

CONTROL

EFFICIENCY

ROOTKITS

PHISHING

THINK APP SECURITY FIRST

# INCREASE VISIBILITY TO BOOST SECURITY

PROTECT YOUR APPS BY ORCHESTRATING YOUR SSL TRAFFIC

FLEXIBILITY

SPYWARE



WE MAKE APPS  SAFER

# INTRODUCTION

We are moving very quickly toward an Internet where nearly every piece of data in transit will be encrypted.

Not long ago, the Secure Sockets Layer (SSL), or Transport Layer Security (TLS), was used almost exclusively by government agencies and large financial institutions. Today, however, it has become increasingly important for organizations of all kinds to protect the data transmitted through countless sites and applications.

The rise of SSL/TLS has also been sped by regulatory standards such as PCI DSS, HIPAA, and the EU's General Data Protection Regulation (GDPR), which require that transmitted data be encrypted. Moreover, organizations have been spurred to adopt SSL/TLS by Google search results policy, which gives preferential treatment to sites that encrypt.

According to research by F5 Labs, more than 81% of all web page loads are now encrypted with SSL/TLS, which means that we are moving very quickly toward an Internet where nearly every piece of data in transit will be encrypted.<sup>1</sup> However, the rise of SSL/TLS isn't all good news. Attackers are increasingly hiding insidious attacks within encrypted traffic—which means that the security protocol itself has become a threat vector. Regaining visibility into that encrypted traffic is one of the most important steps you can take to protect your apps, your data, and your business.

<sup>1</sup> [https://www.f5.com/content/dam/f5/f5-labs/articles/20180423\\_tls\\_2017/2017\\_TLS\\_Telemetry\\_Report.pdf](https://www.f5.com/content/dam/f5/f5-labs/articles/20180423_tls_2017/2017_TLS_Telemetry_Report.pdf)

<sup>2</sup> <https://www.searchenginejournal.com/chrome-browser-https/253801/>



# 10/2018

BEGINNING IN OCTOBER 2018, GOOGLE CHROME WILL HIGHLIGHT ALL HTTP SITES AS "NOT SECURE" IN ITS URL BAR.<sup>2</sup>

## THE SSL/TLS ADOPTION JOURNEY

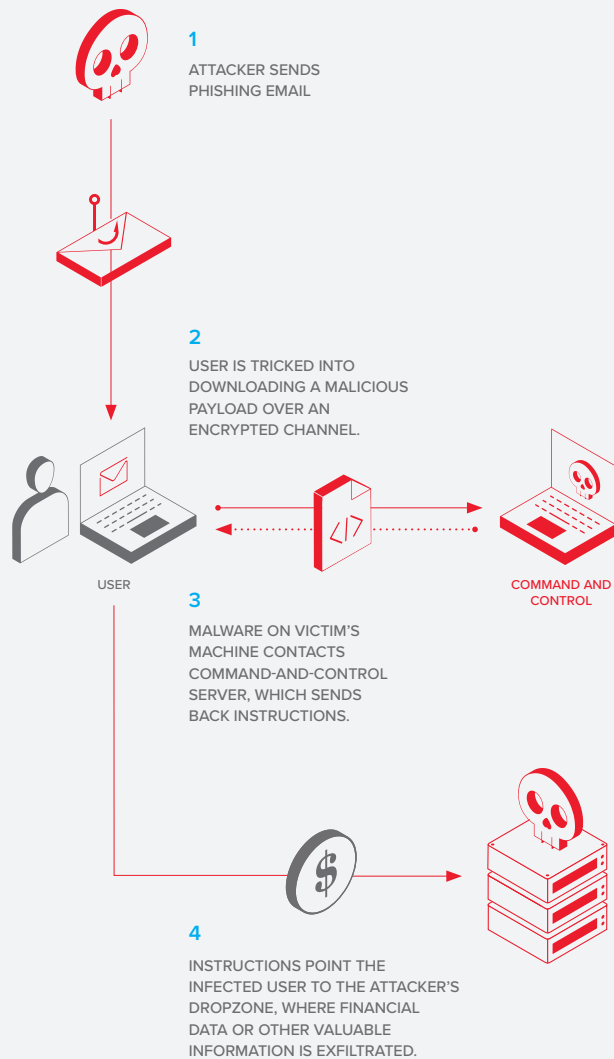
The preferred SSL/TLS protocol version is the broadest indicator of the cryptographic posture of hosts across the Internet.

Today, that favored protocol version is undeniably TLS 1.2. The latest data from F5 Labs shows that TLS 1.2 is preferred by 89% of Internet at-large hosts.<sup>3</sup> Preference for the older SSL v3—mortally damaged by the POODLE vulnerability in 2014—still hovers at around 10%.

Adoption of the newer TLS 1.3 protocol has been slow due largely to the fact that there isn't—yet—a compelling security reason to abandon TLS 1.2.<sup>4</sup>

<sup>3</sup> [https://www.f5.com/content/dam/f5/f5-labs/articles/20180423\\_tls\\_2017/2017\\_TLS\\_Telemetry\\_Report.pdf](https://www.f5.com/content/dam/f5/f5-labs/articles/20180423_tls_2017/2017_TLS_Telemetry_Report.pdf)

<sup>4</sup> [https://www.f5.com/content/dam/f5/f5-labs/articles/20180423\\_tls\\_2017/2017\\_TLS\\_Telemetry\\_Report.pdf](https://www.f5.com/content/dam/f5/f5-labs/articles/20180423_tls_2017/2017_TLS_Telemetry_Report.pdf)



### COMMON ATTACK PATH OF A DATA BREACH

Phishing is one of the more popular attack scenarios. Free and low-cost HTTPS certificate providers make it easier for attackers to infiltrate malware and exfiltrate stolen assets.

## HIDDEN MALWARE: THE THREAT YOU CAN'T SEE

Cybercriminals use malware such as spyware, ransomware, and rootkits to compromise your applications and steal personal data. In fact, in 2018, 30% of all data breaches involved some form of malware according to the Verizon 2018 Data Breach Investigations Report.<sup>5</sup> In addition to being used by criminal organizations for financial gain, malware is increasingly employed by state-sponsored entities for disruptive purposes or espionage.

Malware is one of the most serious threats to the enterprise, and can lead to financial losses, reputation damage, service disruption, and data breaches. Compounding the problem is the fact that any time your users access an infected website or click on a malicious attachment in a phishing email, they may pick up a nasty piece of malware.

This problem isn't new. Over the years, we've come up with many tools that can detect or block malware and malicious traffic. Organizations deploy technologies such as next-generation firewalls to watch user behavior, sandboxes to find zero-day exploits, intrusion protection systems (IPS) to block malicious payloads, data loss prevention (DLP) scanners to prevent data exfiltration, and web gateway services to secure inbound and outbound traffic. These solutions evolved over the years and

became adept at preventing malware from infecting users' systems and compromising applications.

However, the rise of encryption has created an opportunity for attackers—and a headache for network administrators protecting their apps. Although SSL/TLS protects data in transit, it can also function as a tunnel that attackers use to hide malware from your security devices. Encrypted traffic cannot be seen as cleartext by these security devices, so it is passed through without being inspected, creating blind spots in your security. However, using the native decryption support of your security inspection devices—if they even offer it—can seriously degrade their performance (by a mean average of 81% according to the NSS Labs report *SSL Performance Problems*).<sup>6</sup> So, the very devices that are designed to detect malware can't do it effectively if that malware is hidden within encrypted traffic—something attackers understand all too well.

If you want to keep your apps, your data, and your organization protected against malware, you can't afford to not decrypt outbound traffic. The question remains: what's the best way to gain visibility into that encrypted traffic, without adversely affecting the performance of your apps?

<sup>5</sup> [https://www.verizonenterprise.com/resources/reports/rp\\_DBIR\\_2018\\_Report\\_en\\_xq.pdf](https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xq.pdf)

<sup>6</sup> <https://www.nssllabs.com/linkservid/13C7BD87-5056-9046-93FB-736663C0B07A/>



## KNOW YOUR OPTIONS

# CHOOSING A PROTECTION STRATEGY

The growth of SSL/TLS traffic has forced organizations to architect efficient solutions that allow their network and their apps to respond to the increased demands of ubiquitous encryption. You seemingly have a few options—but only one of them is actually worthwhile.



### DO NOTHING

Many organizations allow their malware-scanning and prevention devices to inspect whatever cleartext traffic they can, while praying to avoid any malware hidden in encrypted traffic. However, as attackers are increasingly concealing their malicious code in traffic that security devices can't see, the do-nothing option is more and more a recipe for disaster.



### DEPLOY A DECRYPTION AIR GAP

Some security teams use a decryption “air gap,” where they decrypt inbound and outbound traffic before passing it through a daisy chain of security inspection devices and then re-encrypting it.

This solution at least uncovers the hidden malware, which means that security controls can find it. However, it typically creates a red zone where user passwords are transmitted in the clear. A typical air gap also suffers from total outages when in-line security devices fail.



### ORCHESTRATE!

By applying policy-based decryption and traffic steering to both your inbound and outbound traffic, you can conduct your orchestra of security devices like Herbert von Karajan. A high-performing SSL/TLS orchestration solution improves visibility and protects your apps while increasing the security, efficiency, and resilience of your security stack.

Here's how it works: outbound traffic flows into your SSL/TLS orchestration device, which decrypts it. Then, based on a set of customizable rules (such as user or device profile), the unencrypted traffic passes directly to the associated chain of security devices. Traffic is scanned and cleared by the security devices and it goes back to the SSL/TLS orchestration device, which re-encrypts it and sends it on its way.



## HIGH-PERFORMANCE SSL/TLS ORCHESTRATION

By orchestrating your SSL/TLS traffic, you can maximize the efficiency of your security solutions while optimizing the performance of critical applications.

## THE BENEFITS OF ORCHESTRATION

It's clear that visibility into encrypted traffic is key to protecting your applications and securing your data. An SSL/TLS orchestration solution can provide high-performance decryption and encryption of outbound TLS traffic—without slowing your traffic down.



### VISIBILITY INTO ENCRYPTED TRAFFIC

With a robust SSL/TLS solution, you get decryption and re-encryption, as well strong cipher support, all of which allows you to see what's going on in your encrypted outbound traffic.



### MORE FLEXIBILITY

A solution with a full-proxy architecture gives you more control over, and more flexibility with, different ciphers on either side of the application stack. It also allows you to monitor and load balance your security devices to ensure that they're functioning at peak efficiency. You can even skip a device entirely in case of failure, which adds resiliency to your network.



### EFFICIENT DYNAMIC SERVICE CHAINING

Perhaps the biggest benefit of orchestrating your SSL/TLS traffic is the idea of dynamic service chaining, which makes it easy to categorize traffic to intelligently route it to or around inspection devices based on a number of different factors, including the role of specific users. You can dynamically assign, chain together, and reuse security services on the fly.

This means that you can drive different types of traffic through different security devices, and reuse those devices in different chains—or not use them at all. Dynamic service chaining allows you to scale your SSL/TLS solution, and maximize the usage of your current security devices, by letting them concentrate on the areas in which they can best protect your organization.



### BETTER PERFORMANCE

There's only one decrypt/re-encrypt process rather than several, and it's carried out by a high-performance orchestration device that is built for just that purpose.



### CENTRALIZED MANAGEMENT

By choosing an SSL/TLS solution that provides for centralized management, you can simplify the process of choosing and updating the cipher suites that help secure network connections using SSL/TLS. This drives better performance of your traffic inspection security tools, while allowing greater flexibility in managing the ciphers you use in end-to-end encryption.

# KEY CONSIDERATIONS WHEN ADOPTING AN SSL/TLS STRATEGY

## VISIBILITY AND CONTROL

- Neutralize malware with SSL intercept
- Steer traffic according to classification policy
- Increase cipher agility

## DATA PROTECTION AND PRIVACY


- Choose a data-protection strategy
- Meet or exceed expectations for modern data protection regulations
- Ensure confidentiality of health and financial info

## KEY MANAGEMENT

- Keep high-value keys safe
- Manage SSL certificates efficiently
- Employ SSL offload and transformation







IT'S ESSENTIAL TO REGAIN  
VISIBILITY INTO ENCRYPTED  
TRAFFIC TO PROTECT YOUR APPS  
AND YOUR NETWORK.

## CONCLUSION

The increase of SSL/TLS traffic indicates that organizations are more and more focused on safeguarding the integrity of the data that flows through their Internet-facing applications.

However, the concurrent growth of malware hidden within that encrypted traffic is cause for concern. Without visibility into your SSL/TLS traffic, you'll have some serious blind spots in your security, and these blind spots could lead to financial losses, data breaches, and damage to your corporate reputation.

That's why it's essential to regain visibility into that encrypted traffic and allow your malware-scanning and prevention devices to protect your apps and your network. The most efficient way to get that visibility is by orchestrating your outbound SSL/TLS traffic. With a robust SSL/TLS orchestration solution, you'll enjoy better visibility, increased performance, and more flexibility—so you can stop worrying about hidden malware and focus on developing and supporting new apps to drive your business.

For more information about orchestrating your SSL/TLS traffic, visit <https://www.f5.com/products/security/ssl-orchestrator>.



## THINK APP SECURITY FIRST

Always-on, always-connected apps can help power and transform your business—but they can also act as gateways to data beyond the protections of your firewalls. With most attacks happening at the app level, protecting the capabilities that drive your business means protecting the apps that make them happen.



US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: [info@f5.com](mailto:info@f5.com) // Asia-Pacific: [apacinfo@f5.com](mailto:apacinfo@f5.com) // Europe/Middle East/Africa: [emeainfo@f5.com](mailto:emeainfo@f5.com) // Japan: [f5j-info@f5.com](mailto:f5j-info@f5.com)

©2018 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at [f5.com](http://f5.com).

Any other products, services, or company names referenced herein may be trademarks of the respective owners with no endorsement or affiliation, expressed or implied, claimed by F5. EBOOK-SEC-242467703 09/18