cost destination, illustrating how selective routing can shrink premium data handling for this workflow.
- Full 299K-event retention in Amazon S3 supports compliance, audit, and extended investigations without forcing all data into the premium tier.
- Better analyst efficiency because routine searches can begin against a smaller, more targeted dataset and expand only when deeper context is needed.

For customers, the business impact is a more balanced telemetry strategy: reserve premium Splunk resources for high-value search workflows, retain the rest in cost-efficient storage, and still query both when needed. That combination can improve budget efficiency, reduce data-management overhead, and shorten the path from initial search to full-context investigation.

Summary

Gigamon and Splunk are helping organizations take a more efficient and flexible approach to telemetry management. By combining high-fidelity network-derived telemetry with federated access to distributed datasets, the joint solution helps organizations improve visibility, accelerate investigations, control premium data costs, and preserve access to the telemetry needed for security and operational workflows.

This is the promise of the joint solution: the ability to operationalize high-value telemetry wherever it resides.

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, including 83 of the Fortune 100 and hundreds of public sector agencies and educational institutions.

Learn more at **gigamon.com**.

Gigamon®

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

06.26_01