Gigamon®

Enhance CrowdStrike Falcon Next-Gen SIEM with Gigamon Deep Observability

Overview

Organizations operating across hybrid and multi cloud environments face growing challenges in detecting adversarial attacks and securing critical infrastructure. Siloed tools, rising data volumes, and persistent blind spots across distributed networks, encrypted communications, and east-west traffic make it difficult to detect threats quickly, pinpoint root causes, and resolve performance issues before they escalate. At the same time, many legacy security and monitoring tools struggle to keep pace with today's dynamic workloads, leaving teams with delayed incident response, operational inefficiencies, and increased risk to critical systems and sensitive data.

Gigamon addresses these challenges by delivering network-derived intelligence from packets, flows, and metadata across hybrid cloud infrastructure. With deep visibility into lateral and encrypted traffic, Gigamon helps security teams expose activity that other data sources may miss and deliver higher-value telemetry to cloud, security, and observability platforms.

For organizations using CrowdStrike Falcon Next-Gen SIEM, Gigamon improves the value of SIEM analytics by filtering low-risk traffic, extracting actionable context, and forwarding enriched network intelligence for deeper analysis. The result is better detection, faster investigation, and more efficient use of security resources.

What Gigamon helps you achieve:

- Contain attacks faster and limit business disruption: Correlate CrowdStrike alerts with real network evidence in one place to shorten investigations and support faster containment decisions. Give leaders clearer answers to the question, "Are we contained?" during an incident, helping reduce downtime and financial impact.
- Close visibility gaps across hybrid and encrypted traffic: See activity on unmanaged, IoT/OT, and east-west traffic that endpoint agents and logs may miss. Detect credential abuse, lateral movement, command-and-control activity, and data exfiltration even when traffic is encrypted.

- Improve security ROI while controlling SIEM and tool costs: Pre-filter and enrich traffic before it reaches the SIEM so you index less but learn more. Reduce ingest and storage costs, cut low-value alerts, and free analyst time for higher-risk threats.

The result: organizations can establish robust security and monitoring postures, simplifying access to critical intelligence, eliminating blind spots, and shifting resources to focus on high-risk traffic.

Why SIEM Teams Need Network Visibility

As organizations expand into hybrid and multi cloud environments, security teams must manage reduced visibility and control, fragmented operating models across clouds, and growing complexity in the tools and processes required to maintain consistent security and performance monitoring.

Gigamon improves this picture by tapping into all network traffic, including encrypted and lateral movement, through physical and virtual taps. Traffic is then aggregated, inspected, filtered, and enriched to create rich network-derived intelligence that can be delivered to CrowdStrike Falcon Next-Gen SIEM for broader analysis alongside other telemetry sources. This enables organizations to quickly resolve incidents, and detect security threats that may have previously flown under the radar.

The Challenge

Organizations with hybrid cloud and even multi cloud environments are becoming the norm. However, moving applications to public clouds or developing cloud-native applications bring new challenges, such as:

- Decreased visibility and control, raising security and compliance risks
- Multi cloud “silos” that make it nearly impossible to maintain a consistent security posture and quickly pinpoint the root causes of performance issues
- New tools and processes — which could vary by cloud — for teams to invest in and learn

All of the above can slow your cloud initiatives and make life harder for your teams. But what if Gigamon could address these critical hybrid cloud challenges?

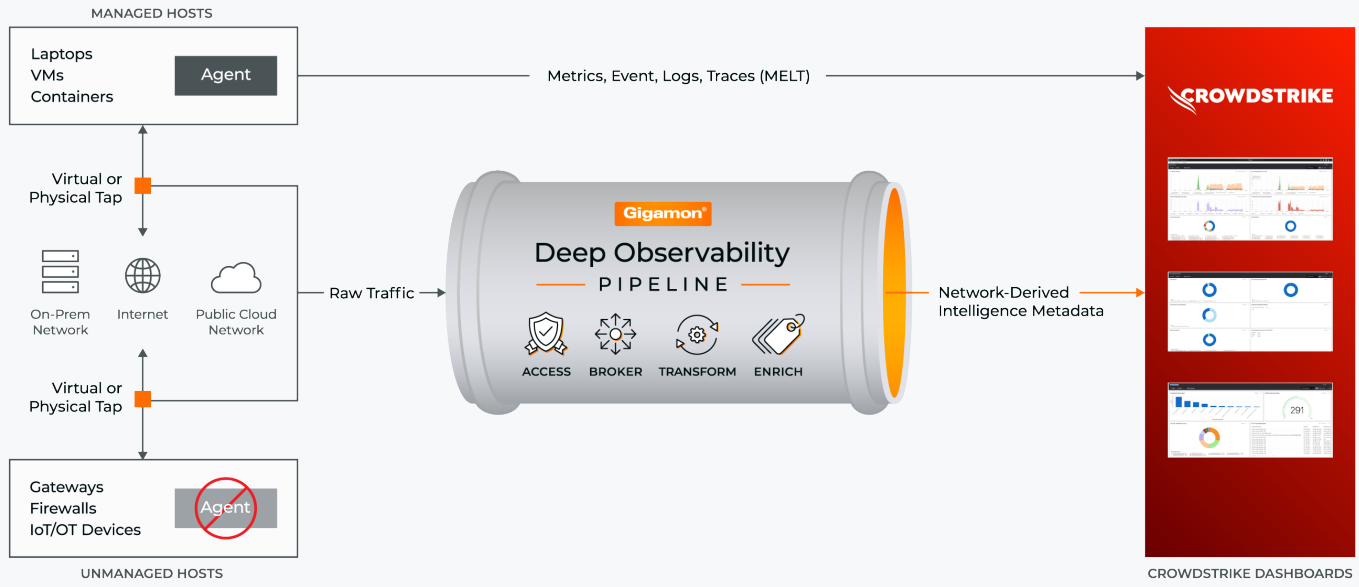

Figure 1. Gigamon accesses all network traffic and efficiently delivers network-derived intelligence and insights to CrowdStrike for comprehensive application monitoring and security.

The Solution

Gigamon Deep Observability Pipeline gives CrowdStrike Falcon Next-Gen SIEM the ability to see what is also happening in hybrid cloud deployments.

How Gigamon Improves CrowdStrike Falcon Next-Gen SIEM Outcomes

1. Faster Investigations and Response

Gigamon adds network context that helps analysts validate alerts, understand what is communicating across the environment, and move more quickly from detection to investigation and containment. This supports faster threat detection, proactive incident response, and reduced mean time to resolution.

2. Broader and Deeper Coverage

Gigamon extends visibility into encrypted traffic, east-west movement, unmanaged systems, IoT devices, container communications, and non-standard port usage, helping security teams uncover threats that may otherwise remain hidden.

3. Better Data Economics for the SIEM

Gigamon helps organizations streamline data delivery by extracting and forwarding actionable network-derived intelligence instead of indiscriminately pushing raw, low-value traffic into downstream tools. That means stronger signal quality for Falcon Next-Gen SIEM and more control over ingest and storage costs.

Key Gigamon Capabilities for Organizations Using CrowdStrike Falcon Next-Gen SIEM

Deep Application Insights

Gain granular visibility into application behavior across hybrid cloud environments to troubleshoot faster and improve performance.

Unified Hybrid Cloud Visibility

Eliminate blind spots with centralized visibility into all network traffic, including encrypted traffic and lateral movement, across any environment.

Streamlined Data Delivery

Deliver actionable network-derived intelligence to existing security and observability tools in a way that simplifies workflows and maximizes tool value.

Real-time Application Awareness

Instantly identify application communication patterns to detect anomalies and potential security risks.

Accelerated Threat Detection

Use real-time network-derived intelligence to speed the identification, containment, and remediation of cyberattacks.

Security and Operations Benefits

Stronger Threat Detection and Security Posture

Combine log data with network-derived intelligence to detect lateral movement, geographic anomalies, vulnerable systems, and previously unseen threats.

API and Encryption Visibility

Identify improper inventory management, broken access controls, and PII exposure risks, while also detecting expired or untrusted SSL/TLS certificates and supporting certificate compliance efforts.

DNS and Network Behavior Analysis

Analyze DNS activity, identify DNS servers, and build a deeper understanding of network traffic patterns to help expose suspicious activity and improve investigations.

Business Outcomes

Gigamon helps organizations using CrowdStrike Falcon Next-Gen SIEM strengthen security coverage, improve operational efficiency, and reduce unnecessary data volume entering the SIEM. By combining deeper network visibility with filtered, enriched telemetry, teams can detect threats earlier, investigate with greater confidence, and focus resources where risk is highest.

Faster Incident Resolution

Minimize MTTR with insight into application and network round-trip times, bandwidth, and CRCs.

Better Application and Protocol Visibility

Pinpoint known and unknown applications and protocols, including crypto mining and non-standard port usage, to improve performance and identify abnormal behavior faster.

Simplified Troubleshooting

Gain insight into DHCP server responsiveness and client-server communication to streamline issue resolution.

Unified Log and Network Intelligence

Complement log usage with network-derived metadata to support more comprehensive dashboards and stronger analytical context inside the SIEM.

Summary

Gigamon enhances CrowdStrike Falcon Next-Gen SIEM by adding deep observability across hybrid cloud environments, expanding visibility into encrypted and lateral traffic, and delivering enriched network intelligence that helps security teams move faster and operate more efficiently. The result is improved threat detection, clearer investigations, stronger coverage of hard-to-see environments, and better control over SIEM data costs.

For more information on the Gigamon Deep Observability Pipeline and CrowdStrike Falcon Next-Gen SIEM, please visit: https://marketplace.crowdstrike.com/partners/gigamon.

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 CrowdStrike, please visit
gigamon.com | crowdstrike.com

Gigamon®

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

05.26_02