WHITEPAPER

The Future of Network Packet Brokers and Cybersecurity

Introduction

Next-generation network packet brokers (NGNPBs) are the foundation of a secure, distributed enterprise, strengthening cybersecurity by making SIEMs more effective, by helping NetOps and SecOps collaborate more harmoniously, by supporting advanced analytics and by enabling advanced threat hunting capabilities.

This white paper will look at all of these elements, especially the importance of network traffic analytics to the future of network packet brokers and cybersecurity. Let's take a look!

SIEMs: Going Beyond Logs

SIEMs originally focused on correlating and analyzing log data from servers and security tools such as firewalls, IPSs and anti-malware products. However, they were often handicapped by the limitations of this data, lack of correlation, lack of context and by lack of visibility into events in virtual and cloud environments. Many installations face performance issues related to the explosion in network traffic and server/tool logs.

Today, NGNPBs are helping make SIEMs more effective tools for security operations center (SOC) and incident response (IR) teams by:

- Feeding network metadata to SIEMs that they can correlate with log data in order to develop deeper insights into threat behaviors based on context
- Providing pervasive visibility so SIEMs have access to encrypted traffic and traffic from throughout the enterprise, including virtual and public cloud environments
- Filtering and de-duplicating network traffic so SIEMs are not overwhelmed by data they can't use
- Masking sensitive information so SOC and IR team members do not violate privacy and security regulations

NGNPBs can also enrich the metadata being sent to SIEMs. The capabilities of a NGNPB include NetFlow, a network protocol used to collect statistics on IP traffic information, such as IP source, destination of traffic, class of service and causes of congestion. NetFlow provides insight into traffic types and usage patterns across systems, enabling enterprises to catch denial of service attacks, data extraction and other events that represent a security risk.

For example, NGNPBs can append HTTP and HTTPS return codes and DNS query and response information to NetFlow and IPFIX records. This contextual information helps analysts spot problems such as potential command and control communications with external websites and rogue DNS services on the network.

The value of metadata cannot be overlooked, as it provides summarized information about raw network packets based on Layer-4 and Layer-7 information. With it, organizations gain insight into:

- Critical details about the flow – for example, 5-tuple, protocol information
- Application-level insights based on Layer-7 traffic information
- Traffic flows across on-premises and public cloud infrastructures

Moreover, by offloading metadata generation to an NGPNB, enterprises can:

- Save time and money by not sending raw data to analytics tools
- Reduce false positives by separating signals from noise
- Accelerate threat detection through proactive, real-time traffic monitoring versus reactive forensics
- Reduce high CPU utilization issues in routers and switches

Harmonizing NetOps and SecOps

Network operations (NetOps) and security operations (SecOps) teams share the goal of providing secure, fast, reliable networks. However, they often have conflicting priorities: optimizing network and application performance as well as productivity on the one hand, and maximizing security on the other.

Historical factors and institutional rivalries often result in the two groups using different tool sets to perform the same tasks. Not only does this lead to duplication and extra costs, it often results in the groups having conflicting views on what is happening and what can be done to solve problems

An NGNPB can help harmonize the interests and activities of NetOps and SecOps groups by:

- Giving both NetOps and SecOps a complete view of network traffic from a single source, with data that can be used for network monitoring and optimization and for threat detection and incident response, eliminating SPAN port contention
- Speeding up deployment/tool evaluation cycles and also being able to easily switch tools between monitoring and inline modes
- Allowing NetOps and SecOps to set policies in their own realms without affecting the other; for example, letting NetOps manage the flow of data to network and application performance monitoring tools, while SecOps manages data going to firewalls, IPSs, SIEMs and security analytics tools
- Filtering traffic to security devices and offloading tasks such as description and metadata generation, so NetOps teams don't have to worry about security tools slowing down network performance when traffic spikes
- Protecting network performance by avoiding planned and unplanned outages caused by security tools

Advanced Analytics

With an NGNPB, companies benefit from rapid deployment and flexibility, because there is no need to define schemas or clean up or summarize information before storing data, creating accessibility of data to a wide variety of analytics, data mining, data visualization and modeling tools, including those that utilize artificial intelligence, machine learning, and pattern recognition technologies.

Moreover, companies benefit from fidelity and data provenance, because original versions of the data are always retained and linked to transformed versions, so analysts can analyze the original data in new ways and auditors can use it to demonstrate compliance. Lastly, NGNPBs centralize data across tool stacks, creating efficiency and better effectiveness for threat hunting. Let's look at that next.

Empowering Threat Hunters

Most IT security activities are either preventive or reactive. They aim to block threats at the network perimeter or respond to "incidents" after they are detected, such as breach remediation.

Recently enterprises have added a third type of security activity: threat hunting. Threat hunters study the modus operandi or "tradecraft" of threat actors, including their tools, techniques and procedures (TTPs). They use this knowledge to search for clues that attackers have been active on the network, using techniques that do not depend on having known signatures or indicators of compromise (IOCs). This allows threat hunters to find ongoing sophisticated hard-to-detect attacks, such as advanced persistent threats (APTs) or slow and low attacks that use previously unknown methods or that have managed to evade existing controls.

Many threat hunting methods involve analyzing network metadata to find evidence of command and control communication into and out of the network and "lateral movement" within the network.

The types of attacker activities and tools that threat hunters look for include in-memory malware, persistence techniques such as storing shellcode within registry keys, the use of common administrative tools such as Windows Management Instrumentation (WMI) and Windows Sysinternals PsExec to perform reconnaissance and malicious tasks on the network, and using tools such as Kerberos to steal user credentials ("Kerberoasting").

An NGNPB is an excellent source for the types of network data and metadata that threat hunters use to answer questions including:

- Is anyone using protocols that enable remote authentication, such as SSH, SMB or RDP?
- Do any persistent objects have a history of initiating network connections to remote sites?
- What is the distribution of certificate authorities (CAs) associated with persistent objects, and do any of those CAs have weak or poor reputations?
- What remote sites have a history of failed login attempts?

The bottom line is that NGNPBs enable organizations to stop managing tools and start securing their environment, by consolidating intrusion detection, forensics and incident response in a single SaaS-based platform that rapidly scales with your business. That's the future of next-generation network packet brokers and cybersecurity.

How Gigamon Can Help

Gigamon Insight gives you the network traffic visibility from the market-leading Gigamon platform combined with the next-generation approach of network traffic analytics for the detection and triage of threats, enabling enterprises to reduce risk and keep pace with the rapidly evolving threat landscape.

Gigamon Insight gives you the power to investigate, hunt, detect and respond to threats — all with one SaaS-based security solution. With the Gigamon Insight solution, security teams can:

- Investigate, hunt, detect and respond to active security threats
- Access core security capabilities, including NetFlow analysis, network intrusion detection and network packet capture through one easy-to-use dashboard or the fully documented API
- Solve advanced business-level risk and vulnerability problems in real time
- Quickly identify and act with confidence on threats of the highest severity

Empowered Security Teams

The Gigamon Insight solution, utilizing sensors deployed in cloud, physical or virtual infrastructures, provides the opportunity to consolidate capabilities and approach security in a new way. The Insight sensors generate network metadata from on-premises or cloud-based environments and process it in the Gigamon Insight solution. The result: enriched multi-tenant data that's centralized for rapid analysis and intelligent detections.

Detect

Gigamon Detect is an Insight application that SOC teams use to quickly identify and act with confidence on threats of the highest severity. The application features an entity-driven architecture with cross-lookup capabilities that provides the critical information responders need to act, including:

- Quick identification of malicious activities
- Whether an entity has previously generated an alert
- Context into traffic type
- Recommendations on next steps

Investigate

Gigamon Investigate is an Insight application that SOC teams use to investigate security incidents in their environment. It features data correlation and enrichment, and real-time search performance to help quickly understand the chain of events leading to an incident — significantly narrowing the window between identifying and remediating an event.

- Quickly identify indicators of interest with the Entity Pane
- Fully enriched, normalized, and searchable event data
- Operationalized threat intelligence matching
- Applied Threat Research Team

Applied Threat Research

Moreover, Gigamon Insight is supported by the world-class Gigamon Applied Threat Research (ATR), which delivers leading-edge detection capabilities via the Gigamon Detect application.

ATR actively hunts for threats and studies their behavior in the wild and throughout customer environments. They also develop detection capabilities and conduct security research to advance the state of detection with curated rule sets — complete with full rule descriptions, justifications and logic — to help protect customer environments.

WITH GIGAMON INSIGHT, COMPANIES BENEFIT

Data Access

Gigamon Insight exposes all information, both raw and enriched data, through a responsive web interface and our full suite of REST APIs. Events are enriched with curated external data sources and correlated threat intelligence to generate unique insights and more data points to find threats.

Real-Time Curated Detections

Review only the most relevant alerts with fewer false positives. Curated threat intelligence and signatures across a broad data set provides targeted insights. This intel means less time with low-quality detections and more time investigating real threats.

Scalable Sensors

Rapid deployment lets you scale up and down as needs shift. The easy-to-install, fully managed sensors can be deployed in minutes across a variety of environments.

The Ability to Build, Add, Integrate, Customize

Fully documented APIs allow workflow integration to optimize visibility and easily connect to existing security tools without increasing workloads.

Summary

With a rapidly evolving threat landscape, organizations can no longer afford to rely on a set of disparate security tools which produce siloed views of the same data. The duplication of functions such as data acquisition, analysis and alerts lead to inefficiencies in the security stack and higher operational costs, and only aggravates the gap between NetOps and SecOps. Security teams, already suffering from chronic resource constraints and threat fatigue, must complete significant correlation after an event to produce actionable output and understand which events to investigate and which to ignore.

With network traffic analytics combined with the visibility of a next-generation network packet broker, companies are able to use network traffic data as the voice of truth in threat hunting, detection and investigation.

Next Steps

- Learn more from Gartner analysts Sanjit Ganguli and Lawrence Orans in their note: Align NetOps and SecOps Tool Objectives with Shared Use Cases.
- Download the Gigamon Insight solution brief
- Visit the Gigamon website to learn more about the power of network traffic analytics in Gigamon Insight
- Find out why Gigamon is the best choice: Speak to a Gigamon expert, ask for a demonstration or sign up for a free trial today!

About Gigamon

Gigamon is the company leading the convergence of network and security operations to help organizations reduce complexity and increase efficiency of their security stack. The company's GigaSECURE® Security Delivery Platform is a next-generation network packet broker that helps customers make threats more visible across cloud, hybrid and on-premises environments, deploy resources faster and maximize the performance of their security tools. Global 2000 companies and government agencies rely on Gigamon solutions to help stop tool sprawl and save costs. Learn how you can make your infrastructure more resilient, more agile and more secure at www.gigamon.com, on our blog and Twitter, LinkedIn and Facebook.

Gigamon®

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