JOINT SOLUTION BRIEF

Gigamon and Splunk Federated Search

As data volumes continue to grow across hybrid cloud and AI-driven environments, organizations are increasingly challenged to balance visibility, operational efficiency, compliance requirements, and cost. Security and IT teams need access to telemetry across distributed environments, but centralizing every dataset for search and analysis can increase complexity and drive up costs.

Gigamon and Splunk address this challenge by combining high-fidelity network-derived telemetry with federated data access. Together, the Gigamon Deep Observability Pipeline and Splunk Federated Search provide a more flexible approach to accessing and analyzing telemetry where it resides, helping organizations reduce unnecessary data movement while improving visibility across security, operations, and compliance workflows.

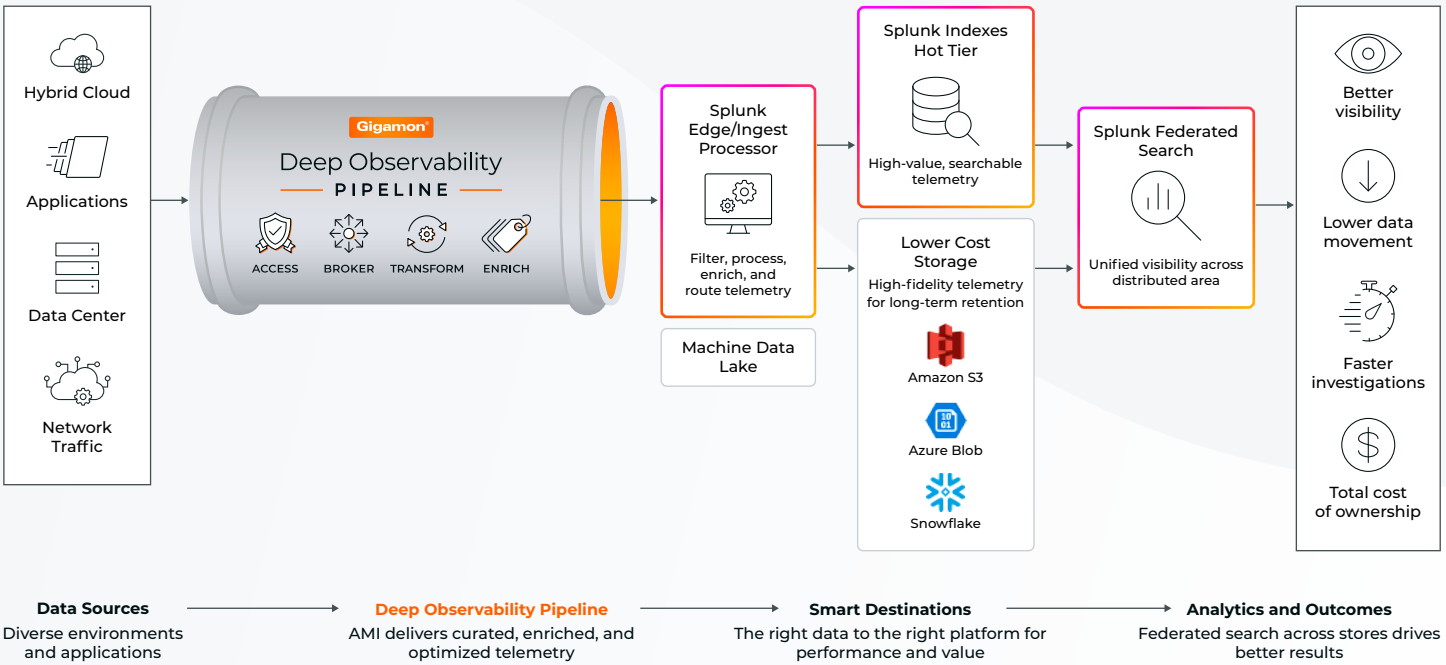

Figure 1. How Gigamon and Splunk deliver unified visibility across indexed and lower-cost telemetry repositories.

The Challenge of Accessing Distributed Telemetry

Modern enterprises generate and store telemetry across on-premises infrastructure, public and private clouds, and lower cost data repositories such as Amazon S3 and Azure Blob Storage. As data volumes continue to grow, security and IT teams are often forced to choose between maintaining complete visibility and controlling the cost and complexity of managing large volumes of telemetry.

In many environments, organizations difficult tradeoffs:

- **Centralize** all telemetry for analysis and absorb higher ingestion and storage costs
- **Limit** data collection and risk losing access to valuable operational and security insights
- **Manage** fragmented workflows across disconnected tools, repositories, and teams

These challenges can slow investigations, increase operational complexity, and make it more difficult to support security, compliance, and business requirements across distributed environments.

The Joint Solution

The Gigamon Deep Observability Pipeline transforms raw network traffic into high-fidelity, actionable telemetry by extracting and enriching application metadata across physical, virtual, cloud, and containerized environments.

Using Gigamon Application Metadata Intelligence (AMI), organizations can generate network-derived telemetry that provides deeper visibility into applications, services, and communications across hybrid cloud infrastructure. This telemetry can be routed to Splunk indexes and lower-cost storage repositories such as Amazon S3 and Azure Blob Storage, helping organizations retain access to valuable data while optimizing storage and analytics costs.

Splunk Federated Search extends this value by enabling teams to access and analyze distributed datasets where they reside, reducing unnecessary data movement while providing unified visibility across security, operations, and compliance workflows.

GIGAMON FEDERATED SEARCH APP

Available today on Splunkbase, the Gigamon Federated Search App simplifies deployment and operationalization of the joint solution.

The app includes:

- **Pre-built processing pipelines** for Splunk Edge Processor and Ingest Processor
- **Federated search templates**
- **Unified dashboards**
- **Guided workflows** for analyzing distributed telemetry

Together, these capabilities help organizations accelerate deployment and gain faster access to network-derived insights across distributed environments.

How It Works

The joint solution supports a practical distributed data strategy:

1. Capture and enrich traffic using the Gigamon Deep Observability Pipeline and Gigamon AMI across physical, virtual, cloud, and containerized environments.
2. Process, filter, and route high value network-derived telemetry to Splunk indexes, Amazon S3, Azure Blob Storage, and other supported repositories.
3. Use Splunk Federated Search to access and analyze distributed datasets directly without requiring centralized storage or duplication.

4. Investigate, Visualize and operationalize telemetry through unified search, dashboards, and security workflows.

This model provides organizations with more control over what is ingested, what is retained in lower-cost storage, and how data is accessed over time.

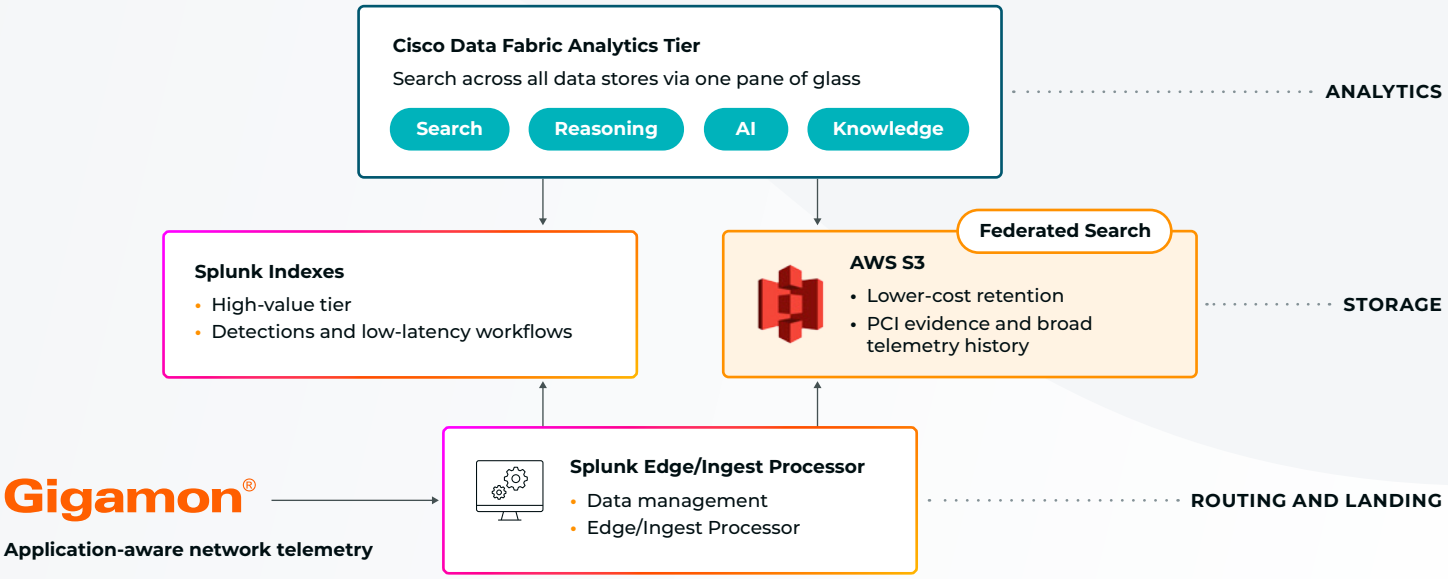

Figure 2. Application-aware network telemetry with federated access across distributed storage.

Key Benefits

Gain deeper visibility across distributed and hybrid cloud environments

The Gigamon Deep Observability Pipeline delivers high-fidelity network-derived telemetry that provides visibility into encrypted, lateral, and application traffic across hybrid environments. Splunk Federated Search extends access to that telemetry wherever it resides.

Reduce data movement and optimize telemetry costs

By intelligently filtering, enriching, and routing telemetry before storage and analysis, organizations can reduce unnecessary ingestion, retain more data in cost-efficient repositories, and improve overall telemetry economics.

Enable earlier threat detection and faster investigations

Combining federated access with rich network context helps security and operations teams investigate issues faster, uncover hidden activity, and reduce time spent moving between disconnected datasets and tools.

Support security, operations, and compliance initiatives

The joint solution provides a scalable foundation for threat investigations, operational troubleshooting, service analysis, audit readiness, and long-term telemetry retention strategies.

Example Use Cases

Security and threat investigation

Security teams can access and analyze distributed telemetry enriched with network-derived context to investigate suspicious activity, uncover hidden threats and accelerate incident response across hybrid cloud environments.

Operations and service analysis

Operations teams can analyze application and network performance across distributed environments without centralizing every dataset, helping improve troubleshooting efficiency and service visibility.

Compliance reporting

Organizations can retain historical telemetry in cost-efficient repositories while maintaining federated access for compliance reporting, audit investigations, and long-term retention requirements.

Financial services and PCI-focused workflows

Industries with stringent regulatory and compliance requirements, including financial services, can benefit from long-term telemetry retention, encryption visibility, audit support, and cost-effective access to distributed data.

Conclusion

Together, Gigamon and Splunk help organizations gain access to high-fidelity, network-derived telemetry wherever it resides. By combining the Gigamon Deep Observability Pipeline with Splunk Federated Search, customers can improve visibility, reduce unnecessary data movement, optimize telemetry costs, and accelerate security and operational outcomes across distributed environments.

The result is a more flexible, scalable, and AI-ready approach to accessing, analyzing, and operationalizing distributed telemetry.

About Splunk

Splunk was founded to pursue a disruptive new vision: make machine data accessible, usable and valuable to everyone. Machine data is one of the fastest growing and most pervasive segments of “big data”—generated by websites, applications, servers, networks, mobile devices and all the sensors and RFID assets that produce data every second of every day. By monitoring and analyzing everything from customer clickstreams and transactions to network activity and call records—and more—Splunk turns machine data into valuable insights no matter what business you’re in. It’s what we call Operational Intelligence.

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.

For more information on Gigamon and Splunk please visit:

gigamon.com | splunk.com

Gigamon®

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

07.26_01