IDC
Analyze the Future

THE BLIND STATE OF RISING SSL/TLS TRAFFIC: ARE YOUR CYBER THREATS VISIBLE?

ROBERT WESTERVELT
JULY 2016

IDC WHITE PAPER
SPONSORED BY F5

INTRODUCTION

Traditional security gateways, network firewalls, and intrusion prevention systems are increasingly blinded by the rising tide of encrypted traffic, and some enterprise chief information security officers (CISOs) are alarmed by this lack of visibility. The growing volume of bandwidth associated with cloud-based services and the rising amount of encrypted traffic are a double blow to these traditional security solutions. Encrypted traffic blinds prevention systems from hacker communications to command and control infrastructure and attacker movement within an organization to critical resources. This traffic also prevents many of these network security appliances from identifying signs of targeted attacks, malicious scripts, and other criminal tools and tactics used to infiltrate corporate networks.

Recent IDC research involving IT executives and professionals demonstrates the rising concern associated with the influx of Secure Sockets Layer/Transport Layer Security (SSL/TLS) encrypted traffic. Nearly 90% of respondents cited a seriously diminishing field of vision, according to IDC's *State of SSL/TLS and Threat Visibility Survey* of 300 IT security executives and network and security architects as well as their line-of-business (LOB) colleagues. The survey, commissioned by F5 Networks, found that data loss prevention systems are sending fewer alerts and network firewalls, IPS appliances, and other security gateways designed to protect end users and critical resources are failing to handle the rising volume of traffic that requires SSL decryption for inspection.

Key findings include:

- **Rising concern:** Survey respondents said they are very concerned about the effectiveness of their security gateway solutions, their modern specialized threat analysis and protection (STAP) products, and their data loss prevention and other network security solutions as a result of increased SSL/TLS encrypted traffic.
- **Main drivers of SSL/TLS traffic:** Office 365 and other cloud-based application services are among the main drivers of increased bandwidth requirements and additional SSL/TLS encrypted traffic associated with the service. Web applications and social media are also huge drivers.
- **Lacking decryption strategies:** Only 25% of those surveyed said their organization decrypts some network traffic to inspect inbound and outbound communications for potential threats. About 36% of those surveyed said their organization has adopted a standalone SSL decryption appliance. More than 27% use application delivery controller (ADC)-based SSL termination.

These traditional security gateways, network firewalls, and IPS appliances have SSL decryption capabilities, but many organizations are choosing to not enable the functionality out of fear that it could degrade network traffic flow and potentially disrupt business operations. There's also a long-standing perception that network security appliances experience significant performance degradation when SSL inspection is enabled due to the processing power that is required for the capability. Some recent testing firms have also documented the negative impact on some products.

This survey also noted the growing complexity associated with SSL/TLS management as well as data encryption and key management. Nearly all organizations had multiple groups and individuals within the organization responsible for monitoring and key management. The survey also found that maintenance of the SSL/TLS certificates (in some cases, organizations are managing 20 or more certificates) is often done on an ad hoc basis or when a serious vulnerability is discovered or a security update is issued for the protocol.

IN THIS WHITE PAPER

Security solutions designed to monitor network traffic to detect threats and prevent data leakage are becoming less effective as a result of the growing volume of bandwidth associated with cloud-based services and the rising amount of encrypted traffic, according to the results of an IDC survey commissioned on behalf of F5 Networks. This white paper provides an overview of SSL/TLS as well as its current status in enterprise adoption and its impact on the enterprise IT. The document also discusses security issues and challenges associated with failing to inspect SSL/TLS traffic.

Rising Encrypted Traffic, Disintegrating Threat Defenses

Between one-half and three-quarters of attacks cloak their communications in encrypted traffic, and criminals sometimes use stolen digital certificates and encryption keys to evade detection. This tactic is easy to carry out because network components typically provide implicit trust in cryptographic keys and digital certificates. The rising amount of encrypted traffic is hampering the ability of IT security teams to protect customer data and other sensitive corporate assets. Data loss prevention systems, unified threat management appliances, and other security solutions that inspect network traffic often have the ability to decrypt network traffic, but organizations often fail to enable the capability or turn it off due to the perception that performance issues could have an impact on business operations. The survey found that SSL/TLS traffic inspection is enabled in less than half of all network security appliances, with a large number of these solutions blind to malware flowing past them in this encrypted traffic.

Malware researchers found attackers leveraging poorly managed Web sites to set up command and control infrastructure that takes advantage of SSL/TLS for botnet management and malware communication. The threats that may be missed are significant and can be the cause of many security incidents. Increasingly sophisticated attack toolkits include components that automate the process of adding evasion techniques to malware. The toolkits are sometimes designed to be updated on a regular cycle and provide exploits for zero-day vulnerabilities and software flaws in Microsoft Office files, Adobe Flash, Adobe Reader, and browser components where organizationwide patching may suffer delays.

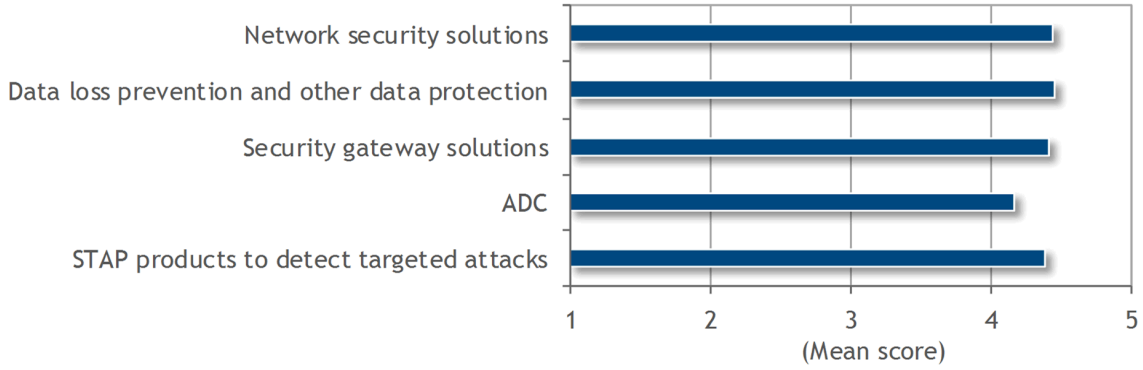
Malware infections, botnet communication, and data exfiltration are common and can hide within an encrypted traffic stream from employee PCs to remote Web servers. Adding to the complexity of the problem is that the encrypted tunnel cannot always be inspected. Careful consideration must be paid to regulatory data, such as banking, healthcare, and other transactions that include personally identifiable information (PII).

As shown in Figure 1, 90% of those surveyed indicated they are very concerned about the negative impact encrypted traffic is having on the effectiveness of their network security solutions, data loss prevention solutions, and security gateway solutions. In addition, the concern extends to new investments. According to survey respondents, recently adopted STAP solutions, designed to detect advanced threats, could be hampered by a lack of visibility. Most strategies to offset the limited visibility by enabling SSL decryption for inspection are hampered by business needs requiring constant availability and performance of critical applications. The survey found that 36% of organizations adopted a standalone SSL decryption appliance. More than 29% use an ADC-based SSL termination to inspect encrypted traffic.

FIGURE 1

Impaired Security Solutions: Encrypted Traffic Impact

Q. On a five-point scale, with one being not concerned and five being very concerned, how concerned are you about any negative impact SSL/TLS encrypted traffic may be having on the effectiveness of the following security solutions?



Source: IDC's *State of SSL/TLS and Threat Visibility Survey,* April 2016

Action Items

- **Document the extent of impairment:** Conduct a careful assessment to determine the risks associated with failing to inspect encrypted traffic. Identify how much traffic is failing to be inspected and begin documenting this traffic to report to senior management and other stakeholders.
- **Develop a decryption strategy:** Incorporate SSL/TLS decryption requirements into long-range planning with the aim to raise awareness among senior executives and gain support for allocating funds for improvements.
- **Identify impacted assets:** An assessment must identify the impact security appliance impairment has on the organization's key assets. Consider ways to bolster security, including two-factor authentication and file integrity monitoring solutions to restrict access to sensitive resources.

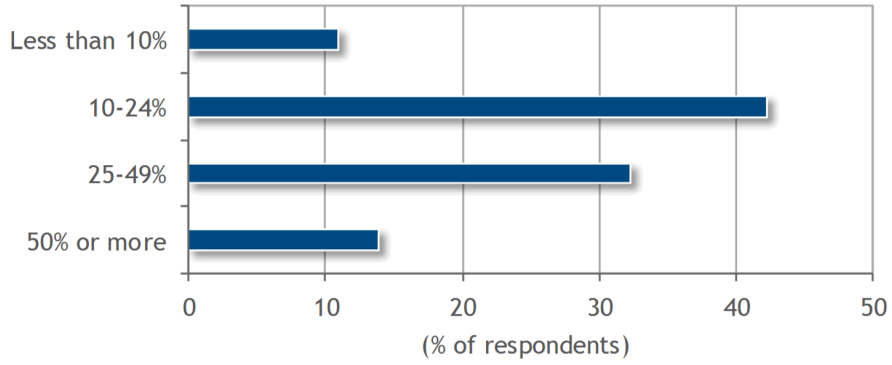
As shown in Figure 2, most survey respondents said 25-50% of their network traffic is encrypted. Nearly all survey respondents said they are concerned or very concerned about the impact of SSL/TLS encrypted traffic on the effectiveness of their security gateway solutions, their STAP products, and their data loss prevention and other network security solutions as a result of increased SSL/TLS encrypted traffic.

Making matters worse, the vast majority of security gateways and other network security appliances are deployed without decryption functionality enabled. This gives security teams and upper management a false sense of security and provides an avenue for criminals to use to evade detection and communicate with the outside world or exfiltrate data.

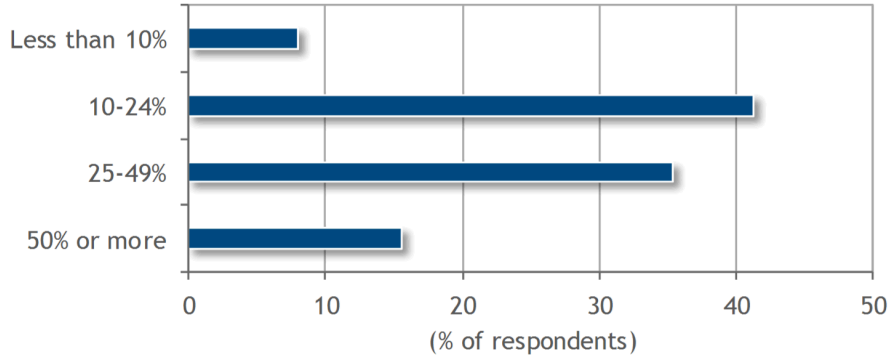
FIGURE 2

At Least Half of All Inbound and Outbound Traffic Is Encrypted

Q. What is the percentage of inbound SSL/TLS encrypted traffic to your organization?



Q. What is the percentage of outbound SSL/TLS encrypted traffic to your organization?



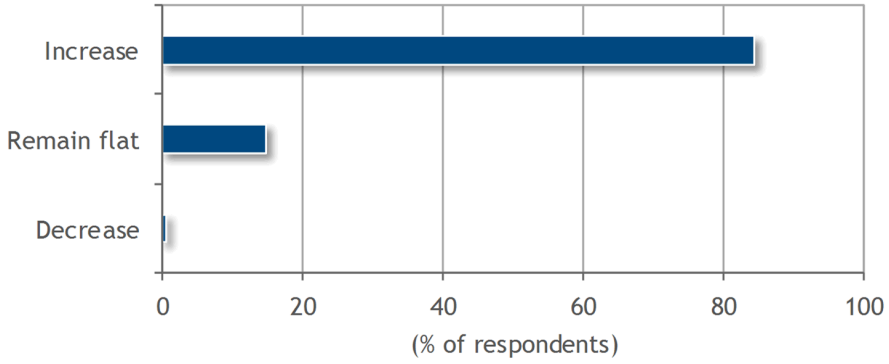
Source: IDC's *State of SSL/TLS and Threat Visibility Survey,* April 2016

As shown in Figure 3, outbound and inbound encrypted traffic is expected to continue to rise. With few organizations decrypting traffic for inspection, visibility will likely continue to decline and threat detection will also take a hit. Some senior security executives have already indicated in interviews with IDC that they have noted data loss prevention and other security appliances are sending fewer alerts to their security operations center. Concern is rising, but currently, spending is on compliance efforts and the adoption of STAP. These modern security solutions may be more powerful than traditional security solutions, but it is questionable whether their embedded decryption components can scale to handle the increased bandwidth requirements over time.

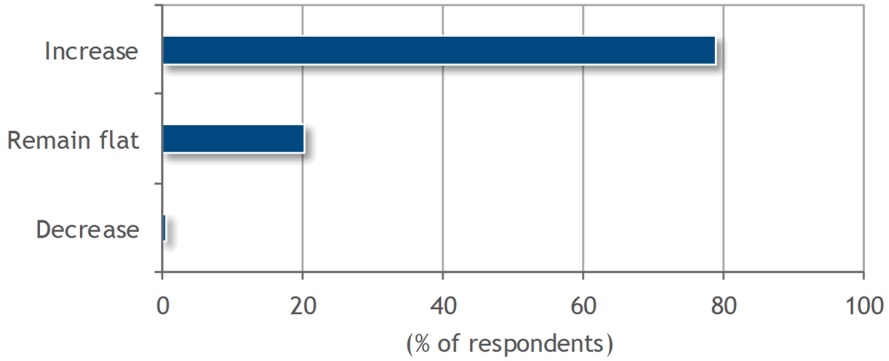
FIGURE 3

Rising Concern: Expected Rise in Outbound and Inbound Encrypted Traffic

Q. Over the next two years, do you think that outbound SSL/TLS encrypted traffic will rise?



Q. Over the next two years, do you think that inbound SSL/TLS encrypted traffic will rise?



Source: IDC's *State of SSL/TLS and Threat Visibility Survey,* April 2016

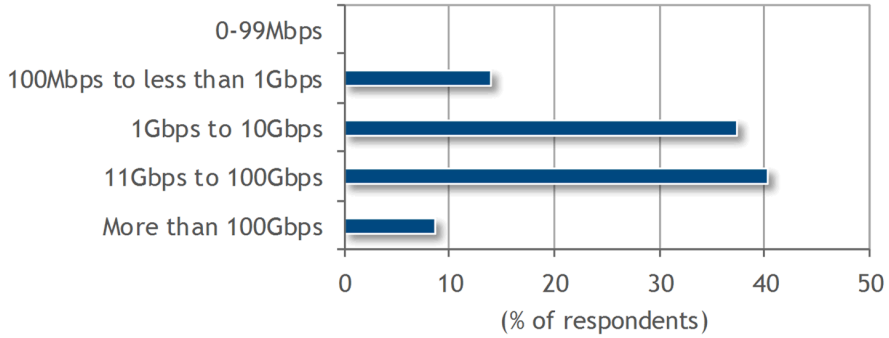
While IT teams are dealing with SSL/TLS traffic growth, they must also address rising bandwidth requirements. Employee adoption of SaaS offerings supporting collaboration is one of the factors driving up overall bandwidth requirements among organizations.

As shown in Figure 4, bandwidth requirements are reaching the 100Gbps level and are expected to rise at least 20% over the next three years. This rising bandwidth also impacts the performance of critical network security appliances. Previous studies have shown that when SSL/TLS traffic inspection is enabled, performance can be negatively impacted by nearly 75%. When the rising amount of traffic these security appliances must handle is added to the mix, enabling inspection of encrypted traffic undoubtedly would have a detrimental impact on throughput and inspection performance.

FIGURE 4

Bandwidth Requirements at 100Gbps

Q. What are your organization's current overall bandwidth requirements?



Source: IDC's *State of SSL/TLS and Threat Visibility Survey,* April 2016

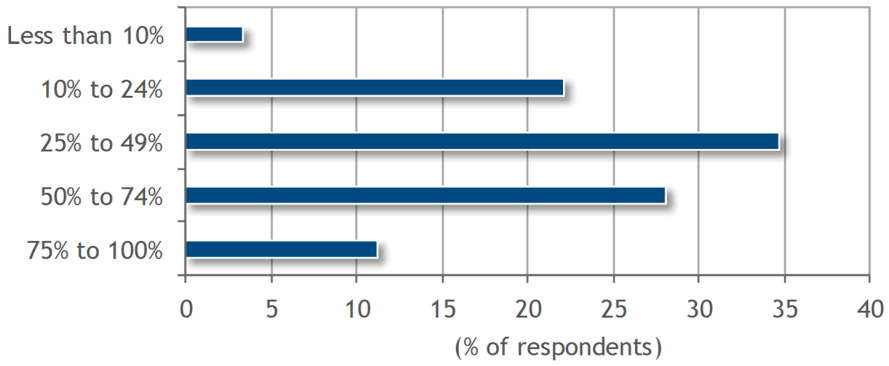
SSL/TLS traffic appears to be already hindering threat detection, according to the survey. As shown in Figure 5, network security appliances have limited visibility into traffic, with only 34.7% of those surveyed indicating that a quarter to half of their security appliances have SSL inspection enabled.

Disabling or failing to enable SSL inspection is particularly concerning. Attackers are shielding themselves in encrypted traffic, giving them the cover they need to communicate with malware and steal data to remote servers. It increases the criminal dwell time and, in turn, the ability of an attacker to direct malware to identify critical resources, identify and steal account credentials of privileged users, and conduct reconnaissance activity over an extended period of time.

FIGURE 5

SSL Inspection Enabled in Less than Half of All Security Appliances

Q. Based on the network security solutions you indicated the organization uses, what percentage of those solutions have SSL decryption enabled?



Source: IDC's *State of SSL/TLS and Threat Visibility Survey,* April 2016

Action Items

- **Examine key/certificate governance:** Assess the status of key and certificate management within the organization and communicate with key stakeholders the need for a strategy to support more robust traffic inspection. This requires the associated keys and certificates to support the decryption functionality.
- **Assess security appliances configuration:** Identify poorly configured security appliances and whether they protect key resources. Map security appliances to the applications they protect and determine how significant the applications are in supporting key business requirements.
- **Determine effectiveness of privacy policies:** Enabling decryption in security appliances or a standalone solution requires analysis of regulatory compliance and an assessment of employee and customer privacy concerns. Privacy policies should reflect the extent of visibility the company has into some encrypted communications and be properly communicated to employees.

Key Factors Behind Surging Encrypted Traffic

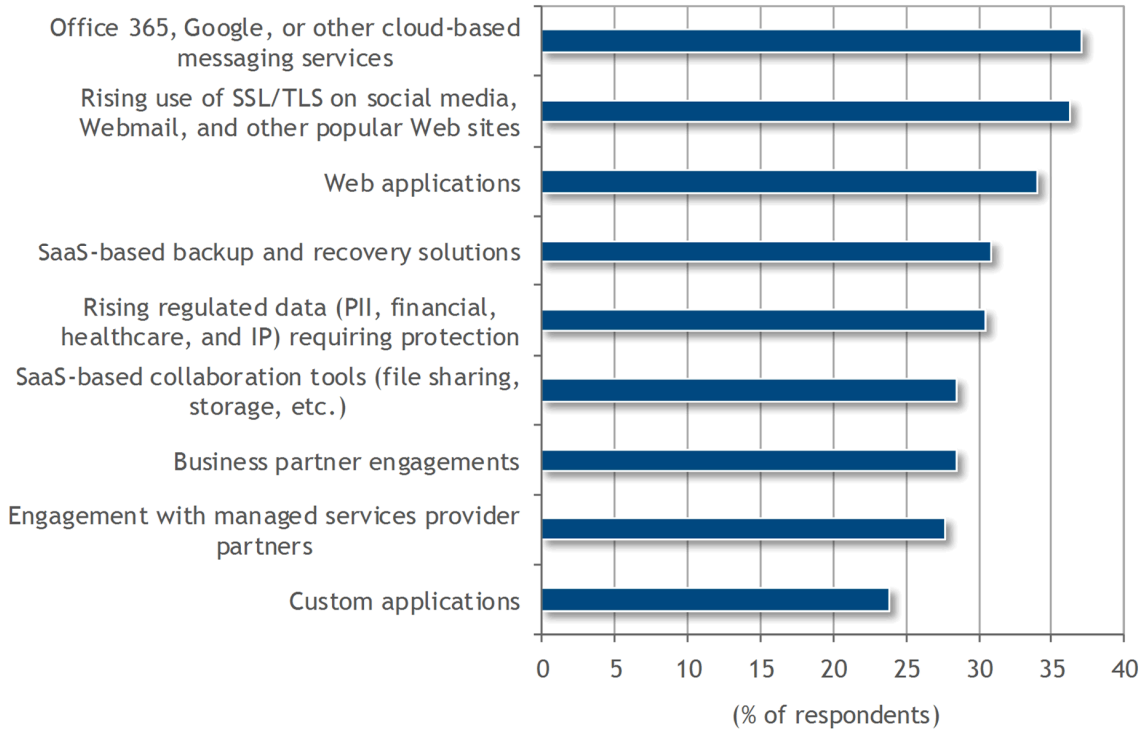
Adoption of Office 365 has increased significantly, but some organizations may not have planned for the increased bandwidth requirements and additional SSL/TLS encrypted traffic associated with the service. As shown in Figure 6, enterprise adoption of Office 365 and employees' use of social media and popular Web sites that encrypt traffic are the main drivers for outbound encrypted traffic increases. SSL/TLS improves the confidentiality of communications, and most messaging services, social networks, and highly visited Web sites encapsulate communication between their servers and their customers. Mobile devices are also contributing to increased SSL/TLS encrypted traffic because mobile developers can easily add support for SSL/TLS using widely available software development toolkits.

Some modern security solutions are designed to identify malicious communication within encrypted traffic without decrypting it, but most of this traffic evades inspection, raising the risk of data leakage or a costly breach.

FIGURE 6

Outbound Encrypted Traffic Tied to Office 365 and Rising SSL/TLS Support

Q. Indicate the top 3 drivers of increased outbound SSL/TLS encrypted traffic in your organization.



Source: IDC's *State of SSL/TLS and Threat Visibility Survey,* April 2016

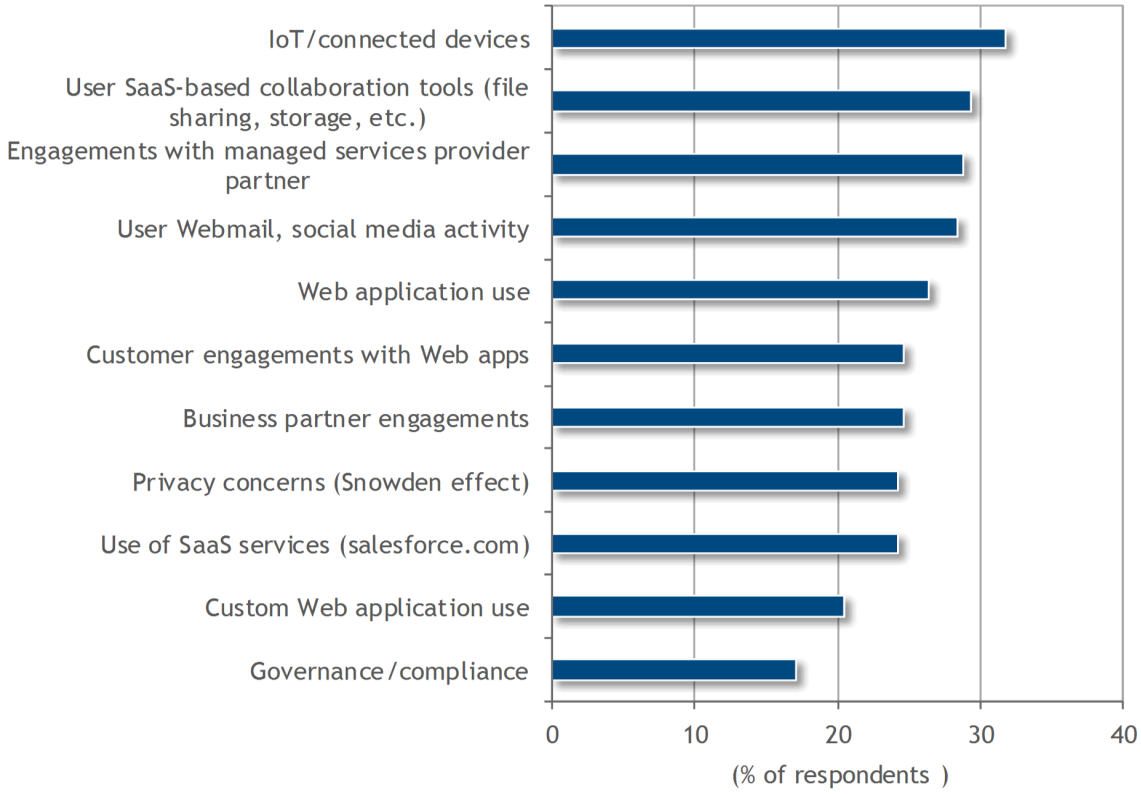
Survey respondents cited smartphones, tablets, and other Internet-enabled devices as one of the factors causing increasing inbound encrypted traffic. As shown in Figure 7, other contributors to the inbound encrypted traffic increase are managed service provider partners and employees' use of SaaS-based collaboration tools.

Inbound encrypted traffic is marginally less of a problem for organizations. IDC's interviews with network or application architects found that many will proactively address the issues as part of network and application performance activities. Decryption for inbound encrypted traffic is often carried out by an ADC performing SSL offloading. A smaller number of survey respondents (27%) indicated they had an ADC deployed in their network. All those survey respondents indicated their organization relies on ADC-based SSL termination to enable inspection of traffic.

FIGURE 7

Inbound Encrypted Traffic Tied to IoT, MSP Engagements, and SaaS Collaboration Tools

Q. Indicate the top 3 drivers of increased inbound SSL/TLS encrypted traffic in your organization.



Source: IDC's *State of SSL/TLS and Threat Visibility Survey,* April 2016

Action Items

- **Assess bandwidth requirements:** Gain a thorough understanding of current and future bandwidth requirements. Consider the performance impact on security appliances that perform SSL inspection. Determine if offloading decryption to an ADC or a standalone decryption appliance is required.
- **Perform SaaS adoption due diligence:** Sensitive data in motion must be protected regardless of whether it is in a public or private cloud environment. IT security should assist in evaluating new SaaS platforms and provide an impact analysis that considers the risks posed by rising SSL/TLS traffic and the need for increased bandwidth.
- **Establish SaaS governance:** Ensure that IT security is reflected in policies regarding SaaS adoption. Ensure that established key and certificate management practices are addressed for new platforms that require data encryption.

Adoption of Standalone Decryption, ADC SSL Offloading Rises

As shown in Figure 8, some organizations have adopted or plan to adopt a standalone decryption appliance to intercept and send encrypted traffic for inspection. IDC believes that spending on standalone decryption appliances, application delivery controllers, and other solutions to decrypt and inspect network traffic will experience rapid growth over the next five years. The market segment is projected to grow by double digits and could reach nearly $800 million by 2020.

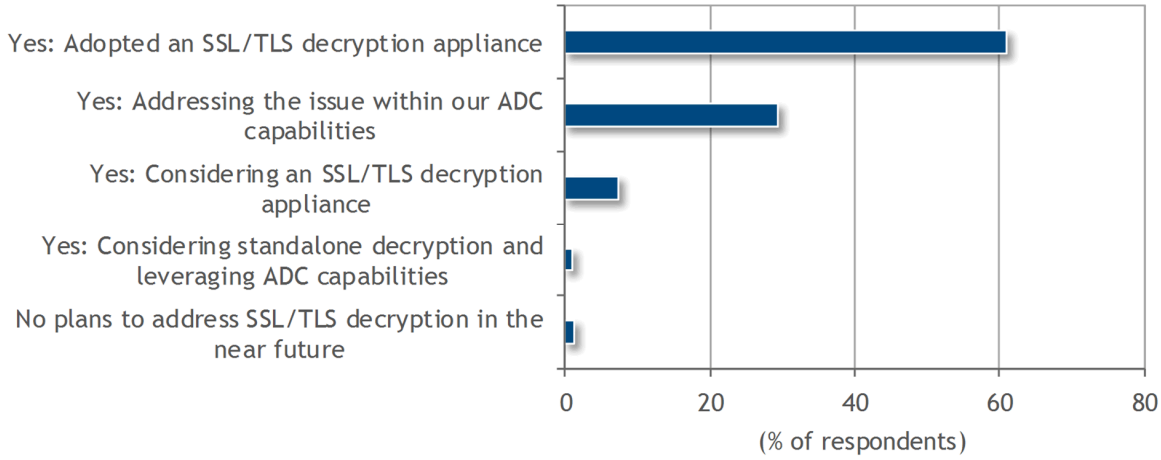
Decrypting traffic can be challenging for network and security teams. In addition to certificate and key management issues, decrypting some outbound traffic streams requires the decryption appliance to be inline. This inline approach must be carried out carefully, or it can generate false positives and block legitimate traffic, potentially disrupting business operations. Inbound traffic can be inspected with an application delivery controller.

Concerns about the impact encrypted traffic is having on the effectiveness of security infrastructure are compounded by the fact that the volume of inbound and outbound encrypted traffic is expected to grow significantly. Ultimately, survey respondents said it could take a data breach, a failed audit finding, or regulatory push to force upper management to approve an additional investment in ways to inspect the encrypted traffic.

FIGURE 8

Intercepting Encrypted Traffic for Inspection

Q. Does your organization currently use or plan to use technology to decrypt and inspect SSL/TLS traffic?



Source: IDC's *State of SSL/TLS and Threat Visibility Survey,* April 2016

SSL/TLS 101

The SSL/TLS cryptographic protocols provide a secure communications link between a client and a server. The protocols are increasingly supported by a wide variety of Web sites to protect banking, ecommerce transactions, email, social media, and other activity that involves personal information and other sensitive data.

Regulatory requirements often prompt organizations to support SSL/TLS. By encrypting data in transit between the user and the server, enterprises can prevent attackers from eavesdropping or sniffing network packets to gain access to sensitive details. If SSL/TLS is properly implemented, the encrypted traffic also mitigates the risk of spoofing attacks, which enable criminals to hijack a user session in order to bypass access controls and steal sensitive data. These spoofing attacks can also be used as a stepping-stone, giving criminals the ability to move laterally in a corporate network to systems containing sensitive intellectual property, account credentials, and customer and/or employee data.

SSL version 3.0 was released by Netscape in 1999 and supported by nearly all popular Web browsers. To support SSL, a Web server administrator must acquire a digital certificate from a certificate authority, which is maintained to ensure the identity of the applications hosted on the organization's application server. Once the server is configured to support SSL connections, the encryption protocol encapsulates communication between the client system and the server, following a key exchange or "handshake" between the client and the server, establishing trusted identities between the two parties. The process leverages the server's digital certificate, which proves the trusted identity of the server owner and the application being accessed has been validated by the certificate authority.

TLS was also released in 1999 as a standard cryptographic protocol. The process it uses to validate the integrity of the two parties is slightly different. SSL and TLS support RSA, Diffie-Hellman, and other exchange algorithms.

Threats to SSL/TLS

The SSL/TLS protocol helps prevent eavesdropping and other attacks, but over the past decade, security researchers have identified weaknesses that could be used by attackers to hijack an encrypted session. A "man-in-the-middle attack" is the most common tactic to exploit SSL/TLS vulnerabilities. Financially motivated criminals can capture and reinstate a secure session as well as conduct spoofing to conduct fraudulent banking transactions without the victim's knowledge. Antifraud software adopted by most banks and financial services organizations can identify malware-infected systems attempting to establish a secure connection.

Attacks that leverage SSL/TLS surface nearly every year. The POODLE (Padding Oracle On Downgraded Legacy Encryption) is a good example of a prominent SSL vulnerability that led Web browser makers to pull support for outdated versions of the protocol. The vulnerability, identified by Google researchers in 2014, enabled attackers to eavesdrop on encrypted traffic by sending spoofed packets to downgrade the secure connection between a user and a Web site to a weaker version of the protocol.

In 2015, a 14-year-old weakness in the Rivest Cipher 4 (RC4) encryption algorithm supported by approximately 30% of the Internet's TLS implementations enabled attackers to conduct sniffing or eavesdropping. A weak key pattern enabled criminals to identify a private key and view the traffic in plain text.

Survey Identifies Complexity with Digital Certificate Growth

Implementing SSL/TLS and managing encryption within the organization have become more complex as organizations increasingly maintain multiple digital certificates. Survey respondents expressed confidence in their ability to manage digital certificates, but the process of maintaining them varied. For example, the survey found that organizations are more likely to assess the state of their SSL/TLS configuration when a security update is released or a weakness is publicly identified. Less than half of those surveyed (45.2%) said they routinely assess the SSL/TLS configuration.

Solving the problem of inspecting encrypted traffic is also complex. SSL/TLS is leveraged by multiple applications across the organization, and network security appliances require the right keys and certificates to decrypt the traffic. These applications are increasingly supporting 2048-bit and 4096-bit SSL keys. IT personnel also have to manage expired and revoked certificates and keys.

The survey found that key management, an often challenging part of data encryption use, is a shared responsibility within organizations. Despite the responsibility being shared across various individuals, 77.2% of those surveyed said their approach to key management is very well managed. There are policies in place, communication is coordinated across all departments involved, and appropriate training is conducted.

Most organizations manage SSL/TLS certificates centrally, but more than 76% of those surveyed said their organization maintains 10-19 certificates, and that number is expected to grow. In addition, some monitoring systems that share keys require architectural changes to be fully supported, but 85.8% of those surveyed said they were very confident in their IT organization's ability to adequately address those required architectural changes.

CONCLUSION AND GUIDANCE

This study has found that encrypted traffic and rising bandwidth requirements are having a negative impact on the efficacy of network security solutions. The impact is alarming and is already giving a growing army of sophisticated cybercriminals the ability to further capitalize on their attack campaigns. Financially motivated attackers have adopted tactics associated with nation-state espionage activity, including the ability to carry out multistaged attacks that support reconnaissance on their targets, capture sensitive information, and increase their persistence on corporate systems for an extended period of time.

The following guidance can help organizations proactively address the rising amount of SSL/TLS encrypted traffic:

- Assess your current visibility and SSL/TLS decryption efforts.
- Assess data loss prevention and other data protection solutions that require network visibility.
- Consider adopting a standalone SSL appliance or an ADC solution to support traffic inspection. The solution can get more value out of investments in specialized threat analysis and protection products: file analysis sandboxes, network sensors, and modern endpoint security solutions for the detection of targeted attacks and other threats.
- Consider your compliance obligations and ability to extend policy over decryption activity as well as capture logs and report on inspected traffic.

When evaluating potential solutions, IT teams should consider decryption products that support forward and explicit proxy configurations to support both inline and passive security solutions to inspect traffic. Solutions are available that provide more benefits than offloading SSL/TLS decryption. These solutions support traffic optimization efforts. The solutions should be able to integrate with a variety of third-party network security solutions and provide a measurable increase in performance of those appliances and security gateways. But technology is only one part of the equation. Policies enabling IT security to review SaaS adoption plans should be clearly communicated to all employees. In return, IT security should be clear about traffic inspection. Document and describe how privacy and regulatory concerns are being addressed.

METHODOLOGY

This study presents results from IDC's *State of SSL/TLS and Threat Visibility Survey* conducted in April 2016. Its premises and opinions are based on leveraging a combination of research sources, including:

- A survey of IT security managers and network and security architects representing 300 firms across the United States (The interviews were conducted in April 2016.)
- IDC's primary conducted research on SSL/TLS encryption, key management, and security
- Historical and current research through IDC customer and vendor surveys
- Monitoring information on the subject of SSL/TLS encryption reported in blogs, the press, and other online information sources

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data – Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2016 IDC. Reproduction without written permission is completely forbidden.