DEFENDING THE DIGITAL ENTERPRISE

Seven things you need to improve security in a world dominated by encryption.

Use of Encryption Is on the Rise

Transport Layer Security (TLS), the de facto standard for websites, is now increasingly used for internal network traffic.

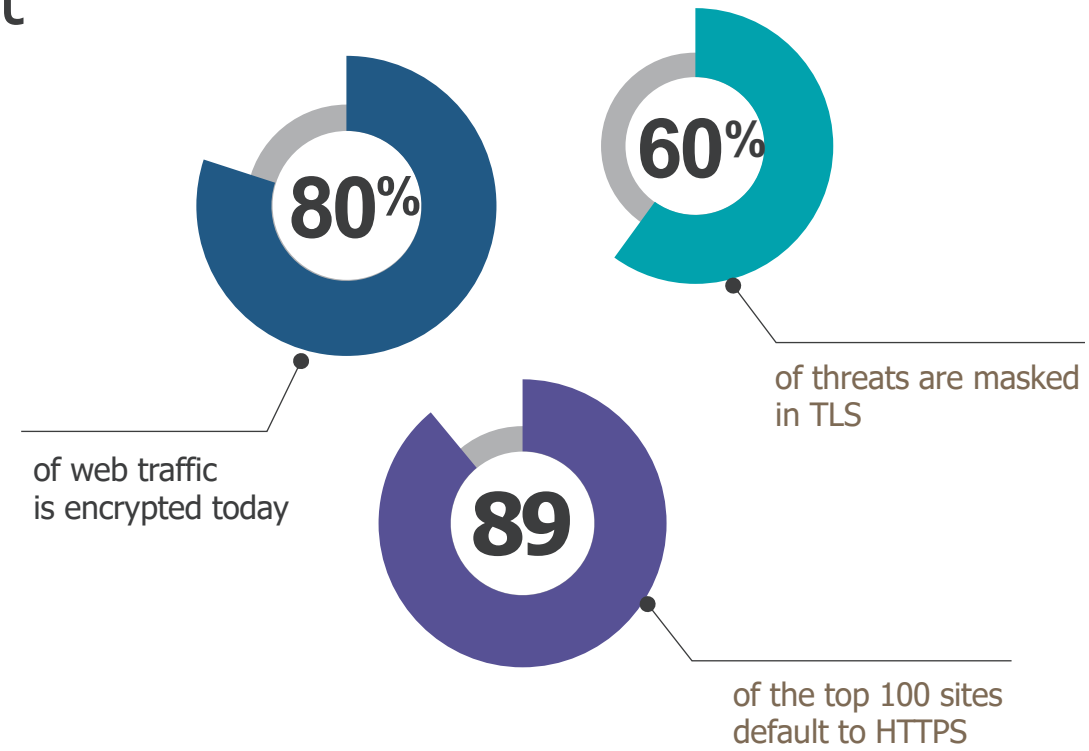
Enterprises are deploying more and more software to private and public clouds and making wider use of SaaS applications.

Attacks Through SSL/TLS

Threat actors are increasingly exploiting SSL/TLS sessions to:

- ✓ Conceal malware
- ✓ Mask command-and-control traffic
- ✓ Cloak the exfiltration of stolen data
- ✓ Disguise DDoS attacks

Decrypt and Inspect

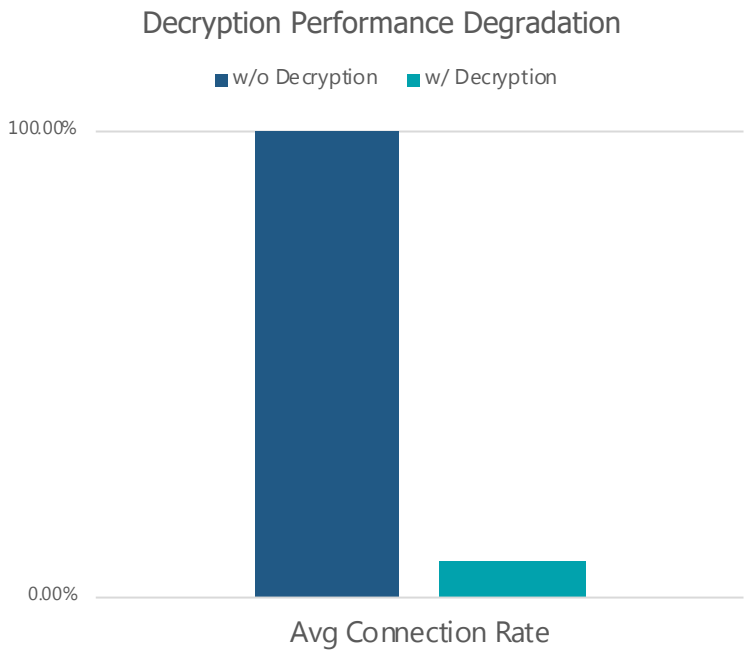


Eliminating Blind Spots

As the volume of SSL/TLS encrypted traffic rises exponentially, organizations become even more vulnerable to attacks.

Operations teams must have visibility into encrypted traffic for analysis.

Scaling the Security Stack

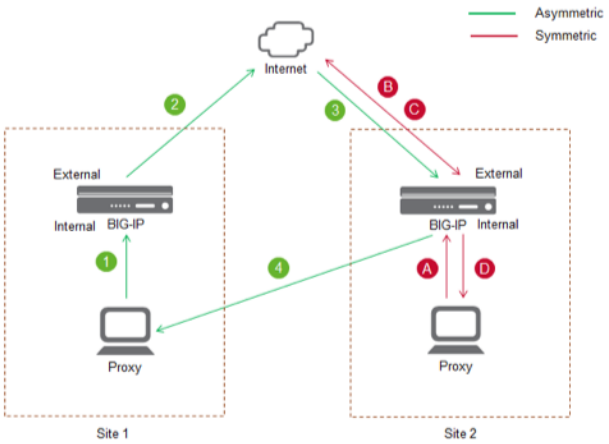


Security and analytics tools struggle to keep up with decryption.

Offloading decryption to a centralized platform ensures security tools focus on what they were designed for: detection and mitigation of malware.

Seven

Do's for SSL/TLS Decryption



Seven Things You Need to Do Now

1. Get to know your traffic

Before deploying any SSL/TLS decryption solution, be aware of your total volume of network traffic and how much of it is SSL/TLS encrypted.

Know how and where your traffic is traversing the network. For an SSL/TLS solution to work effectively, it needs to see both directions of traffic.

Asymmetric traffic can cause incomplete decryption if all traffic is not combined and fed to the solution.

2. Inbound vs. outbound

It's important to know which traffic needs to be decrypted.

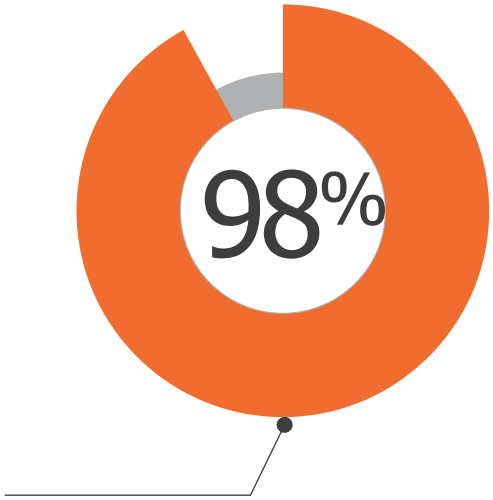
Either you're hosting on-premises web apps, internally or externally, or you want to decrypt all the traffic leaving your network.

Each case requires different techniques.

In the first scenario, you'll need a private key for decryption; for outbound traffic only, you'll need to use man-in-the-middle (MITM) decryption.

Seven

Do's for SSL/TLS Decryption



drop in average connection rate of products running SSL/TLS

Seven Things You Need to Do Now

3. Understand limits

Different solutions offer different SSL/TLS decryption capacity for inbound or outbound traffic.

It's important to know how much traffic can be decrypted by a solution based on the active number of connections and volume of SSL/TLS traffic.

4. Define the need

Once you have traffic decrypted, where do you need to steer that traffic?

Does just one tool need to see decrypted traffic, or multiple tools?

5. Prioritize

Many security tools and firewalls offer an SSL/TLS decryption solution that sometimes impairs their primary function.

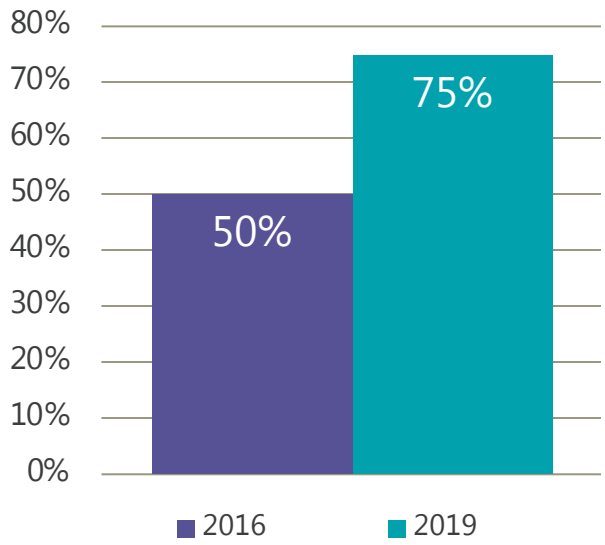
In these cases, enabling SSL/TLS decryption can cause high CPU usage which degrades the tool's ability to inspect or block traffic.

According to NSS Labs Test Reports, there is a 92 percent drop in average connection rate of products performing SSL/TLS decryption, with connection degradation from 84 percent to 99 percent.[1]

1. NSS Labs. "*NSS Labs Expands 2018 NGFW Group Test with SSL/TLS Security and Performance Test Reports.*" AP News. July 24, 2018.

Seven

Do's for SSL/TLS Decryption



Encrypted web traffic increased 25 percent between 2016 and 2019[1].

[1] NSS Labs. "TLS/SSL: *Where Are We Today?*." October 2016.

6. Anticipate growth

SSL/TLS decryption may be easy to configure for your current setup, but what happens if your traffic volume grows?

How easy it would be to scale your SSL/TLS decryption solution over time? What would be the cost impact?

7. Measure twice, cut once

Do your research. Different solutions offer varied performance with different ciphers.

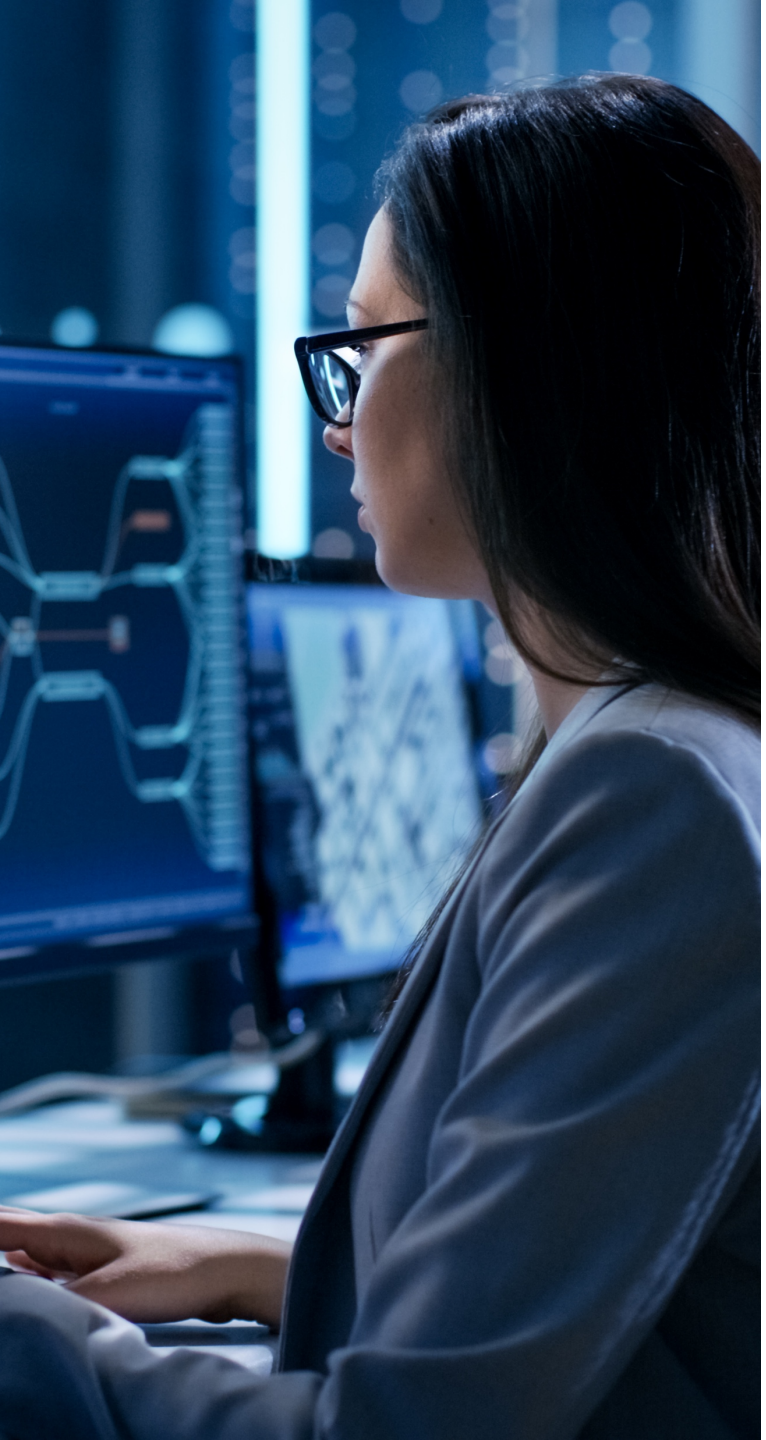
Some solutions are easier to deploy or scale better than others.

Thoroughly research available solutions and their pros and cons.

Simplify Your Operations

Use a next-generation network packet broker to get the operational simplicity of centralized decryption and distribution to multiple inline security tools prior to re-encrypting the traffic.

To see a demo and learn what Gigamon can do for you, check out www.gigamon.com/ssl-tls.



Why Gigamon?

Gigamon enables organizations to run fast, stay secure and innovate in the digital economy by providing complete visibility and intelligence on all data in motion across their hybrid cloud network.

The numbers below highlight the Gigamon journey that started in 2004. Since then, we've been awarded over 60 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organizations around the world.

#1 in Market Share

7 of 10 Global Banks

83 of the Fortune 100

8 of 10 Top Tech Companies

3000+ Customers

10 of 10 Top Government Agencies

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA +1 (408) 831-4000
www.gigamon.com