Prepared for

LiveAction®

In an Era of Ubiquitous Encryption, Security Based on Traditional Packet Analytics Won't Protect You

April 2022 EMA White Paper
By Shamus McGillicuddy, Vice President of Research

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

The Problem of Network Traffic Encryption

It is often said that packets are the best source of truth about what is happening on a network. With encryption, this axiom remains valid, but the means of revealing that truth are shifting. As encryption rises in popularity, traditional packet analytics are no longer as feasible as they once were.

Packet visibility is the foundation of countless security analytics solutions today. Packet analytics technology inspects the payload of every packet that crosses the wire, looking for signs of malicious or unauthorized network activity. When those payloads are encrypted, packet-based visibility breaks down.

Today, networks are increasingly encrypted. Businesses encrypt their traffic to protect sensitive data. The public internet is increasingly encrypted by default. Pick a website at random and it will establish a secure HTTPS connection when you visit. As a result, packet payloads are now locked, leaving security analysts who rely on multiple packet analytics tools scratching their heads.

Networks are Moving Toward 100% Encryption

In 2014, **50% of internet traffic was encrypted**, which meant that security solutions based on traditional packet analytics could read only half of traffic by default. The rest would require some kind of decryption before analysis could proceed. Things have only become more challenging for security professionals. Today, 95% of internet traffic is encrypted, and much of it is hitting the security perimeters of businesses every day.

Encryption is becoming pervasive for many reasons. Laws and regulatory frameworks like HIPAA, PCI-DSS, and GDPR require businesses and service providers to encrypt data to protect medical privacy, financial transactions, and general privacy. Consumers are becoming more concerned about privacy, too, which adds bottom-up demands for more encryption to the bottom-down requirements of regulatory frameworks.

Many technology giants (e.g., Google) have become champions of consumer privacy and advocating for 100% encryption of the internet. Total encryption is not that far away anymore. LiveAction predicts that 99.9% of all traffic will be encrypted by 2025.

Malicious Actors Hide Inside Encryption

Encryption ensures privacy and protects sensitive data, but these benefits come with a downside—lost visibility.

When the IETF developed TLS 1.3, an encryption standard that includes an ephemeral key technique, it broke the shared-key decryption model that information security teams relied on for inspecting packets. Many information security leaders lobbied the IETF to include a mechanism that would allow them to continue inspecting packet payloads. They were not successful.

Information security professionals were concerned about this lost visibility because cyber-criminals and hostile nation states increasingly use encryption to hide attacks, penetrations, exfiltration, and command and control communications. Last year, **91.5% of malware** detected by one security vendor was hidden within encrypted traffic.

Hackers disguise malicious network traffic as harmless communications. For instance, encrypted packet streams associated with the HTTPS protocol may appear on the surface to be simple web transactions, but malware can lurk within the encrypted packet payloads, invisible to signature-based packet analytics technology. For example, the hackers responsible for the Sunburst hack of SolarWinds in 2020 used HTTPS to hide command and control traffic and data exfiltration.[1] Organizations that spend millions on security solutions based on traditional packet analytics, such as the US Department of Defense, were compromised by this attack.

To conserve resources and minimize impact on user experience, some security teams are tempted to trust traffic where it makes sense to do so. This is a mistake. For instance, stolen credentials can turn an encrypted VPN tunnel into a back door. Many information security groups treat VPN connections as trusted communications, partly because packet analytics tools are already overburdened with the other sources of encrypted traffic hitting the network. They own the VPN connection, so they assume it can't be a vector of attack. This assumption can be catastrophic. Hackers perpetrated the Colonial Pipeline attack of 2021 with stolen VPN credentials. This attack shut down the largest refined oil pipeline in the United States for five days and the hackers collected $4.4 million in ransom payouts.[2]

Network security solutions that rely on packet payload analysis can find themselves blind to these kinds of attacks.

[1] Cybersecurity and Infrastructure Security Agency, "Malware Analysis Report (AR21-039A)," February 2021.
[2] Bloomberg, "Hackers Breached Colonial Pipeline Using Compromised Password," June 2021.

Encryption Degrades Traditional Network Security

Many network security solutions rely on traditional packet analysis techniques to detect malicious activity. Intrusion detection, intrusion prevention, and next-generation firewalls try to match malware signatures to packet payloads to uncover attacks. Data loss prevention solutions inspect packets for sensitive data that is being exfiltrated.

Traditional packet analysis is a resource-intensive process that requires full access to the packet, not just header information. Encryption locks down the packet and breaks visibility. Only packet headers are visible, which gives a security monitoring tool information about the source and destination of traffic and the ports and protocols that the traffic will engage. Packet analytics tools have no way to know, for instance, whether the message that is actually carried within the packet is safe unless that packet is decrypted. Today, 56% of enterprises say encryption is currently challenging the security teams' ability to analyze network traffic data.[3]

Decryption is Not a Universal Solution

Network security vendors that rely on packet payload inspection will advise customers that the problem of encryption is easy to solve. Simply decrypt traffic.

Decryption is not as easy or feasible as some security vendors suggest. First, there is an issue of privacy. Some regulatory systems forbid decryption of certain types of traffic. The very act of decrypting traffic will put a company out of compliance with important regulations.

Second, access to ciphers and keys is limited. Security teams may have decryption keys for traffic originated on their networks, but not for incoming internet traffic that was encrypted by a malicious actor. Moreover, the ephemeral keys of TLS 1.3 make decryption more complex.

Finally, decryption adds cost and complexity. Traditional packet analytics is a resource-intensive process in any circumstance, but decryption adds even more of a processing burden to security appliances. Inspection simply takes longer when decryption is involved, which slows down the detection of attacks and adds latency to communications. Also, managing key access, configuring decryption, and ensuring data is re-encrypted is complex. One mistake can lead to new vulnerabilities. It can also take time to get right. Security and networking teams will have to carefully implement and administer these decryption solutions, and these skills are in short supply today.

[3] Enterprise Management Associates, "NetSecOps: Aligning Networking and Security Teams to Ensure Digital Transformation," October, 2021.

Encrypted Traffic Analysis can Restore Lost Visibility

There is a way to see deeper into encrypted network traffic without decryption. A network detection and response (NDR) solution that uses encrypted traffic analysis (ETA) can combine what is known about encrypted traffic with behavioral analysis. Regardless of encryption, there remains plenty of information available about packets. It starts with the header information, which remains undecrypted. There are also objective metrics that can be gleaned via observation of the network, such as latency and jitter.

An NDR solution with ETA intelligence solution can observe the deep packet dynamics of traffic and generate metadata based on what is known about the encrypted traffic. This metadata can specify jitter, session resets, packet retransmits, byte distributions, round trip and connection setup times, SPLT, producer/consumer ratios and more. The NDR tool then performs streaming analysis of these deep packet dynamics using machine learning to correlate metadata, process events, and identity patterns associated with malicious activity.

This technique enables real-time analysis of encrypted data without the need for encryption and without any inspection of packet payloads. ETA solutions are capable of spotting attacks via DNS over HTTPS, command and control traffic from malicious actors, exfiltration of sensitive data from a compromised network, and frontline incidents like phishing attacks.

In this era of ubiquitous encryption, ETA is a realistic and proven solution for security visibility. Rather than add complexity and risk with decryption-dependent packet analytics tools, information security teams should accept reality. Decryption simply isn't as practical as it was when encryption was the exception, rather than the norm. Technology exists today that can mitigate the rise of encryption without violating privacy requirements and slowing down communications.

About LiveAction

LiveAction provides end-to-end visibility for network security and performance. By relying on a single source of truth (the packets), LiveAction gives modern enterprises the confidence needed to ensure the network is securely meeting business objectives, providing full network visibility to better inform NetOps and SecOps, and reducing 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 identify, troubleshoot, and resolve issues across increasingly large and complex networks proactively and quickly. To learn more about LiveAction, visit **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**

4169.040422