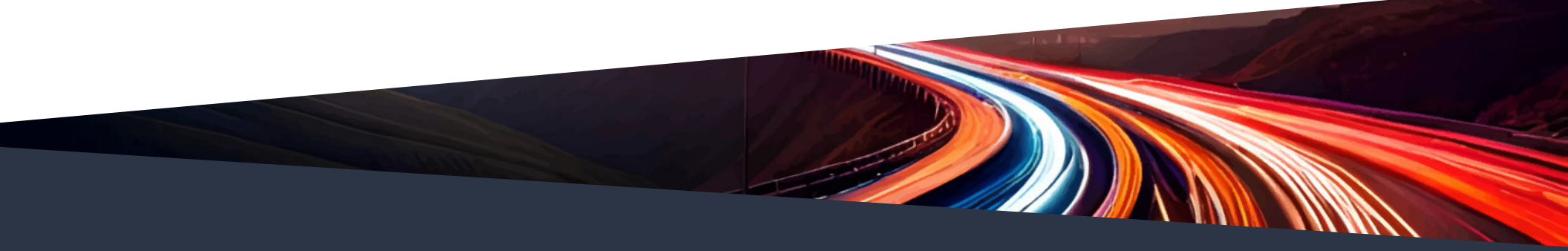


Prepared for

Gigamon®

IT Organizations in a Quandary Over Visibility into Cloud Traffic

September 2023 EMA White Paper
By **Christopher M. Steffen, CISSP, CISA**, Vice President of Research
Information Security, Risk and Compliance Management

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

Introduction

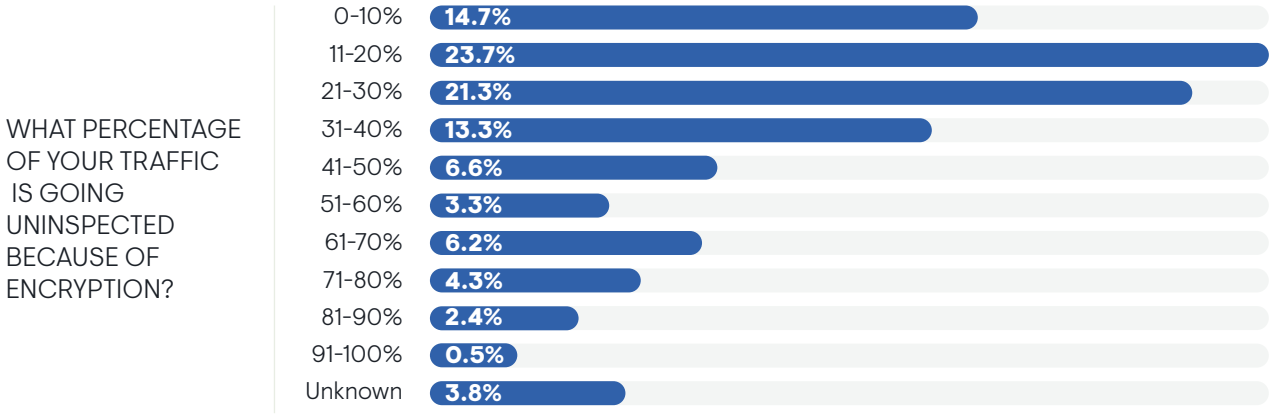
The push for the finalized IETF Transport Layer Security (TLS) 1.3 standard for network encryption started in 2018 and the major web server and browser vendors backed it with heavy promotion. Back then, the 10-year-in-the-making standard promised better privacy, but it also threatened to break how IT networking and security professionals troubleshoot networking problems and monitor the presence of malware and malicious actors operating within those networks.

Fast-forward to 2023: the adoption of TLS 1.3 encryption still presents both opportunities and complexities. While it offers heightened security and efficiency, its integration into organizational frameworks has faced considerable roadblocks, most notably the loss of network traffic visibility that rendered many security and technology teams helpless to protect their environments. Gigamon teamed with Enterprise Management Associates (EMA) to conduct a survey to investigate perceptions and beliefs of end users surrounding the adoption of the TLS 1.3 standard. The survey looked at the factors that contributed to the gradual adoption of TLS 1.3 encryption, investigating monitoring tools' compatibility, regulatory compliance challenges, and misconceptions surrounding perimeter security.

Research Findings

When examining some of the challenges network traffic encryption creates, first take a look at the amount of traffic that is going uninspected because of encryption on an organization's network.

In this survey, 14.7% of organizations had 10% or less of their network traffic left uninspected, but over 16% believe that 50% or more of their traffic was uninspected.



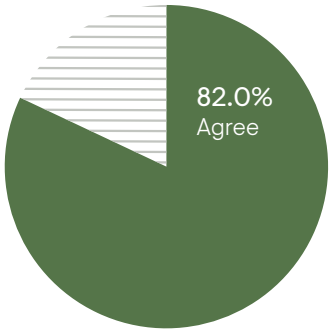
Thirty-eight percent of organizations encountered incidents involving malware concealed within encrypted traffic over the past 12-18 months. This demonstrates the emerging threat landscape and the tactics cyber adversaries employ to exploit encrypted channels.

HAS YOUR ORGANIZATION EXPERIENCED AN INCIDENT FROM MALWARE HIDDEN IN ENCRYPTED TRAFFIC IN THE PAST 12-18 MONTHS?

The prevalence of incidents involving malware concealed in encrypted traffic underscores the evolution of threat tactics. As hackers leverage encryption to obscure their malicious activities, organizations face the challenge of maintaining effective detection mechanisms. This statistic emphasizes the imperative of advanced monitoring and detection solutions capable of identifying threats within encrypted communications, ensuring the continued efficacy of cybersecurity measures.

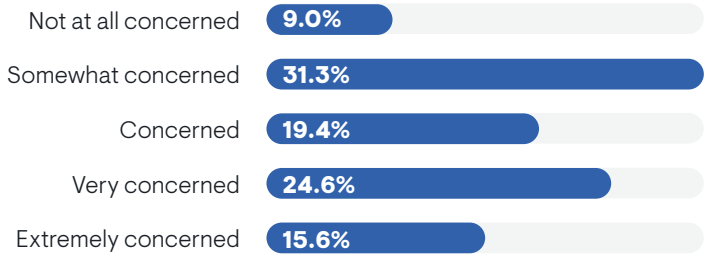
Eighty-two percent of respondents acknowledge hackers' use of encryption to conceal lateral movement and data exfiltration within private and public cloud environments. The acknowledgment of hackers' exploitation of encryption to conceal malicious activities underscores the importance of dynamic and adaptive security approaches. As threat actors adapt their tactics to exploit encrypted channels, organizations must adapt their strategies to effectively detect and counteract these threats. This statistic reinforces the urgency of integrating encryption solutions that bolster security without compromising visibility.

PLEASE RATE THE FOLLOWING STATEMENT: HACKERS ARE USING ENCRYPTION TO HIDE LATERAL MOVEMENT AND/OR DATA EXFILTRATION IN OUR PRIVATE AND PUBLIC CLOUDS.



The apprehension regarding the potential disruption caused by TLS 1.3 to existing network and security monitoring functions is palpable, with a substantial 91% of respondents expressing varying degrees of concern. This concern revolves around the possibility of losing critical visibility into both inbound and internal encrypted traffic, highlighting the pivotal role monitoring plays in effective threat detection and response.

HOW CONCERNED IS YOUR ORGANIZATION THAT TLS 1.3 MAY DISRUPT EXISTING NETWORK AND SECURITY MONITORING FUNCTIONS, CAUSING THEM TO LOSE VISIBILITY INTO INBOUND AND INTERNAL ENCRYPTED TRAFFIC?



The overwhelming concern reflected in the statistic underscores the significant impact that TLS 1.3 can have on the existing network and security monitoring ecosystem. This apprehension stems from the realization that the advanced security features of TLS 1.3, while enhancing encryption, simultaneously introduce challenges for deep packet inspection. The statistic underscores the urgency for organizations to recalibrate their monitoring strategies to adapt to the encryption standards, ensuring a robust defense against potential threats while maintaining situational awareness.

Nearly one-quarter of organizations (22.7%) reported encountering security incidents or breaches due to the loss of visibility resulting from the implementation of TLS 1.3. This statistic underscores the delicate balance organizations must strike between encryption's security benefits and the potential challenges it poses to threat detection and response mechanisms.

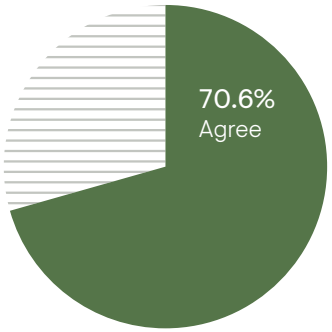
HAS YOUR ORGANIZATION EXPERIENCED ANY SECURITY INCIDENTS/BREACHES DUE TO THE LOSS OF VISIBILITY FROM THE IMPLEMENTATION OF TLS 1.3?

Twenty-three percent may seem small, but the number demonstrates the real-world impact that a TLS implementation has on visibility. It also does not consider the incidents the organization experienced that went unreported, so the number is likely even more significant. These incidents serve as cautionary tales, illustrating the importance of maintaining visibility into encrypted traffic while deploying measures to mitigate risks arising from the loss of such visibility.

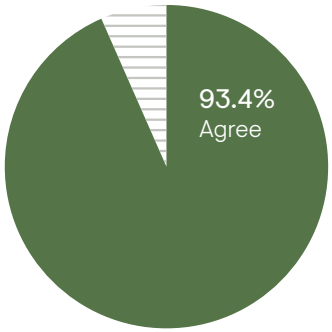
Seventy percent of respondents perceive network encryption as causing blind spots in the monitoring of cloud and virtual environments. This demonstrates the difficulties that TLS blind spots create and underscores the challenges organizations encounter when monitoring encrypted traffic in dynamic cloud and virtual environments. It also reinforces the importance of developing adaptive monitoring strategies that align with encryption advancements, ensuring comprehensive coverage while preserving operational agility.

Ninety-three percent of respondents express confidence in the efficacy of their organization's security tools to protect network traffic within the network perimeter. Ninety-one percent of those surveyed believe that their organization's security tools are effective at protecting incoming network traffic at the network perimeter.

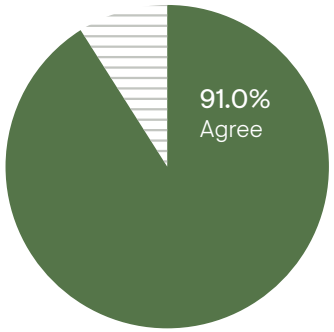
NETWORK ENCRYPTION IS CREATING BLIND SPOTS IN OUR ABILITY TO MONITOR OUR CLOUD AND VIRTUAL NETWORK TRAFFIC.



THE SECURITY TOOLS MY ORGANIZATION USES ARE EFFECTIVE AT PROTECTING NETWORK TRAFFIC INSIDE OUR NETWORK PERIMETER.



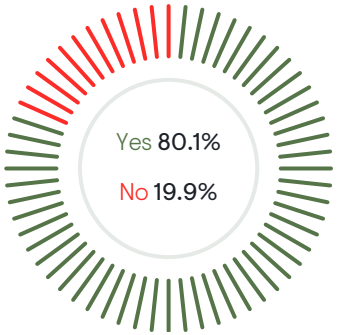
THE SECURITY TOOLS MY ORGANIZATION USES ARE EFFECTIVE AT PROTECTING NETWORK TRAFFIC THAT COMES INTO OUR NETWORK PERIMETER.



The high level of confidence expressed in this statistic indicates that organizations generally have misguided faith in the ability of their network tools to safeguard against external threats at the network perimeter. There are also concerns about existing perimeter tools and topologies for organizations with firewalls and microsegmented networks. The harsh reality is that both of those methods provide a false sense of network security, yet do very little to solve emerging and modern security threats. The evolving threat landscape and the adoption of encryption standards like TLS 1.3 challenge this perimeter-centric approach. Organizations must continue to evolve their security strategies to address threats that may evade perimeter defenses through encrypted channels.

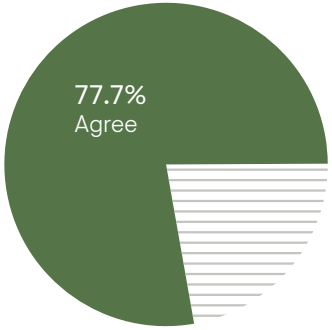
Eighty percent of respondents identify compliance and regulatory requirements as the driving force behind their organization's motivation to implement TLS inspection in cloud environments. The prominence of compliance and regulatory motivations emphasizes the interconnected relationship between encryption, cloud environments, and adherence to industry-specific regulations. Organizations are compelled to align their encryption practices with regulatory standards to ensure the security and privacy of sensitive data. It shows that compliance serves as a driving catalyst for the adoption of TLS inspection, reflecting the need to ensure data protection while capitalizing on the advantages cloud computing offers.

DO YOU SEE COMPLIANCE AND REGULATORY REQUIREMENTS AS THE PRIMARY MOTIVATION FOR YOUR ORGANIZATION TO IMPLEMENT TLS INSPECTION IN CLOUD ENVIRONMENTS?



Nearly 78% believe that their organization recognizes the need for supplementary compensating controls (additional tools/processes beyond what is already implemented in their environments) to address the lack of visibility arising from network traffic encryption, highlighting the proactive approach organizations are taking to mitigate potential challenges. The necessity for additional compensating controls aligns with the evolving understanding that encryption, while bolstering security, can introduce complexities that demand innovative solutions.

PLEASE RATE THE FOLLOWING STATEMENT: MY ORGANIZATION REQUIRES ADDITIONAL COMPENSATING CONTROLS DUE TO THE LACK OF VISIBILITY NETWORK TRAFFIC ENCRYPTION CAUSES.



Conclusion

There is no question that organizations MUST protect their data – either in the cloud, in a container, on-premises, or in some other virtual environment. However, the concerns organizations have regarding using TLS 1.3 to encrypt that data and network traffic are well-founded. The journey toward adopting the TLS 1.3 encryption standard has been characterized by a blend of opportunities and challenges deeply rooted in the shifting sands of the cybersecurity landscape.

The prevailing sentiment reveals both a recognition of the advantages TLS 1.3 encryption brings and an acknowledgment of the potential complications it introduces. The concerns related to the disruption of existing network and security monitoring functions highlight the critical role of monitoring in identifying threats within encrypted traffic. As encryption evolves, so must the strategies that maintain visibility while upholding security.

Regulatory compliance emerges as a powerful catalyst, driving organizations to align their encryption practices with industry standards. This speaks to the symbiotic relationship between encryption, cloud environments, and the necessity to safeguard sensitive data. While the statistics showcasing confidence in internal security tools are encouraging, it also creates a false sense of security that their perimeters and networks are well-defended. Also, it doesn't address the evolving threat landscape, which necessitates a continuous reevaluation of strategies to ensure efficacy in the face of dynamic adversaries.

The incidents involving concealed malware within encrypted traffic underline the need for advanced monitoring and detection mechanisms. Encryption, while enhancing security, presents adversaries with a cloak to exploit. Organizations must embrace solutions that can navigate this duality, simultaneously harnessing the benefits of encryption and detecting threats that seek refuge within it.

Ultimately, the TLS 1.3 adoption journey unveils a complex interplay of security, compliance, operational efficiency, and threat resilience. While the adoption of TLS 1.3 remains a process marked by challenges, the insights drawn from this study provide a compass to navigate these complexities. In this dynamic realm, the security landscape evolves and the journey toward effective TLS 1.3 implementation continues to unfold, driven by the pursuit of fortified cyber defenses and resilient data protection strategies.

Luckily, organizations (such as Gigamon) are rising to this challenge, offering – for the first time – a truly actionable and effective solution to encrypting and monitoring network traffic. Others may soon follow, giving organizations an opportunity to address security concerns, meet compliance and regulatory requirements, and refrain from compromising their technology-strategic vision.

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**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4342.090523