Take Control of Intelligence Across Your Infrastructure with Gigamon and Cribl

Overview

Organizations are faced with the challenge of securing their complex infrastructure from an ever-changing threat landscape. Unfortunately, this challenge includes many different obstacles. The threat landscape is aggressively becoming more sophisticated, infrastructures are constantly evolving, technological advancements like new applications and IoT/OT devices present a new frontier of challenges, and a lack of consistent investment in modernizing monitoring efforts have left organizations short-handed in the battle to secure their infrastructure.

Gigamon and Cribl provide a joint solution to help organizations gain complete observability across their entire infrastructure for efficient and effective identification of performance and security risks.

The Gigamon Deep Observability Pipeline helps organizations access traffic across their entire hybrid cloud infrastructure and sends the raw packets simultaneously to all their tools. This centralized approach to accessing visibility allows organizations to efficiently monitor performance and secure their infrastructure without blind spots.

Gigamon can also use deep packet inspection to extract insightful metadata from packets accessed across an infrastructure. Teams can access this valuable network and application metadata (L2-L7) to add a vital layer of intelligence to existing monitoring and security postures. Through Application Metadata Intelligence, Gigamon provides organizations visibility into the applications currently communicating in East-West traffic. This new source of intelligence combines traditional usage of metrics, events, logs, and traces (MELT) with over 7,000 applications and security-related attributes.

Cribl takes metadata extracted by Gigamon, reformats the data to match how each tool ingests data, and delivers the accessed intelligence to the specific tool. The reformatting of accessed intelligence simplifies an organization's ability to monitor and secure their infrastructure by eliminating the complexity of mapping data flows between the network to the tools themselves.

Organizations can now focus on solely monitoring and securing their infrastructure without needing to worry about visibility blind spots or the complexities that come with delivering the accessed intelligence to tools.

Challenges

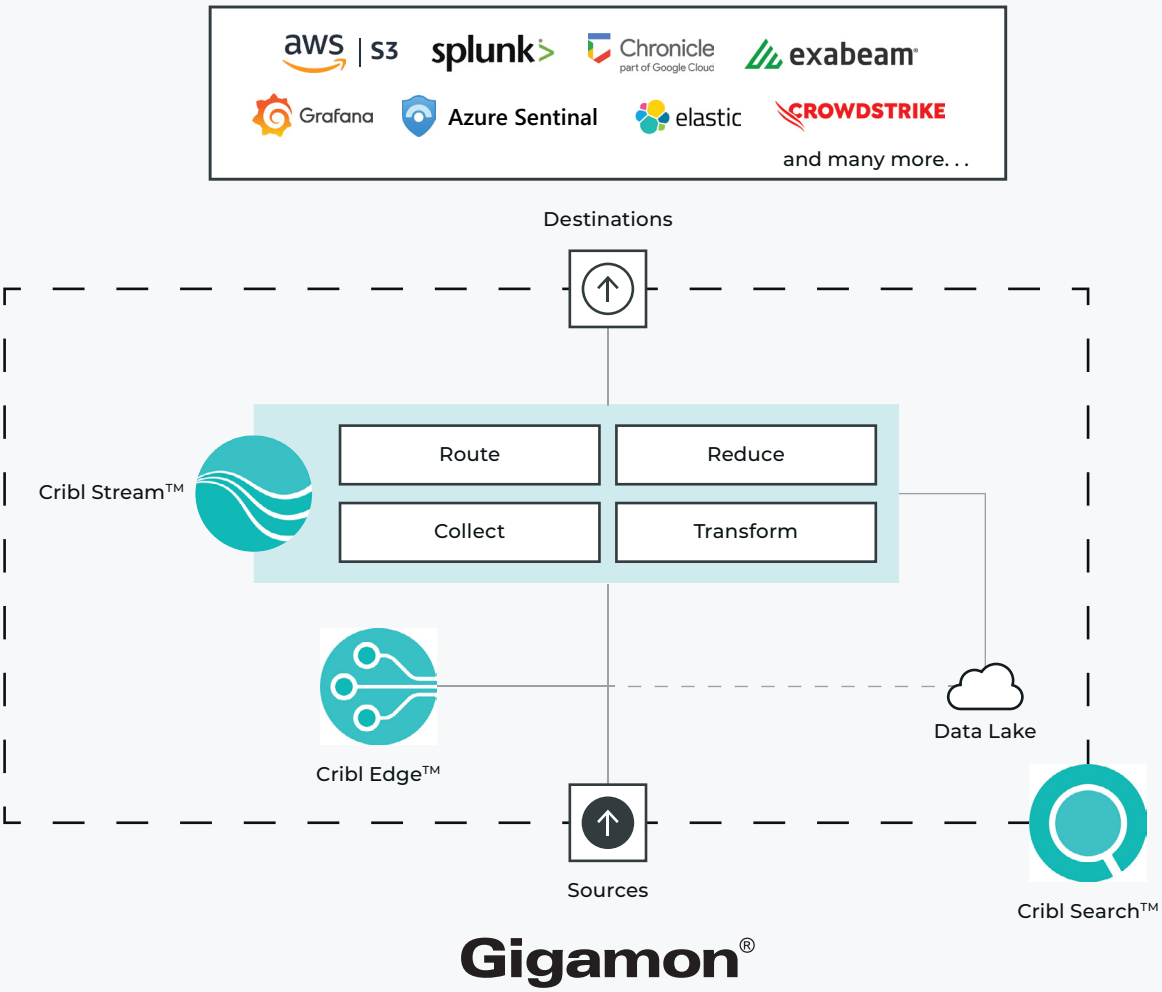
Organizations with hybrid and multi-cloud environments are becoming the norm. However, having efficient access to deep observability for the identification of risks is extremely hard to accomplish given the complexity of infrastructures and the ever-changing threat landscape. Security and monitoring postures are faced with many challenges including:

- Network visibility blind spots as infrastructures scale, raising the chance of security and monitoring risk
- Difficult and time-consuming process of accessing and delivering the intelligence necessary for tools
- Inefficient response and identification of security and monitoring risks

The Gigamon Deep Observability Pipeline gives you complete visibility across your entire hybrid cloud infrastructure, and together with Cribl, the power to efficiently access the intelligence needed.

The Solution

The Gigamon Deep Observability Pipeline provides an organization's entire security and performance tool stack with complete visibility across their entire infrastructure. In the case of Cribl, organizations can leverage their formatting capabilities to simplify the process of delivering intelligence to tools in the format they require. Altogether, organizations can focus solely on identifying potential security and performance risks rather than having to deal with the complexities of delivering the data to tools.



Key Features

- Access to 7,000+ L2–L7 application-related attributes that can be forwarded to your entire tool stack to solve security and performance use cases
- Centralized observability into all East-West and North-South traffic across on-premises, virtual, public cloud, and containers
- Simplified delivery of network-derived intelligence to tools
- Visibility of all applications running on your network
- Centralized decryption helps provide your tool stack with visibility into all encrypted data
- Metadata derived from packets provide visibility into the applications currently communicating in East-West traffic

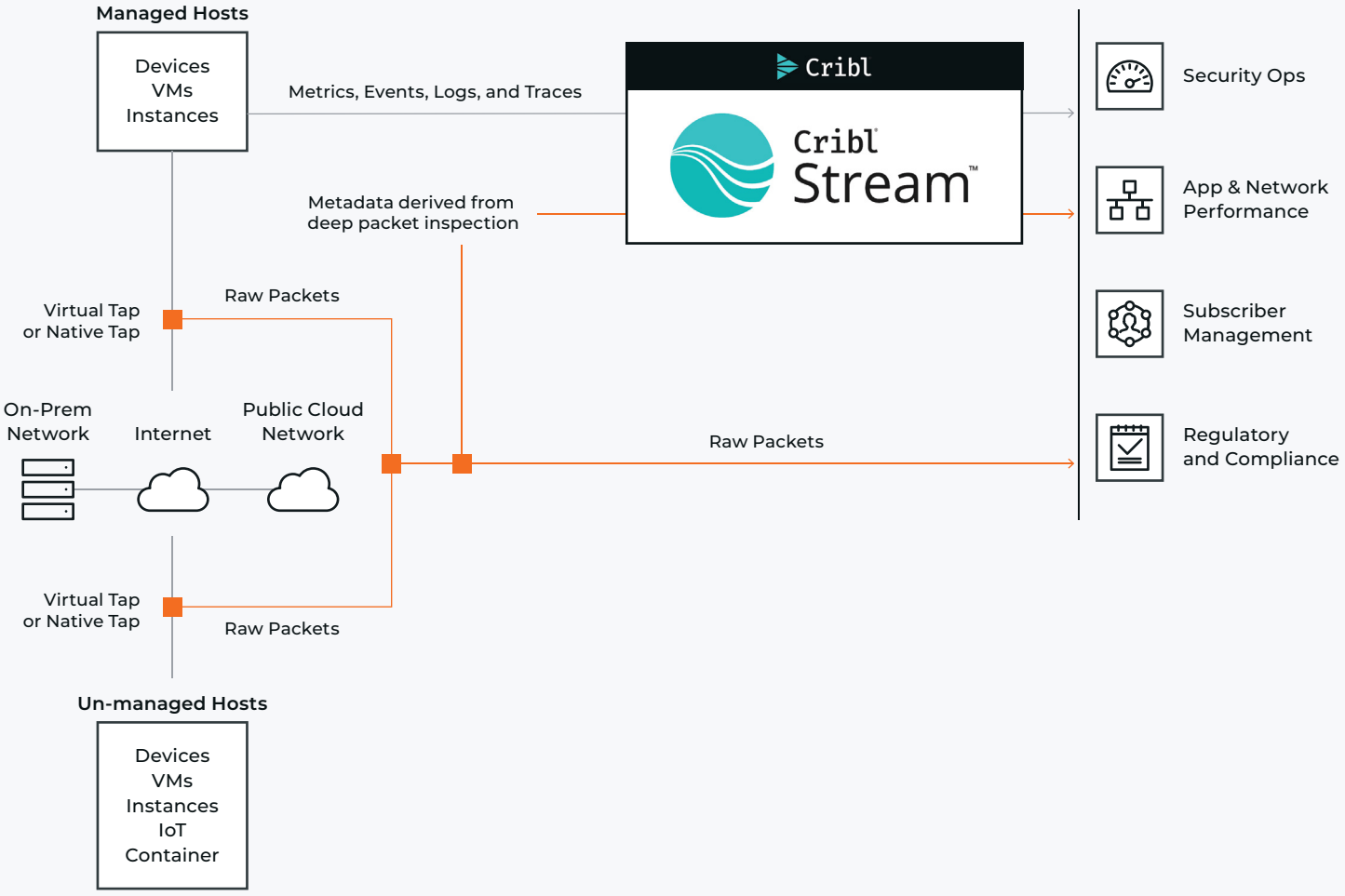


Figure 1. Gigamon accesses traffic from all sources in the form of raw packets and uses deep packet inspection to extract metadata attributes from the packets accessed. Cribl takes the metadata generated by Gigamon, consolidates this with other streams of intelligence, reformats the acquired intelligence to the format in which each tool receives it, and sends the intelligence to each specific tool individually.

Key Features

Here are just a few examples of security use cases enabled by the joint Gigamon and Cribl solution:

- **Data Routing:** Cribl Stream can route data collected from Gigamon to security, logging, and analytics platforms
- **Data Transformation:** Cribl can transform data into popular data formats such as OCSF, CIM, CEF, and ECS
- **Logs to Metrics:** High volume data sources can be converted to metrics using Cribl Stream. This optimizes the storage on many security and logging platforms
- **Data Sharing:** Security teams can now share the data collected from their Gigamon infrastructure with their operations and application teams
- **Data Masking:** Mask, redact, or encrypt data routed through Cribl Stream securing and mitigating any potential Personally Identifiable Information (PII) data leaks
- **Data Enrichment:** Add context to your data as it is routed from Gigamon through Cribl Stream and into your SIEM or analytics platforms

Summary

Gigamon plus Cribl helps you establish complete visibility across your entire infrastructure without blind spots, and simplifies the process of accessing the intelligence your tools need.

Put your organization in control, even as infrastructures become more complex and threat actors become more sophisticated.

About Cribl

Cribl makes open observability a reality, giving customers the freedom and flexibility to make choices instead of compromises. Our suite of products puts the customer back in control of their telemetry data, giving them the power to choose what is best for their organization, the control to find and get the data where they want, and the flexibility to put it in any format needed.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-derived intelligence to amplify the power of observability tools. This powerful combination helps IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the ten largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

For more information on Gigamon and Cribl please visit gigamon.com | cribl.io

Gigamon®

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

10.23_01