FORTINET

WHITE PAPER

# Encryption Is Now a Trojan Horse: Ignore It at Your Peril

## Executive Summary

**The game of leapfrog between hackers and data security professionals continues. No sooner do organizations start to feel secure with the latest encryption standards than cyber criminals find ways to violate that security. Black hats are infiltrating company networks by abusing encryption to shield their application-embedded malware and ransomware from detection. It's little wonder that 87% of CIOs feel that Secure Sockets Layer (SSL) encryption puts their organizations at greater risk of cyber threats.[1]**

**The zero-tolerance solution to such Trojan horses is to use SSL inspection to ferret out malicious code. But most inspection technologies available today put an untenable drag on network performance. Security professionals need a less-compromising way to resolve the trade-off between data security and application performance to capably support enterprise-wide digital transformation.**

**By 2030, organizations worldwide will have deployed 125 billion IoT devices.**

**This additional exposure creates more security risks.**

## Encryption Is Everywhere, for Better and for Worse

By some estimates, as much as 65% of global data traffic is now encrypted.[2] And while many still use the terms encryption and SSL synonymously, SSL's successor protocol, Transport Layer Security (TLS), is gradually gaining momentum; the Internet Engineering Task Force (IETF) recently approved TLS Version 1.3. In its latest transparency reports, Google refers only to TLS when it discusses encryption in transit.[3]

It is easy to see the imprint of digital transformation in the growing use of encryption. As a major component of data security, encryption has emboldened organizations to radically change the way they work, sell, communicate, and regulate their activities.

### Addressing Mobility and IoT Vulnerabilities

In years past, website developers used Hypertext Transfer Protocol (HTTP) for most webpages, reserving the encrypted Hypertext Transfer Protocol Secure (HTTPS) for pages that received or presented confidential data, such as credit card numbers, usernames, passwords, and other private information. Today, HTTPS is the norm for all pages on most websites.[4] Furthermore, according to NSS Labs, 75% of all web traffic will be encrypted by 2019.[5] A key driver behind the proliferation of encryption is web-user mobility. With most users accessing the Internet using mobile devices, any unencrypted web content is exposed on public networks. Those unencrypted pages not only reveal confidential personal information but also expose the entire URL and page content, including every page a user visited on a site, all search terms, and all content viewed.

Another source of vulnerability outside the walls of the enterprise is the web of connected devices known as the Internet of Things (IoT). IHS predicts that, worldwide, the number of IoT devices will jump 12% on average annually, from nearly 27 billion in 2017 to 125 billion in 2030.[6] Encryption adoption has been slower for these devices. Because they are limited in bandwidth, memory, and power resources, it is harder to deploy the full suite of encryption tools on the devices themselves. Nevertheless, the vulnerability of IoT devices (they are often deployed outdoors or in unsecured buildings) and their increasingly central role in critical infrastructure underscore the need for more robust solutions for this category.

### SaaS Subscribers and Providers Are Both on the Hook

The global cloud market is growing at an annual rate of 22% and is expected to account for more than 50% of all IT budgets by 2019.[7] Part of this investment will likely go to updating security for data in transit between on-premises networks and cloud providers. And this is not just a burden on enterprises. Software-as-a-Service (SaaS) providers have a stake in encryption, too, as their shared-responsibility models mandate protecting the data that their platforms transmit to subscribers, as well as the data at rest in their clouds.

### Encryption Is Compulsory for Compliance

Organizations across various industry segments are required to use encryption on certain types of sensitive data that is in transit, in order to remain in compliance with regulations such as PCI DSS (Payment Card Industry Data Security Standard) and HIPAA (Health Insurance Portability and Accountability Act). Regardless of the communications method (email, websites, SaaS applications, etc.), encryption is a requirement when data that is transmitted falls within the purview of these regulations.

### Email Users Flock to Encryption

A few years ago, Google started flagging unencrypted emails sent to Gmail users. In response, the number of inbound emails using SSL encryption increased by 25%.[8] As a result, 89% of inbound and 90% of outbound emails are encrypted on the Gmail network.[9] Yet, the encryption phenomenon extends beyond Gmail. In Europe, for example, end-to-end encrypted email providers Tutanota and ProtonMail have seen a sharp increase in adoption rates.[10]

The jury is in. Encryption is the new normal—so pervasively normal that complacency may be IT security's next biggest threat. As security professionals become more comfortable with the protection encryption offers, there is a real risk that they might not notice how this protection is quietly being subverted. The evidence lies deep in the packets, but not everyone is prepared to look.

**Because so much of the activity in a digitally transforming organization relies on the protection of data encryption, trust in encryption runs high.**

**And that's just what the bad guys are banking on.**


**90% of CIOs have experienced a network assault using SSL encryption.[14]**

## The Perils of Avoiding Packet Inspection

The unavoidable and uncomfortable truth is that what is good for security protectors is good for the criminals as well. A report from one application delivery vendor revealed that in August 2016, approximately 41% of cyberattacks used encryption to evade detection. By early 2017, that number had risen to more than 50%. Another company dealing in cloud security counted 600,000 malicious activities using SSL per day.[11]

Traditional cybersecurity solutions, such as intrusion detection systems (IDS) and intrusion prevention systems (IPS), are trained to trust encrypted traffic. Because encrypted traffic is considered "bottom of the barrel" in terms of inspection priority, criminals have begun using it as a Trojan horse, an unguarded entrance, to walk past the front door into the enterprise network.

Cyber criminals have found various ways to abuse encryption's defenses:

- **Hiding the initial infection.** Cyber criminals encrypt their malware and send it through an approved port; users click on embedded links that take them to sites containing the payload or as an attached file. Hackers have been able to hide the Zeus botnet, for instance, in SSL sessions.
- **Hiding command and control.** Certain malware families use encryption to hide command and control communications. One example of this, the Heartbleed exploit, takes advantage of SSL weaknesses to extract information from host servers, including private encryption keys, which they use to access encrypted communications.[12]
- **Hiding data exfiltration.** Many malware families also use encryption to hide network information such as passwords and stolen information (e.g., bank accounts and passwords).

Because of the potential payoffs for criminals, attacks via encrypte channels are reaching epidemic proportions. 90% of CIOs indicate they have experienced a network assault using SSL encryption.[13] It may seem logical to rely on digital certificates from trusted vendors as a means of preventing encryption abuse. However, obtaining legitimate certificates is easy and inexpensive—for good and bad actors alike. Certificates are bundled with many web browsers, and the cost of using them on a website ranges from free to a few hundred dollars per year. Moreover, cyber criminals are becoming increasingly adept at stealing certificate keys that allow them to encrypt malicious emails, websites, and applications typically tagged to a whitelist. In both these instances, IDS and IPS may identify them as valid due to the identity of the certificate.

## Why Security Pros Hold Back on Inspection

Currently, security architects face a conundrum in trying to address the growing encryption problem. In theory, businesses can implement SSL inspection at network entry points. But many organizations have been hesitant to take that step. Reasons vary, but they can be divided broadly into two cases: lack of inspection tools and reluctance to employ them, primarily due to performance concerns.

### When Inspection Loses Ground to Other IT Priorities

As noted above, security professionals sometimes trust encryption to the point of downplaying its vulnerabilities. Even when they are aware of the danger, however, other needs take precedence over investing in SSL inspection capabilities. The security team is already burdened with keeping up with evolving encryption standards and managing digital certificates. Thus, inspection may seem like one task too many.

Moreover, digital transformation and increasing pressure to trim operating costs are driving IT leaders to reduce their data-center footprints. Consequently, they are scrutinizing all new hardware investments more heavily. New hardware purchased for SSL inspection capabilities often does not make the cut.

### When Inspection Is Turned Off

Among enterprises with inspection capabilities, many have chosen not to enable them or have turned them off after a period of use. So, what is holding them back? One of the primary factors is the performance impact to their networks. Studies show that when SSL/TLS traffic inspection is enabled, performance can be impacted by nearly 75%.[15] Couple this with the growing enterprise investment for high-speed Ethernet and increased demand for WAN bandwidth,[16] and it makes a lot of sense that many IT security leaders have been reluctant to activate packet inspection. Inspection would have a detrimental impact not only on traffic throughput and inspection performance, but also on user productivity.

Decryption and inspection can also increase the complexity of managing network security by introducing additional hardware and software to manage as well as new security policies and workflows. Organizations need to develop and maintain whitelists, build and manage rules, and resolve false positives. But this is a problem, as many security solutions do not actively manage whitelists, and their management becomes a huge overhead.

Certain websites enable HTTP Public Key Pinning to prevent man-in-the-middle attacks. However, several things can go wrong. Certificate authorities can change their issuance practices without notice, and new certificates may not use the same chain of trust as old ones. If the new certificate chain no longer includes the pinned keys, the website will not be accessible until the HTTP Public Key Pinning policy expires. Mistakes or oversights could result in a business being without a website for weeks or months. With more than 75% of enterprises managing 10 to 19 SSL certificate keys, this is a widespread concern.[18]

**SSL/TLS traffic inspection can cause early 75% degradation in network performance.[17]**

**More than 75% of enterprises manage 10 to 19 SSL certificate keys.[19]**

**Average cost of a cybersecurity breach: $7.35 million[22]**

## Inspection Quality: An Urgent Concern

With the average cost of a cybersecurity breach now pinned at $7.35 million, enterprises need to pay heed.[20] Encryption is at a critical crossroads for protection and hacking. Organizations without an encryption strategy are at much greater risk of cyber threats. And it is not simply encrypting email, websites, and applications. Because bad actors are tapping encryption to execute over half of their attacks, a number that will continue to rise,[21] enterprises must simultaneously have a decryption and inspection strategy.

The tradeoff between SSL inspection and application performance does not have to be a fact of life. Solving this problem requires devoting technology and development resources to the engine that drives inspection. Some vendors offer point solutions that rely on off-the-shelf components. An attractive upfront price tag belies the cost of owning such devices when one factors in the real-world demands of expanding traffic volumes, advanced threat protection requirements, and security staffing constraints. Organizations that need to deliver secure data at the pace of digital business should make SSL inspection quality a higher priority.

[1] Brian Barrett, "Most Top Websites Still Don't Use a Basic Security Feature," WIRED, March 17, 2016.

[2] Siggi Stefnisson, "Private, But Not Secure: HTTPS is Hiding Cybercrime," SecurityWeek, September 22, 2017.

[3] Google Transparency Report, accessed March 2018.

[4] "Threat Landscape Report Q4 2017," Fortinet, February 12, 2018.

[5] "NSS Predicts 75% of Web Traffic Will Be Encrypted by 2019," NSS Labs, November 9, 2016.

[6] Jenalea Howell, "Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says," October 24, 2017.

[7] Fredric Paul, "Cloud to consume almost half of IT infrastructure sales by 2019," Network World, July 7, 2015.

[8] Ashley Carman, "Gmail's encryption warning spurs 25 percent increase in encrypted inbound emails," The Verge, March 24, 2016.

[9] Google Transparency Report, accessed March 2018.

[10] Natasha Lomas, "Another European e2e encrypted Gmail alternative reports rising signups," TechCrunch, March 23, 2017.

[11] Eva Hanscom, "Most Cyber Attacks Now Use Encryption: Are You Prepared for the Good, the Bad and the Ugly?" Venafi Blog, March 22, 2017.

[12] Ananda Rajagopal, "How SSL encryption gives a false sense of security," CSO, accessed April 2, 2018.

[13] Jai Vijayan, "When Encryption Becomes The Enemy's Best Friend," Dark Reading, March 5, 2016.

[14] Ibid.

[15] "NSS Labs Research Finds SSL Traffic Causes Significant Performance Problems for Next Generation Firewalls," NSS Labs, June 12, 2013.

[16] Stan Gibson, "2018 State of Infrastructure," InteropITX, accessed April 12, 2018.

[17] "NSS Labs Research Finds SSL Traffic Causes Significant Performance Problems for Next Generation Firewalls," NSS Labs, June 12, 2013.

[18] Robert Westervelt, "The Blind State of Rising SSL/TLS Traffic: Are Your Cyber Threats Visible?" IDC, July 2016.

[19] Ibid.

[20] "2017 Cost of Data Breach Study: United States," Ponemon Institute, June 2017.

[21] Ibid.

[22] "Threat Landscape Report Q4 2017," Fortinet, February 12, 2018.





September 18, 2019 11:42 PM

485412-0-0-EN

D:\Fortinet\White Paper\Refresh - Trojan Horse\wp-encryption-is-now-a-trojan-horse-v3