Prepared for

LiveAction

ML-Driven Deep Packet Dynamics can Solve Encryption Visibility Challenges

November 2021 EMA White Paper
By Shamus McGillicuddy

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

Executive Summary

Encryption may provide data security and privacy, but it also reduces visibility into network traffic. Both security teams and network teams are finding that their deep packet inspection technology cannot provide enough insight into encrypted traffic. This white paper explores an emerging class of technology called deep packet dynamics, which combines metadata generation and traffic behavior with machine learning and advanced analytics to restore this lost visibility and enable improved collaboration between security and network teams.

Security Teams Need to Inspect Packets

Network packets are the ultimate source of truth about a network. Network engineering and operations teams are an IT organization's resident experts on packet data. They own the infrastructure that carries packets, and they are experts in collecting and analyzing packets.

However, Enterprise Management Associates (EMA) research recently confirmed that security teams need this data as well. A survey of IT professionals revealed that 91.8% believe it is somewhat to very important for their security teams to have access to full packet data collected from their networks. The security team's need for packet data is driven primarily by their use of network detection and response tools (69.4%), incident response processes (57.7%), real-time packet payload analysis (55.2%), and forensic packet analysis (41.5%).[1]

Network and Security Teams Need to Partner on Packet Data Access

Network teams are a key player with packets. They are more knowledgeable about how packet data relates to the business, they have more experience with accessing packet data, and they are usually the ones who configured the technology that provides access to this data, such as TAPs and network packet brokers. When a security team needs to analyze this data, they often request access from the network team. Security teams know how to identify threats in packet data, but they don't necessarily know how to get the exact data set that they need. In fact, the security team's need for network traffic data has driven increased collaboration between network and security teams in 83.1% of IT organizations.

[1] Unless otherwise noted, all research results cited in this paper were originally published by EMA in the October 2021 report, "NetSecOps: Aligning Networking and Security Teams to Ensure Digital Transformation."

Encryption is Threatening Visibility

For security and privacy reasons, much of the traffic associated with newer web browsers (Chrome, IE, etc.), SaaS applications, and public cloud applications, which all traverse the internet, is now encrypted. As enterprises have increased their adoption of these newer technologies, more of their network traffic has become encrypted. This ubiquitous encryption is challenging visibility.

In fact, 55.5% of IT organizations reported that network teams struggle to share network data with the security team due to this encryption ubiquity. The network team can easily send encrypted packets to security team's tools, but those tools often can't do much more than analyze the unencrypted part of the packet—the header that switches and routers use to forward traffic and establish sessions. A packet header is usually just 20 bytes or so of information, such as source and destination IP addresses, protocols, and other instructional data. The packet payload is protected by encryption, and the payload is where malware is hidden.

EMA asked organizations how they resolve challenges associated with this encryption. First, 20.7% of organizations decrypt the packets to get at the payload. This process is expensive, complex, and often impossible, given that decryption keys are not available in all cases. Decryption can also violate compliance policies on privacy. Thus, decryption is not very popular.

Instead, 28.1% turn to other data sources, such as NetFlow. NetFlow and other network flow records are summaries of network traffic, as seen from the perspective of the network device that generates the record. Some network flow records technologies can be enriched with metadata that can give application layer information not gleanable from packet headers, but these flow records are not granular sources of data that can enable deep analysis.

The most popular strategy for dealing with visibility lost to encryption is enriched analysis of packet data. EMA found that 48.8% take this approach. A new class of technologies is emerging that combines packet header data with other perspectives for improved network intelligence. One example is deep packet dynamics.

Deep Packet Dynamics can Solve Encryption Visibility Challenges

Encryption undermines the deep packet inspection (DPI) technologies that can reveal malware and enrich visibility in network performance management solutions. In encrypted traffic the payload may be hidden, but traffic behavior can reveal plenty.

Deep packet dynamics solutions enrich the unencrypted packet header info with analysis into behavioral baselines and anomalies. Packet headers reveal where traffic came from and where it's going. Artificial intelligence (AI), machine learning (ML), and other heuristics enable deep packet dynamics technology to baseline traffic patterns and endpoint behavior associated with traffic patterns. These solutions also generate metadata about traffic based on its overall analysis of the observable characteristics of encrypted traffic, such as byte distributions, jitter, retransmits, connection setup time, round-trip time, TCP metrics, and even inferred L7 application classification.

ML algorithms infer insights from their analysis of metadata and behavior to understand whether anomalies are phishing attacks, brute force attacks, or other issues. For example, ML can analyze the characteristics of an HTTPS session and compare it to known patterns of phishing sites as opposed to normal websites without ever decrypting the actual payload. Coupled with behavioral analytics that can characterize patterns of activity over time, these technologies provide valuable insights into encrypted traffic. Behavioral analytics examples include alerting security teams to large volumes of data exchanged between an internal database server and an IP address associated with an internal host that usually only communicates with the company's external web services, or highlighting the exchange of large volumes of UDP traffic between a real-time communications application and an internal accounting application.

Bridging the NetSecOps Gap

EMA research found that 75.4% of IT organizations experienced an increase in the amount of collaboration that occurs between network teams and security teams. We also found that 80.3% of organizations are interested in consolidating network teams and security teams onto a shared traffic monitoring and analysis tool. Given that encryption challenges visibility for both of these groups, deep packet dynamics can provide a foundation for collaboration. It can uncover fault and performance insights in addition to security insights.

An NPM tool or tool suite that includes a deep packet dynamics capability can serve both network operations and security operations, improve collaboration between the two groups, and reduce costs. It can also help them work together to enforce policies. For instance, it can detect improperly encrypted traffic and it can reveal shadow IT, such as applications and services that are avoiding normal change controls and exposing network ports to unsafe traffic.

A shared toolset that enables NetSecOps collaboration can be invaluable. EMA research found that successful collaboration between these groups led to faster resolution of security issues (57.9%), reduced security risk (51.6%), improved operational efficiency (46.4%), faster resolution of user experience and network performance issues (45.1%), and more influence over technical initiatives (42.6%).

Successful NetSecOps collaboration leads to cost savings for 33.1% of organizations and sharing tools can help an organization realize that benefit. EMA research found that 86.1% of organizations are starting to combine budgets between networking and security teams, and 45.6% of organizations are spending at least some of these pooled budgets on network monitoring and analysis tools.

EMA Perspective

Encryption is a threat to visibility, which is in turn a threat to security and end-user experience. When encryption obscures visibility into the packet payload, the DPI technologies used for performance management and security analysis are less effective.

Deep packet dynamics uses ML-driven analysis of packet header metadata and traffic behavior to mitigate lost visibility. This technology can help security regain insight into malicious traffic and help the network team regain their visibility into performance problems. A traffic analytics toolset with deep packet dynamics can serve the needs of both SecOps and NetOps as these two groups increasingly collaborate to support digital transformation.

About LiveAction

LiveAction provides end-to-end visibility for network security and performance from a single source of truth. This gives enterprises confidence that the network is securely meeting business objectives, provides full network visibility to better inform NetOps and SecOps as they drive critical decisions for performance and threat response, and reduces the overall cost of network and security operations. By unifying and simplifying the source of collection, inspection, presentation, and analysis of network traffic, LiveAction empowers network and security professionals to proactively and quickly identify, troubleshoot, and resolve issues across increasingly large and complex networks. Learn more at **https://www.liveaction.com**.

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 You can also follow EMA on Twitter or LinkedIn

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 www.enterprisemanagement.com 4139.110821