Packet-Based Security Forensics

A Next-Generation Approach to Attack Remediation

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Viavi Solutions

November 2016

EMA™
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Packet-Based Security Forensics: A Next-Generation Approach to Attack Remediation

Executive Summary

Growing in number and becoming increasingly more malicious, security threats and attacks pose a severe threat to the survival of a business. Security operations teams need to leverage every available tool to respond more quickly and effectively to these incidents. While network packet capture and forensic analysis has traditionally been used by network operations, such a tool can also help security teams augment existing defenses and get on top of these threats. Given the hostile IT security environment, close collaboration between these groups is crucial to overall IT organizational success.

This white paper explains the importance of packet capture and forensic analysis to security operations, examines the dynamics of this growing collaboration between security and network teams, and explores a leading platform in this market from Viavi Solutions.

Security Operations Needs to Leverage Insight Into the Packet

Security is a major business challenge that every IT organization must address, and the scope of security threats continues to expand. Today external threats are a given, and insider threats are a growing concern as well, one that is underreported. In the face of all this, security teams are typically understaffed and often overwhelmed.

Security is a major business challenge that every IT organization must address, and the scope of security threats continues to expand.

Meanwhile, the stakes are only getting higher. IBM's 2016 Cost of Data Breach Study found that in the United States, the average total organizational cost of a data breach grew from $6.53 million to $7.01 million over the last year. These breaches can lead to lost revenue, a tarnished brand image, and customer churn. Malicious attacks can pilfer valuable intellectual property. Liability for lost customer data is potentially immense and governmental and organizational regulatory requirements are formidable.

When a breach occurs, an IT organization must be prepared to deliver quick answers to these five critical questions:

- What was compromised, and what data was exposed?
- Who was responsible for the vulnerability?
- Who was responsible for the attack itself?
- Has the breach been resolved?
- Can the resolution be validated?

Security operations teams have a multifaceted set of tools to address these problems and answer some of these questions. These tools include firewalls, intrusion prevention systems (IPS), security incident and event management (SIEM) systems, data loss prevention (DLP) systems, and many others. And while these solutions can detect or prevent breaches, they won't necessarily help IT understand the full nature of an attack and the extent to which it was successful in compromising an organization's IT assets and sensitive data. And they can't always validate that the breach has been resolved and the data secured.

Fortunately, network groups can close these gaps and aid the security team in their efforts through packet-based monitoring tools that capture, store, and analyze vast amounts of network traffic. IT can use packets to reconstruct network conversations. These network conversations can provide the most complete picture of what exactly happened when the security breach occurred, or they can provide evidence that an attack was unsuccessful.

After a security team is alerted to a breach or attack by frontline security systems like firewalls or SIEM, IPS, or DLP systems, security engineers can use a packet-based analytical tool to isolate the event. Packet analysis can recreate the relevant network sessions involved in the attack, identify the nature of the breach, track its lateral path through the network, and reveal what was compromised (and by inference, what data or assets were protected).

Enterprise Management Associates (EMA) research found that many security teams are relying on packet analysis for security investigations. Fifty-one percent (51%) of enterprises use packet data in security incident investigations today, and another 30% would like to do so. Thirty-five percent (35%) of organizations use deep packet inspection for security analytics and reporting. The most popular type of network traffic data that IT organizations store for security investigations is full packet captures (54% of all enterprises). Furthermore, most enterprises (58%) maintain a historical baseline of network traffic data for performing behavioral anomaly detection, and another 35% consider network traffic baselining important even though they are unable to do it at this time.[1]

There are numerous scenarios in which packet-based analysis can bolster security operations. For example, a packet monitoring tool can often identify the anomalous network behavior associated with a malware attack, such as a situation in which a Russian IP address starts sending a large volume of HTTP requests directly to a database server.

Once this attack is detected, security operations can use packet captures to recreate network sessions related to the attack. This packet-based analysis can reveal:

- Where the attack came from
- Which users (if any) were involved
- Which internal assets communicated with the malicious activity
- What data was accessed in the attack
- Whether (and how) the attack spread laterally through the network

Some distributed denial-of-service (DDoS) attacks are actually smokescreens meant to overwhelm security systems so an attack can sneak through or distract security operations from a more targeted attack. Here, too, packet-based monitoring can help.

First, packet-based monitoring can detect the performance problems indicative of a DDoS attack and determine whether existing security tools are able to cope with the attack. Analysis can help security operations understand if a flood of traffic is in fact a DDoS attack. Next, analysis of packet headers and payloads can reveal if the attack is related to any other activity on the network. If the DDoS attack is a distraction, security operations can scan the network for the associated attack, while forensic packet analysis can reveal what else happened during the DDoS attack and determine whether a breach occurred.

Packet-based monitoring can detect the performance problems indicative of a DDoS attack and determine if the attack is related to any other activity on the network.

[1] EMA, "Achieving High-Fidelity Security," February 2016.

Packet Visibility for Security and Network Operations

Packet-based network monitoring tools are typically used by network operations teams for performance management and troubleshooting of applications and services. But their usefulness in security analysis and response workflows points to an opportunity for increased collaboration between network operations and security. Viavi's "State of the Network 2016" study reveals this cross-functional partnership with 85% of enterprise network infrastructure teams assisting in security investigations.

EMA research has further revealed that the barriers between IT operations and security operations have started to dissolve. Twenty-six percent (26%) of enterprises manage IT operations and security operations within the same group and with tightly aligned processes and workflows. Another 52% of enterprises manage IT operations and security operations separately but maintain tightly aligned processes and workflows.[2]

Many network operations teams are aware of the value their packet monitoring tools can offer to their security counterparts, and they are responding to the mandate for packet visibility in security operations. For instance, when EMA asked network managers to identify their integration requirements for network management tools, 47% indicated that integration with security monitoring tools was a priority. Of the network managers who said they provided custom views of their network management tools to external constituencies, 58% said they provided visibility directly to the security team. Furthermore, the networking initiative that was shown to most affect decision-making around network management was network security (47% of all network infrastructure teams). Network management teams are clearly supporting security operations, and packet-based monitoring tools are key enablers of that assistance.

Packet-Based Tools Strengthen Security Operations

Viavi Solutions offers an integrated packet capture and analysis platform with its Observer® GigaStor™ and Analyzer solutions. While network operations teams value this solution for network and application monitoring and troubleshooting, it is also highly applicable to security operations. In a recent TechValidate survey, 41% of Observer Platform customers used captured packets for resolving security issues.

GigaStor is a high-fidelity network recorder that can capture, write to disk, and analyze traffic without packet loss. This packet capture fidelity is critical to forensic security analysis, where dropped packets can cause gaps in visibility that will undermine a security investigation.

GigaStor is also a highly scalable platform with a storage capacity of more than a petabyte. While stored within GigaStor, sensitive data is fully protected with AES-256 encryption. This encryption will not impact GigaStor's read or write performance.

GigaStor's "back-in-time" functionality allows security operations to conduct forensic analysis of incidents and view events in their full context. This capability helps security teams narrow the window of analysis by identifying where and when the threat occurred in the packet capture. Additionally, Viavi supports packet pre-processing to counter techniques that attackers use for hiding malicious activity. Users can also apply advanced filtering to detect zero-day attacks.

Viavi Solutions offers an integrated packet capture and analysis platform with its Observer® GigaStor™ and Analyzer solutions. GigaStor is a high-fidelity network recorder that can capture, write to disk, and analyze traffic without packet loss. This packet capture fidelity is critical to forensic security analysis, where dropped packets can cause gaps in visibility that will undermine a security investigation.

[2] EMA, "Achieving High-Fidelity Security," February 2016.

Analyzer, the packet analysis tool integrated with GigaStor, has access to the network recorder's packet captures. It can analyze these packets for behavioral anomalies and review network ingress and egress activity to rebuild network sessions, allowing security operations teams to see what was done—where, when, and by whom. Analyzer can reconstruct HTTP sessions to see what malicious actors requested and received from data repositories and other assets. It can also apply any available private keys to encrypted traffic, giving it visibility into traffic flows that many security tools are unable to scan.

Viavi recently added new capabilities to its Observer Platform that are aimed at enabling collaboration between security and network operations. First, it introduced a web-based GigaStor console that allows users to mine packets from any browser and share packets with third-party monitoring and analysis tools. As it allows security operations to access and extract GigaStor packet captures, this console is useful even if the network team is the primary operator of the device.

Viavi also recently integrated its solution with Cisco FirePOWER IPS, a leading intrusion prevention solution. From within FirePOWER's management console, users can access GigaStor's long-term packet capture and analysis. From within the context of a snapshot view of a security event in the FirePOWER console, users can even replay network events that were reconstructed from packet captures in GigaStor.

EMA Perspective

EMA research found that security operations teams have recognized the value of network packets for analyzing and responding to security events. This research also found that network operations and security operations are collaborating to mitigate security threats—and this is becoming more and more critical to business survival. Network packets are essential to this collaboration. They help response teams trace, replay, and mitigate breaches.

Network operations and security operations are collaborating to mitigate security threats—and this is becoming more and more critical to business survival.

Packet-based network monitoring solutions, which evolved from performance monitoring and troubleshooting tools for network operations, are ideal for forensic analysis of security incidents. As a result, both network operations and security operations are finding value in sharing access to these tools. With GigaStor and Analyzer, Viavi Solutions offers an integrated network recorder and packet-based monitoring solution that answers the call.

About Viavi Solutions

Viavi (NASDAQ: VIAV) is a global provider of network test, monitoring, and assurance solutions to communications service providers, enterprises, and their ecosystems, supported by a worldwide channel community including Viavi Velocity Solution Partners. We deliver end-to-end visibility across physical, virtual, and hybrid networks, enabling customers to optimize connectivity, quality of experience, and profitability. Viavi is also a leader in high-performance thin film optical coatings, providing light management solutions to anti-counterfeiting, consumer electronics, automotive, defense, and instrumentation markets. Learn more about Viavi at www.viavisolutions.com. Follow us on Viavi Perspectives, LinkedIn, Twitter, YouTube, and Facebook.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3474.110916