Enterprise Strategy Group | Getting to the bigger truth.™

White
Paper

Network Encryption and its Impact on Enterprise Security

By Jon Oltsik, Senior Principal Analyst

February 2015

This ESG White Paper was commissioned by Blue Coat and is distributed under license from ESG.

Contents

Executive Summary

In late 2014, the Enterprise Strategy Group (ESG) and Blue Coat Systems conducted a collaborative research survey of 150 IT and information security professionals with knowledge of or responsibility for network encryption and the associated security policies, processes, and controls used at their organizations.

Survey respondents were located in North America and came from companies ranging in size: 18% of survey respondents worked at organizations with 500 to 999 employees (i.e., large mid-market organizations) while 82% worked at organizations with over 1,000 employees (i.e., enterprise organizations). Respondents represented numerous industry and government segments with the largest participation coming from the information technology industry (33%), financial services industry (12%), manufacturing industry (12%), retail/wholesale (11%), and health care (9%).

This research project was intended to assess the adoption of SSL/TLS network encryption technology and evaluate the information security practices used to decrypt and inspect encrypted traffic. Based upon the data collected, this paper concludes:

- **Network encryption is ubiquitous and growing.** A large percentage of organizations (87%) already encrypt at least 25% of their overall network traffic today. Furthermore, 88% of organizations say they will increase the amount of network traffic they encrypt in the future. Network encryption is increasingly used to protect data privacy and confidentiality and reduce the risk of network snooping or man-in-the-middle attacks.
- **Organizations are decrypting and inspecting SSL/TLS traffic for security purposes**. While network encryption can protect traffic from eavesdroppers, it also introduces a threat vector where cyber-criminals and hackers can cloak malicious activities and circumvent existing network security controls. Recognizing this threat, 87% of organizations inspect at least some of their SSL/TLS traffic as part of their network security operations. Once decrypted, security professionals examine network packets looking for things like malicious content coming from trusted sites, malicious files and/or hidden scripts, and sensitive data leakage. It is worth noting that while organizations are inspecting SSL/TLS traffic, they may not being doing so to an appropriate level necessary for addressing risk. This is especially important because cyber risk will continue to grow proportionally to the increase in overall encrypted traffic.
- **SSL/TLS decryption and inspection is done tactically today.** Security and networking teams are decrypting and inspecting SSL/TLS traffic using a myriad of disparate technologies such as next-generation firewalls, SSL/TLS appliances, and cloud-based services. Unfortunately, this tactical approach is growing more complex and cumbersome as network encryption increases. On the other hand, things appear to be changing. The ESG data also suggests that 20% of organizations have already created a more comprehensive SSL/TLS decryption and inspection strategy while another 66% are in the process of implementing an SSL/TLS decryption and inspection strategy, plan on implementing an SSL/TLS decryption and inspection strategy, or are interested in doing so in the future. Establishing this type of holistic SSL/TLS decryption strategy is critical as today’s tactical approaches add operational overhead and can’t scale to address emerging encrypted cyber risks.

The data points to enterprise-wide SSL/TLS decryption and inspection strategies in the future but what does this type of strategy look like? ESG believes it will be implemented as a hub-and-spoke architecture featuring a high-speed decryption “service” embedded throughout the network which will then collect, process, and forward cleartext network traffic to the various security devices that can further process and analyze it (e.g., security analytics, firewalls, intrusion detection and prevention systems (IDS/IPS), anti-malware/sandboxing appliances). This will not only improve the efficiency of incident detection and response but also provide real-time actionable intelligence to automate network security remediation.

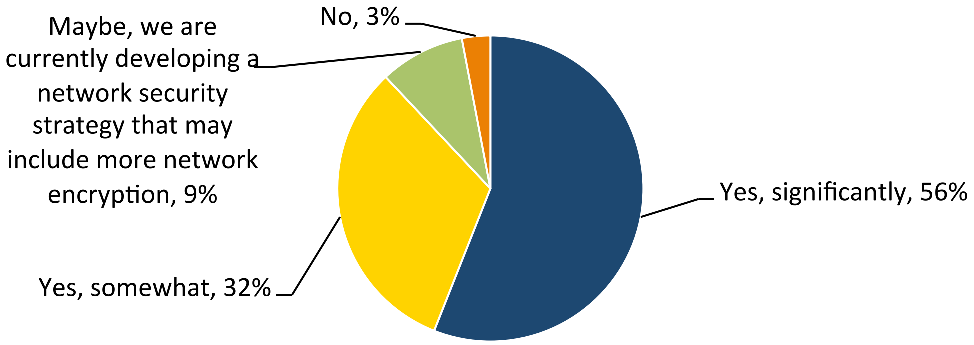
Pervasive Network Encryption

Encrypted traffic has become increasingly ubiquitous at most organizations. A vast majority (87%) of organizations surveyed encrypt at least 25% of their overall network traffic today. Furthermore, some organizations have incorporated network encryption to a much greater degree—25% of the organizations surveyed say they already encrypt as much as 75% of their network traffic!

While encrypted traffic already makes up a significant percentage of total network communications, 56% of organizations say that their percentage of encrypted network traffic will increase significantly over the next 24 months while another 32% believe that their percentage of encryption network traffic will increase somewhat during the same timeframe (see Figure 1).

Figure 1. The Percentage of Encrypted Network Traffic Will Increase at Most Organizations

Do you believe that the percentage of your organization's network traffic that is encrypted will increase over the next 24 months? (Percent of respondents, N=150)



Source: Enterprise Strategy Group, 2015.

Why are organizations increasing their use of network encryption? Respondents pointed to a number of drivers:

- 42% of organizations are increasing their use of network encryption because they believe that network encryption is a security best practice.
- 41% of organizations are increasing their use of network encryption because of an increase in server-to-server (i.e., east-west) traffic that needs to be protected.
- 37% of organizations are increasing their use of network encryption for regulatory compliance.
- 33% of organizations are increasing their use of network encryption (specifically, SSL/TLS) to provide better protection for internally-developed web applications.

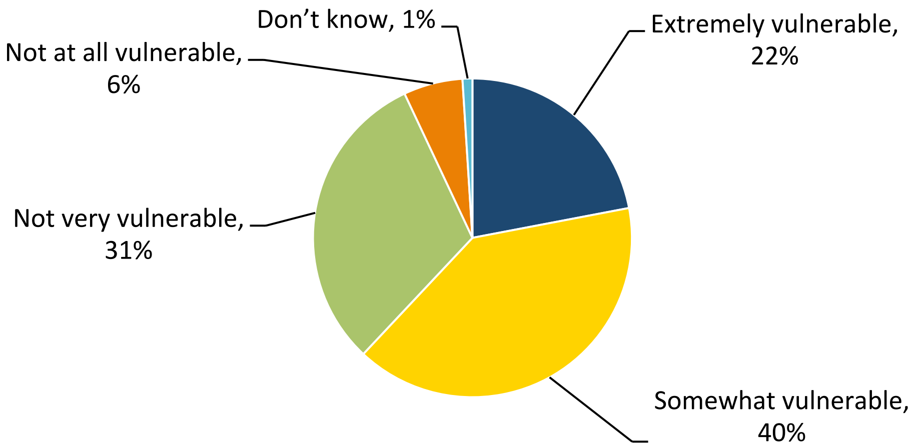
Network Encryption and Information Security

Network encryption is a security best practice as it protects the privacy and confidentiality of network traffic as it travels from source to destination. While this can be beneficial, security professionals understand that network encryption can also be used for malicious purposes. Cyber-criminals and hackers can use encrypted channels to hide reconnaissance activities, malware distribution, and command-and-control (C&C or C2) traffic alongside benign SSL/TLS sessions. By encrypting their malicious actions, hackers are able to circumvent traditional network security tools used for packet filtering, traffic inspection, and advanced threat detection/prevention that can only examine unencrypted network packets. The dilemma is also exacerbated by the fact that advanced persistent threats (APTs) are increasingly using non-standard ports—beyond HTTPS/web on tcp port 443—to infiltrate organizations and confiscate proprietary data. CISOs must also realize that this threat will only increase as organizations encrypt more and more of their overall network traffic.

Are organizations vulnerable to cyber-attacks that use network encryption as a cloaking technique? The IT and security professionals surveyed certainly believe that they are—22% say that their organization is extremely vulnerable to some type of cybersecurity attack that uses SSL/TLS encryption as a cloaking technique to circumvent their existing security controls while 40% believe that their organization is somewhat vulnerable to some type of cybersecurity attack that uses SSL/TLS encryption as a cloaking technique to circumvent their existing security controls (see Figure 2).

Figure 2. Organizations are Vulnerable to Cyber-Attacks Through Encrypted Channels

In your opinion, is your organization vulnerable to some type of cybersecurity attack (e.g., APT, data exfiltration, insider threat, etc.) that uses SSL/TLS encryption as a cloaking technique to circumvent your existing security controls? (Percent of respondents, N=150)



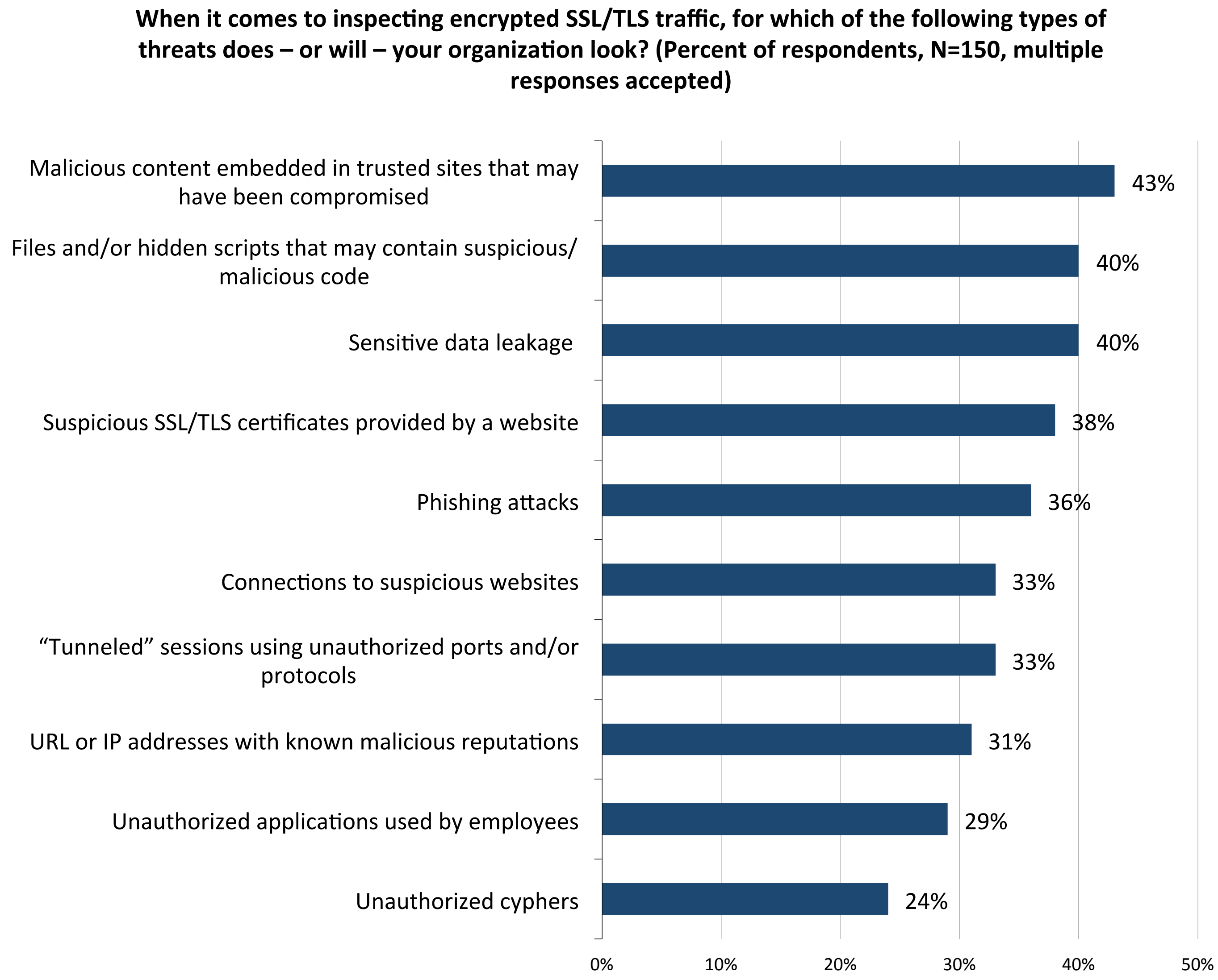
Source: Enterprise Strategy Group, 2015.

Given the rising threat represented by SSL/TLS traffic, most organizations say they are actively implementing network security countermeasures. A strong majority (87%) of the organizations surveyed decrypt and then inspect SSL/TLS traffic for signs of reconnaissance activity, malware, C2 communications, etc. Of the remaining organizations, 8% say they are rolling out the right network security technologies enabling them to inspect SSL/TLS traffic within the next 12 months. The remaining 5% are not decrypting/inspecting encrypted SSL/TLS traffic today but are interested in doing so in the future.

The survey results indicate that SSL/TLS decryption is executed across a variety of protocols (i.e., HTTP, FTP, POP3, IMAP, etc.) using a variety of different tools and technologies, including next-generation firewalls, cloud-based SaaS services, and dedicated SSL/TLS decryption appliances. Organizations also use a variety of technologies for traffic inspection such as web threat management gateways, antivirus gateways, and security analytics/forensic tools.

Just what are security professionals looking to find buried within encrypted sessions? Forty-three percent look for malicious content embedded in trusted sites that may have been compromised (i.e., waterholing) 40% have their eyes out for files and/or hidden scripts that may contain suspicious/malicious code, and 40% monitor SSL/TLS traffic for sensitive data leakage (see Figure 3).

Figure 3. Potential Threats Within Encrypted Traffic



Source: Enterprise Strategy Group, 2015.

Network Security Challenges with SSL/TLS Decryption/Inspection

ESG research indicates that security professionals recognize the threat posed by encrypted network traffic and are proactively implementing security controls to mitigate this risk. In fact, 55% of organizations say they will actually increase the decryption/inspection of SSL/TLS traffic significantly in the future, while 40% will increase the decryption/inspection of SSL/TLS traffic to some degree.

In spite of their current activities, decrypting and inspecting SSL/TLS traffic has created a number of operational and technical challenges. Over the past 5 years, many organizations have slowly increased their use of SSL/TLS in homegrown web applications and adopted cloud-based SaaS applications instrumented with Layer 5/6 encryption. As this occurred, security and network professionals followed on, implementing a variety of SSL/TLS decryption and inspection tools on various network segments and multiple locations across global enterprise networks. This chain of events has resulted in a rather haphazard SSL/TLS decryption and inspection infrastructure made up of a mixture of technologies and operational processes/procedures. This may account for the high percentage of organizations that are decrypting SSL/TLS traffic for security purposes—albeit in a tactical and incomplete fashion.

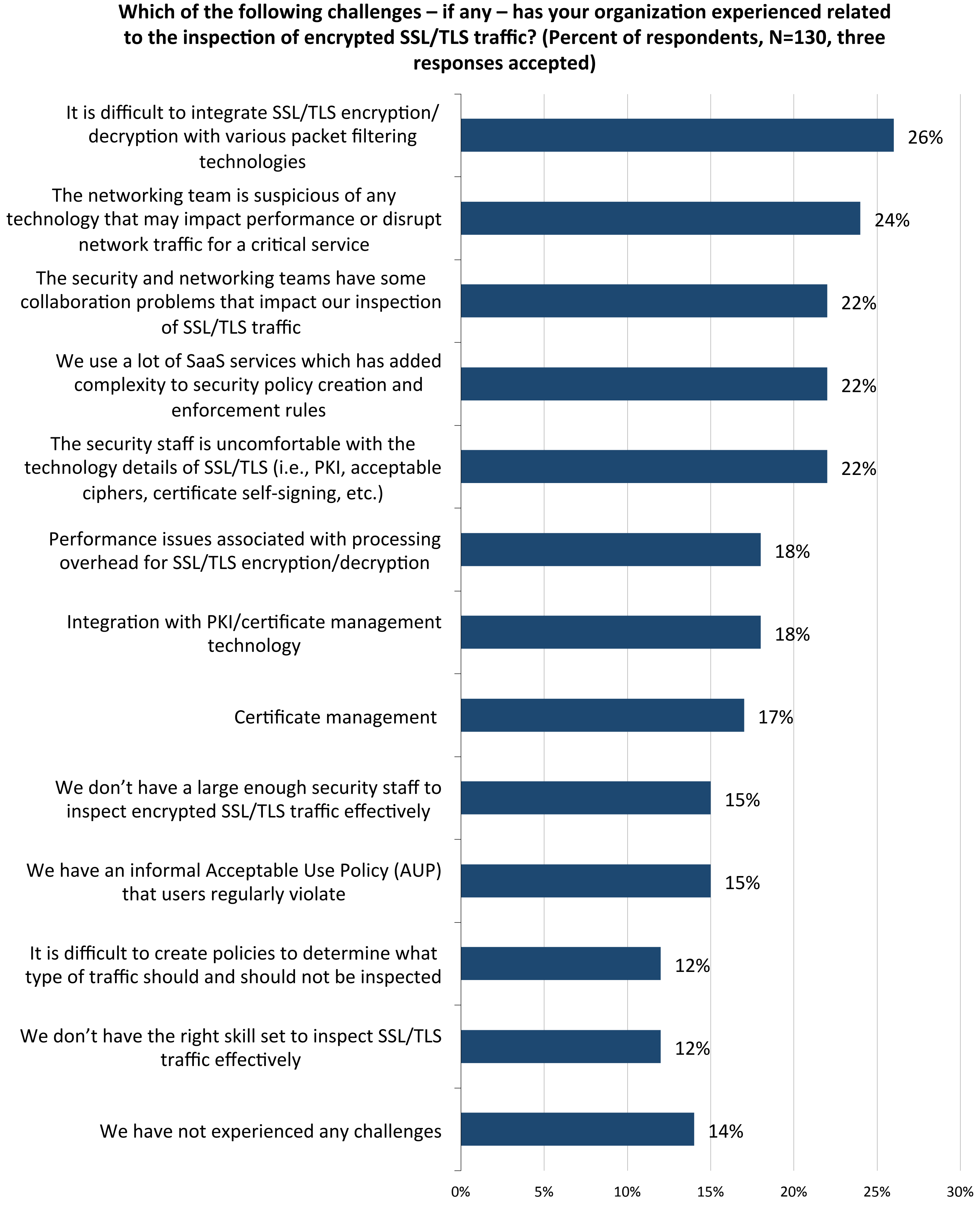
The current assortment of network encryption and security methods is illustrated in the ESG research data. When asked to describe the way their organization approaches SSL/TLS decryption and inspection for security purposes:

- 14% of organizations say that they inspect encrypted SSL/TLS traffic tactically by implementing technologies on the network on an ad-hoc or as-needed basis.
- 21% of organizations say that they currently inspect encrypted SSL/TLS traffic tactically by implementing technologies on the network on an ad-hoc or as-needed basis, but they are interested in creating a more comprehensive enterprise strategy in the future.
- 21% of organizations say that they currently inspect encrypted SSL/TLS traffic tactically by implementing technologies on the network on an ad-hoc or as-needed basis, but they are planning on creating a more comprehensive enterprise strategy in the future.
- 24% of organizations say that they currently inspect encrypted SSL/TLS traffic tactically by implementing technologies on the network on an ad-hoc or as-needed basis, but they are in the process of implementing a more comprehensive enterprise strategy in the future.
- Only 20% of organizations say that they have already implemented a comprehensive enterprise strategy for the inspection of encrypted SSL/TLS traffic.

The aggregate data clearly illustrates the 80/20 rule: 80% of organizations are decrypting/inspecting SSL/TLS traffic tactically while only 20% have embraced a more strategic approach. This will obviously change in the future as 66% of organizations are in the process of implementing an SSL/TLS decryption/inspection strategy, plan on implementing an SSL/TLS decryption/inspection strategy, or are interested in doing so.

While this bodes well for the future, many organizations face growing challenges with SSL/TLS inspection and decryption today. These challenges range across organizational, technology, process and data privacy issues. For example, 26% of security professionals claim that it is difficult to integrate SSL/TLS encryption/decryption technologies with assorted network security packet filtering technologies, 24% say that the networking team is suspicious of any technology that may impact/disrupt the network, and 22% point to collaboration problems between the networking and infosec teams at their organizations (see Figure 4).

Figure 4. Challenges Associated with the Inspection of Encrypted Network Traffic



Source: Enterprise Strategy Group, 2015.

What Does SSL/TLS Decryption and Inspection Strategy Look Like?

The ESG research clearly indicates that most organizations will only increase their use of network encryption and accompanying SSL/TLS decryption and inspection technologies. Furthermore, most firms intend to create a more holistic SSL/TLS decryption strategy in the future, indicating that their current tactical approaches are not working.

This begs an obvious question: Just what does a comprehensive SSL/TLS decryption and inspection solution and strategy look like? At a high-level, ESG believes that this type of network security strategy is highlighted by:

- **High-performance purpose-built SSL/TLS decryption "services."** In today's tactical implementations, organizations are using a variety of technologies scattered about the network for SSL/TLS decryption. This creates a lot of operational overhead and can lead to complex network proxy implementation and SSL certificate management challenges. To alleviate these bottlenecks, organizations are or will likely create an SSL/TLS decryption hub-and-spoke "service" based upon purpose-built technology. It's likely that SSL/TLS decryption technology will be anchored by a software architecture featuring central command-and-control (i.e., policy management, certificate management, configuration management, reporting, etc.) and distributed enforcement. Furthermore, actual decryption operations will be executed in various form factors—high-performance appliances for the data center and/or network core, small or virtual appliances for remote offices, and cloud-based virtual appliances to protect IaaS, SaaS, and PaaS networks.
- **Multi-layer integration with security tools.** Once traffic is decrypted, the SSL/TLS decryption architecture will process and forward traffic to various security tools (e.g., NGFW, IDS/IPS, malware analysis, security analytics) for further content inspection. This will also resemble a hub-and-spoke architecture with the SSL/TLS decryption service acting as a centralized middleware bridge. This approach preserves the existing security infrastructure, while adding a scalable and adaptable encrypted traffic management solution. Security analytics tools, more specifically, will inspect traffic individually while a master analytics engine correlates threats across all network security analytics tools and services.
- **Automated remediation.** Based upon this type of enterprise strategy, SSL/TLS decryption and inspection will be coordinated across high-speed devices and networks with near real-time performance. Given this, CISOs should work with network engineers and architects to implement automated network security controls into the network. When advanced malware detection, network forensic, and endpoint forensic tools identify a compromised PC uploading encrypted files to an IP address in Eastern Europe with a high degree of confidence, the network should have the ability to automatically terminate this connection while creating new IDS/IPS signatures and firewall rules to block similar activities in the future.

The SSL/TLS decryption and inspection architecture described above will get a symbiotic boost as organizations embrace software-defined networking (SDN) and network functions virtualization (NFV) technologies over the next few years. Both SDN and NFV make network functions programmable through standard software APIs. When the network detects encrypted packets, it can be programmed to create a dynamic VLAN to route traffic to an SSL/TLS decryption service. Once decrypted, the SSL/TLS service can then create multiple dynamic VLANs to route the cleartext traffic on to various security devices, as needed. This will greatly ease network hard-coding complexity and ease the burden of implementing an enterprise-wide SSL/TLS strategy.

The Bigger Truth

The data presented in this report represents a familiar story to IT and information security professionals. IT implements a new technology that the infosec team is asked to secure. This is a fluid process with different adoption schedules, processes, and technologies employed throughout the enterprise. The IT and security groups collaborate on balancing business enablement against risk management but the complex mix of people, processes, and technologies leads to a chaotic infrastructure that is difficult to manage and monitor.

This report indicates that many organizations have reached this exact tipping point. They are increasingly encrypting network traffic to protect data confidentiality, but this means decrypting and inspecting SSL/TLS traffic for security purposes. While they are addressing risk, this process has grown extremely complex and introduced snowballing operational overhead.

Since so many organizations are abandoning their tactical SSL/TLS decryption and inspection methodologies in favor of a more strategic approach, it is safe to assume that existing SSL/TLS decryption and inspection methodologies are growing increasingly ineffective and complex. Since most organizations plan to increase their use of network encryption, CISOs shouldn’t let their SSL/TLS decryption and inspection strategies languish. Rather, they should make encrypted traffic management a near-term priority so they can simultaneously address increasing SSL encrypted traffic and dangerous, potentially hidden cyber threats.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com