Mitigate Threats Faster with Gigamon and Splunk

Overview

Organizations are faced with the challenge of securing their complex infrastructures from an ever-changing threat landscape. 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 has left organizations short-handed in the battle to secure their infrastructure.

Gigamon and Splunk provide a joint solution that helps organizations gain complete observability across their entire infrastructure for efficient and effective identification of various 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 Intelligence, organizations gain visibility into the applications currently communicating in lateral, East-West traffic. This new source of intelligence creates the opportunity for teams to establish new dashboards that give them a deeper understanding of what's occurring across their infrastructure.

Splunk takes metadata extracted by Gigamon and allows users to create dashboards that help identify, detect, and respond to various security threats. The added layer of intelligence helps create security postures that can identify initial signs of anomalous traffic, detect specific security risks, and respond to threats effectively.

Teams can now focus on delivering various business needs while establishing a fortified security posture that protects their critical data.

© 2024 Gigamon. All rights reserved.

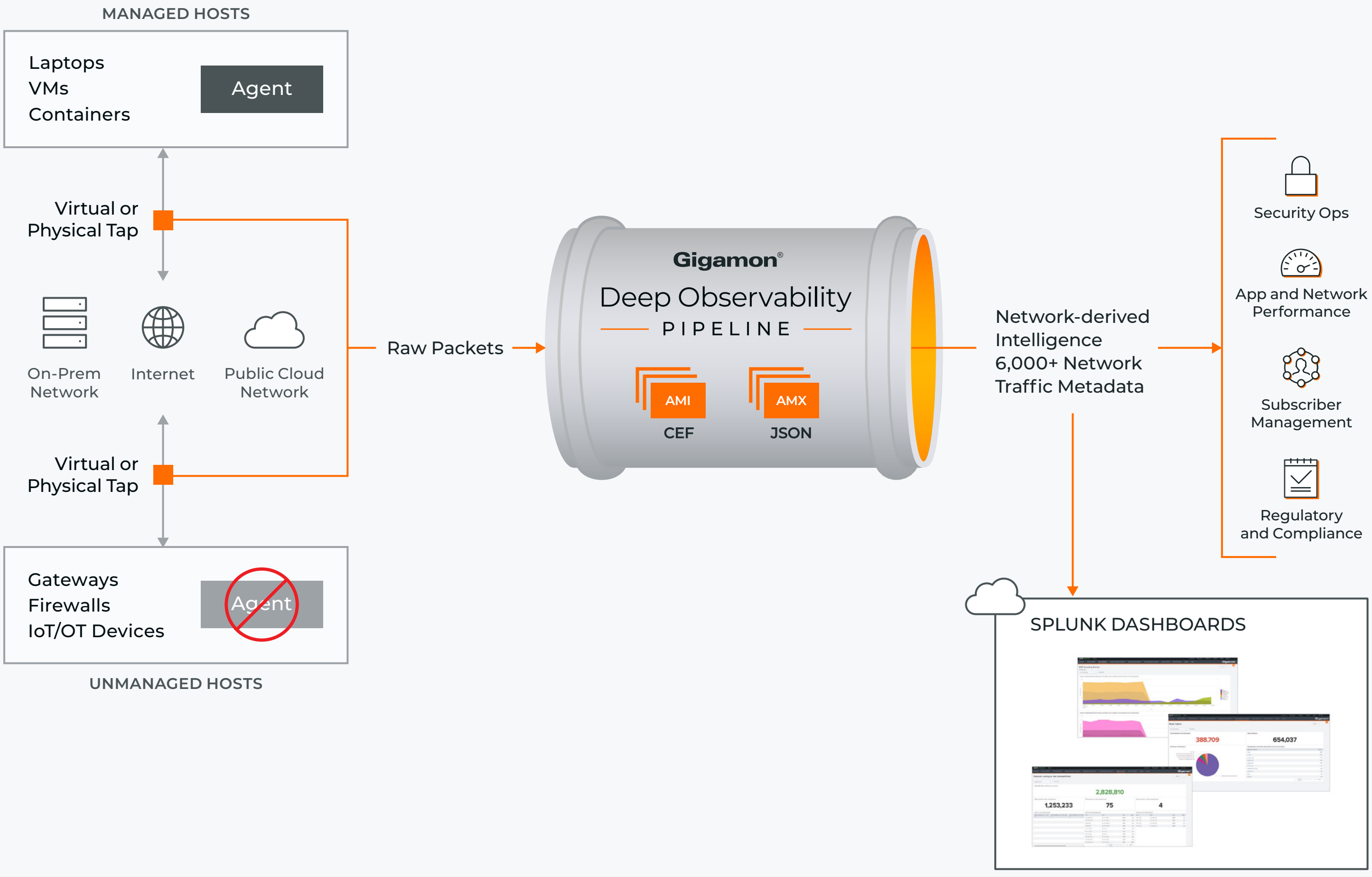
Key Features

- Extract metadata from traffic based on application-related attributes to gain a deeper contextual view into what is occurring in your infrastructure
- Centralized observability into all lateral East-West traffic across on-premises, virtual, public cloud, and container environments
- Simplified delivery of network-derived intelligence to tools
- Visibility into the applications currently communicating in your network
- Centralized decryption that helps provide your entire security posture with visibility into encrypted data
- Optimized network data fed into Splunk to control information overload

Key Benefits

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

- **Address DNS:** Monitor DNS traffic, identify rogue DNS servers, and assess external DNS server queries
- **Make logs application aware:** Combine intelligence received from logs with metadata extracted from network traffic to create dashboards that provide deeper insights
- **Pinpoint applications and protocols:** Gain an understanding of known and unknown applications and protocols currently communicating in your infrastructure, like crypto mining, non-standard port usage, FTP, SMBv1, and NTP



© 2024 Gigamon. All rights reserved.

- **Take control of decryption:** Enhance dashboards with access to decrypted traffic and identification of expired TLS/SSL certificates and any anomalous traffic
- **Secure IoT/OT devices:** Access and identify security risks in traffic going to and coming from IoT/OT devices
- **Fortify secure posture:** Strengthen your existing security posture by complementing your current usage of logs with use cases Application Intelligence can provide, like observation of lateral movement, geographic location of source and destination of traffic, vulnerable systems, and compute that can be targeted by malware

Challenges

Security teams are challenged by a myriad of different obstacles, including:

- Constantly evolving infrastructures that create network visibility blind spots
- Noisy dashboards that present teams with information overload
- An inability to effectively secure lateral East-West traffic
- New risks and methods of attack from a threat landscape that is changing by the day
- Network logs can’t identify applications
- Usage of outdated security systems due to lack of continued investment in new solutions

The Solution

The Gigamon Deep Observability Pipeline provides security postures complete visibility across the infrastructure plus an added layer of intelligence. With Splunk, organizations can use these capabilities to create dashboards that monitor for use cases that logs can’t create independently.

Altogether, organizations can gain a deeper understanding of what’s currently occurring across their infrastructure. Teams can now identify anomalous traffic before a security breach happens, detect the specific attributes to better understand the severity of a risk, and pinpoint where an issue is occurring for swift mitigation.

Supercharge Splunk Common Information Model (CIM)

Gigamon makes network log attributes application aware. This add-on facilitates the mapping of Gigamon-specific fields to the corresponding CIM data model, enhancing the overall visibility and comprehension of Gigamon-generated data within the Splunk platform. Examples of what can be mapped are:

- Certificate information including expiry date
- TLS ciphers in use
- Applications and protocols
- Standard and nonstandard port usage
- Plus much more

The Gigamon CIM data model enables organizations to achieve greater interoperability, reduce costs, improve data quality, and streamline operations, making it a crucial asset in complex and data-driven industries.

© 2024 Gigamon. All rights reserved.

Summary

Gigamon plus Splunk helps you gain a deeper understanding of what's currently occurring in your infrastructure, enabling you to establish a fortified security posture that mitigates threats faster.

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

Discover in Splunkbase

- Gigamon Deep Observability App (JSON)
- Gigamon Deep Observability App (CEF)
- Gigamon CIM

About Splunk

Splunk was founded in 2003 to solve problems in complex digital infrastructures. From the beginning, we've helped organizations explore the vast depths of their data like spelunkers in a cave (hence, "Splunk"). In 2024, Splunk was acquired by Cisco to help customers continue to build resilience across their entire digital footprint. Our purpose is to build a safer and more resilient digital world. Every day, we live this purpose by helping security, IT and DevOps teams keep their organizations securely up and running. When organizations have resilient digital systems, they can adapt, innovate, and deliver for their customers. Resilience is a team effort. Let's build it together.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived intelligence to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations. To learn more, please visit 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

© 2024 Gigamon. All rights reserved. Gigamon and Gigamon logos are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.