VIAVI Solutions

White Paper

Network Performance Management for Security Intelligence

Critical for Detection and Remediation of IT Threats

Escalating Threats and Damage

Nearly half of security leaders at global enterprises reported experiencing a security breach costing more than $500,000 USD in 2018, according to the Fifth Cisco CISO Benchmark Study 2019[1]. Not only do breaches impact the bottom line, but companies also suffer long-term damage from customer churn, tarnished reputation, and potential compliance penalties. So, what can be done?

Looking at the latest attacks, even the best organizations with the most sophisticated IT security and threat counter-measures are still being breached and important assets compromised. It's time to consider another layer that combines insights from across the network for active threat hunting and quick incident response.

The answer lies in acknowledging that the network is the foundation and lynchpin for all things IT. Why? Because every service, infrastructure connection, user action, device communication, and transaction are delivered by the network—whether legitimate or not. This includes malware, intrusion/extrusion events, or any other illicit actions.

Calculating the Business Value of Threat Hunting and Remediation

Making the business case for investing in threat hunting and remediation strategies, requires identifying the costs and risks in protecting critical resources and services. In a nutshell, it's calculating the costs for compromised data, risk of attacks occurring undetected, and understanding the likelihood of attacks.

- **Average cost of resolving a data breach for companies globally:** $3.86 million (U.S. dollars)
- **Average cost of resolving a data breach for U.S. companies:** $7.91 million (U.S. dollars)
- **Mean Time to Identify a breach occurred:** 196 days
- **Mean Time to Contain breach:** 69 days
- **Likelihood an enterprise experiences significant breach in next 2 years:** 28%

Source: Ponemon Institute's 2018 Cost of a Data Breach 2018 study
https://www.ibm.com/downloads/cas/861MNWN2

---

[1] Cisco Newsroom. (2019, February 28). Caution Security Startups, Investors, and Standalone Solutions—Cisco 2019 CISO Benchmark Study Reports Increased Vendor Consolidation

Can a solution that monitors the network potentially add insight here? Network Performance Monitoring (NPM) solutions are at the center of managing all IT activities and provide network perspective insight to strengthen security while ensuring end-user experience, optimizing application delivery, and helping IT achieve operational excellence.

As network environments become virtualized and extend beyond the realm of the traditional data center, comprehensive network performance monitoring solutions provide security and performance insight into cloud, virtual and software-defined networks. NPM solutions provide visibility from the perspective of the hybrid network environment and any virtualized device like a load balancer, firewall, or switch hosted on the network. SD-WAN presents unique monitoring challenges. Be sure the NPM solution can visualize and manage traffic paths and end-to-end service performance.

NPM for Robust IT Security

Depending on the vendor, NPM solutions achieve broad awareness into IT service health—and the underlying network —via a combination of three potential data sources. Additionally, the right NPM data with supporting analytics can provide sweeping insight into traffic patterns, usage, utilization, and information down to individual transaction details. NPM solutions that use multiple forms of network data and provide in-depth correlated insight deliver value by profiling network and application characteristics, identifying aberrant activities, hunting unknown threats, and conducting post-incident investigations.

NPM Security Use Cases

Before discussing NPM data sources in detail, it's best to first outline the use cases in the context of the three primary components of IT security:

Prevention

Detection

Remediation

Threat Hunting and Remediation Saves Millions

Companies that identified a breach in less than 100 days saved more than $1 million as compared to those that took more than 100 days. Similarly, companies that contained a breach in less than 30 days saved over $1 million as compared to those that took more than 30 days to resolve.

2018 Cost of a Data Breach Study
IBM Security and Ponemon Institute

NPM security use cases fall primarily within the Detection and Remediation:

Security Component	Use Case	Goals
Detection Threat hunting and ongoing auditing of usage and utilization against "normal" or "typical" activity	Threat Assessment (black/white listing, devices lacking end-point agents)	Useful for finding unknown rogue devices and reviewing suspicious network conversations. Question answered: Are their illicit actions occurring on the network that have not been detected by existing security measures?
	Traffic Profiling (audit, insider extrusions)	
Remediation ID of and investigations into known or suspected security breaches	Rogue User/Host/ Device Identification	Aid NetOps and SecOps teams in post-event forensic clean-up and compliance with regulatory reporting requirements when security breaches have been confirmed. Questions answered: What assets, hosts, and customer data have been compromised? How did the breach succeed? Is the problem completely resolved?
	Forensic Investigations (malefactor tracking)	

Types of NPM Data

It's important to understand NPM can utilize three broad types of data sources for security and performance monitoring and analysis: wire data (packets and flow), infrastructure (SNMP and Syslogs), and synthetic tests.

NPM Data Sources		
Type	***Useful for Security?***	***Value for Detection and Remediation***
Wire (packet, flow)	Yes	Views into network conversation details: usage, volume and utilization
Infrastructure (e.g. SNMP, syslog)	Yes	Quantify how the traffic traverses through the network
Synthetic (active test)	No	–

At a high-level, for detection and remediation, IT teams should use network traffic in the form of packets to understand what was transmitted across the network. Additionally, it's best to leverage flow and infrastructure data to answer how communications and applications passed through the network, and what devices they interacted with in the process. Though valuable for assessing performance health and assessing the impact of network paths on end-user experience, synthetic testing does not play a significant role in NPM detection and remediation security efforts.

NPM Data for Security

Wire and infrastructure data sources present different visibility into security and performance at the network core and perimeter as well as in the cloud. Conversation-level wire data provides specific details into individual transactions. Depending on the version, traditional flow data such as NetFlow and IPFIX provide numerous volumetric, usage, and utilization summaries as well source/destination IP address and ports among other parameters. Depending on how the environment has been configured, most IT teams will have the following infrastructure data to gain security and performance insight across their hybrid IT network.

Infrastructure	**Host Location**		
	Corporate/Large Site	***Remote Branch***	***Cloud***
Switch/Router	■	■	
Wireless Access	■	■	
Packet Brokers	■		
User Device	■	■	
LDAP/IP Address Management	■	■	
Domain and authentication servers	■	■	■
Proxy servers	■		
Firewall/VPN concentrators/ load balancers	■	■	■
Cloud	■	■	■

Depending on the component, infrastructure typically acts as a gate keeper providing entrance to and through the network. If an asset serves this role, IT teams can use the device's logs to determine if and how a particular network conversation was handled; for example whether a firewall blocked it or by what link a load balancer propagated the connection. Given this, such information complements wire data very well while enhancing overall visibility granularity. In addition, it acts as the glue that ties host/user level details including access device type, actions, usage timing, and physical location to network activity captured with wire data.

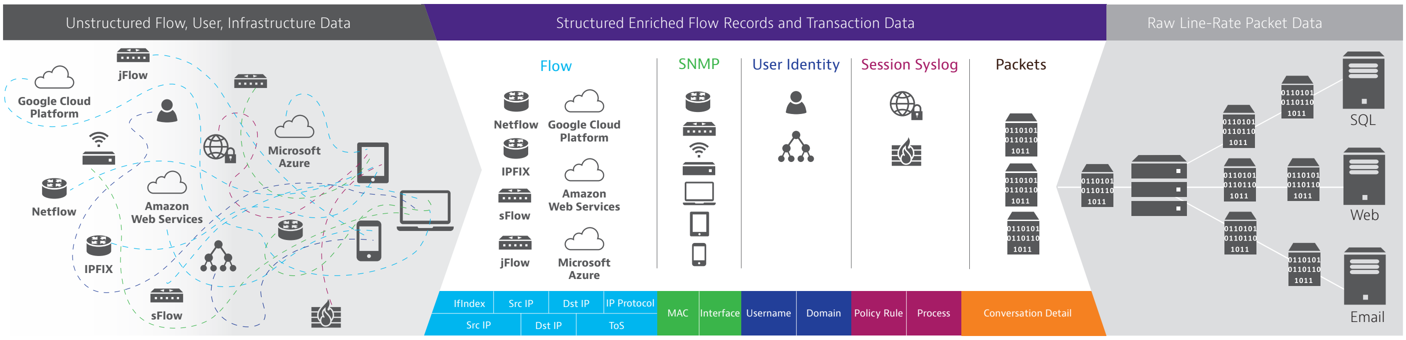
Be aware, the complexity of today's hybrid IT environment including cloud hosting, IoT, SD-WAN, and the proliferation of multiple user device access methods make this data collection difficult. Therefore, it's important to ensure the specific NPM solution being considered is up to the challenge and can capture the proliferating number of data sources. This is especially important as few if any security offerings on the market have comprehensive access to this wealth of rich information.

Bridging NetOps and SecOps Siloes with NPM Data

It's worth noting that NPM solutions can also serve as a direct source of information to your existing IT security assets such as SIEMS, IDS/IPS, or end-point protection. Many of these do not have access to network level conversation details or infrastructure intelligence. Look for formal technology partnerships or easy methods to third-party integrations between the NPM product and your IT security resources.

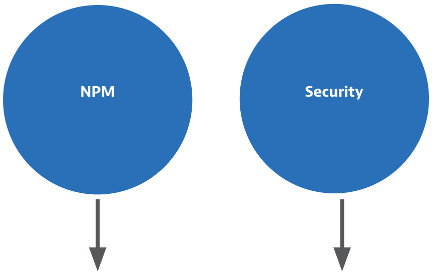
Bringing it all Together

There remains one final step for total network awareness. These sources of data must be combined, correlated, and then analyzed in real-time into a single indexed record to be useful for detection and remediation. Then they must be stored without aggregation or deduplication for extended periods in a relational database for fast and simple forensic access and searchability. Providing a means to enrich and extend the source data with user-defined fields is also valuable. For example, the tagging of IP addresses with known attributes like device type, physical location, or routing interface simplifies detecting anomalous behavior.

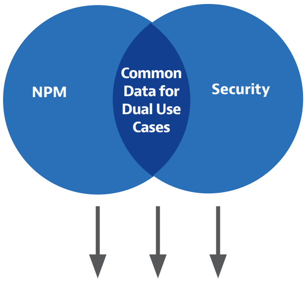


Example fields shown; actual GigaFlow record can contain dozens of unique fields

NPM and IT Security – A Perfect Combination



The best NPM solutions can serve dual roles. The first is monitoring and managing IT for improved end-user experience and optimization of IT resources.



Second, utilizing the same data to bolster existing detection and remediation security assets. Doing so offers organizations a cost-effective method to maximize NPM solutions' ROI while also operationally streamlining internal processes for fast service troubleshooting and rapid security threat containment.

Given the wide range of data sources and in-depth network awareness provided by some NPM offerings, the right solution can become the go-to platform to definitively confirm if a breach has occurred and whether it has been eliminated from the environment. In these days of never-ending security threats, escalating attacks, and growing data protection regulatory requirements NPM solutions can provide NetOps and SecOps teams with ultimate peace-of-mind.

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

© 2019 VIAVI Solutions Inc.
Product specifications and descriptions in this document are subject to change without notice.
npmdnetworkforensics-wp-ec-ae
30179963 901 0719