5 STEPS TO ENHANCE YOUR ENTERPRISE SECURITY

WITH HIGH PERFORMANCE SSL/TLS DECRYPTION

TABLE OF CONTENTS

INTRODUCTION: IT'S ALL ABOUT THE DECRYPTION

The risks and benefits associated with encryption are well understood. On the one hand, everyone acknowledges that encrypting connections helps protect data from eavesdroppers, man-in-the-middle attacks, and would-be hijackers while ensuring the ongoing integrity and privacy of those communications. On the other hand, there is a general understanding that hackers are increasingly taking advantage of this encryption to hide what they are doing.

Year over year, encrypted traffic continues to increase, with the latest data showing **85% of the internet in North America is encrypted**. This gives cybercriminals a large blind spot to spread malware undetected. It is predicted that as much as **70% of cyberattacks** will use encryption as part of their delivery mechanism by 2019. For example, **Yahoo!**, which saw around 6.9 billion monthly page views on its main site alone in 2015, was the target of a scheme that used HTTPS-protected URLs to deliver infected traffic at the network layer.

Your legacy security infrastructure is not built to take care of these types of evolved hidden attacks, and **almost two-thirds of organizations** are not able to decrypt and inspect their SSL/TLS traffic.

Cybercriminals can use encryption to hide both the delivery of malware as well as the extraction of data, which leaves your legacy Data Loss Prevention (DLP) systems blind to such data breaches. Breaches can have a disastrous impact on your company's reputation, brand, and stock value, and subject you to disciplinary action and strict fines.

COUNTRIES AFFECTED INITIALLY BY THE WANNACRY RANSOMWARE ATTACK

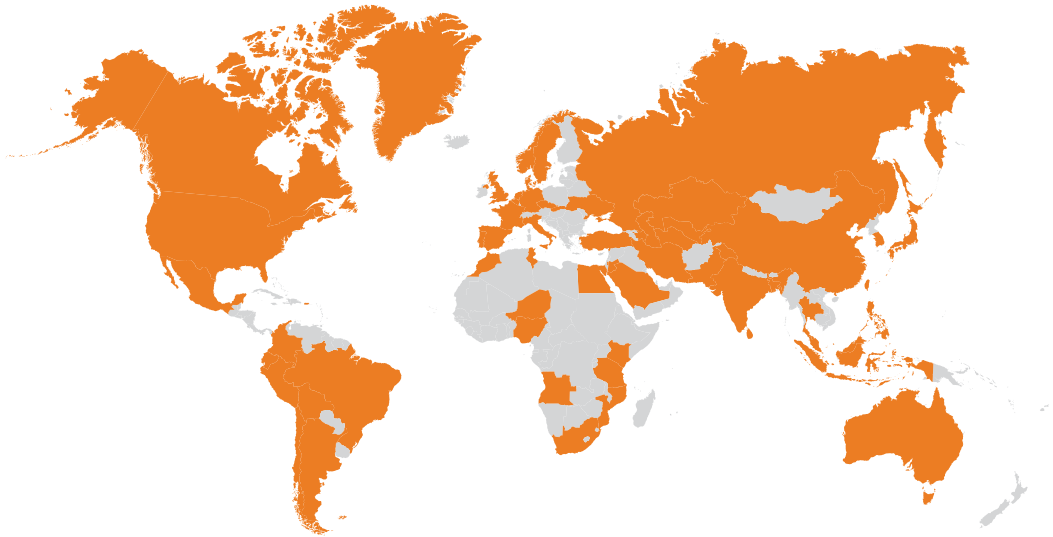


Figure 1. Countries Affected Initially by the WannaCry Ransomware Attack[1]

► 1. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

In last year's WannaCry ransomware attack, more than 200,000 computers worldwide, including those used by healthcare organizations, were affected. Most notably, this attack affected Britain's National Health Service (NHS), causing serious disruptions in the delivery of health services across Britain.

Besides understanding what is hiding in all this encrypted traffic, you also need to ensure your company is enforcing security and regulatory compliance for current and future standards, rules and regulations. Your job is becoming even more complex.

You need an easy-to-use, fast, and versatile inspection technology that will give you full visibility into your encrypted traffic without performance degradation from your existing security devices while ensuring compliance.

How can you accomplish this? In the following 5 steps, you will see how you can improve your enterprise security, help you meet regulatory compliance, and maximize your security performance and ROI.

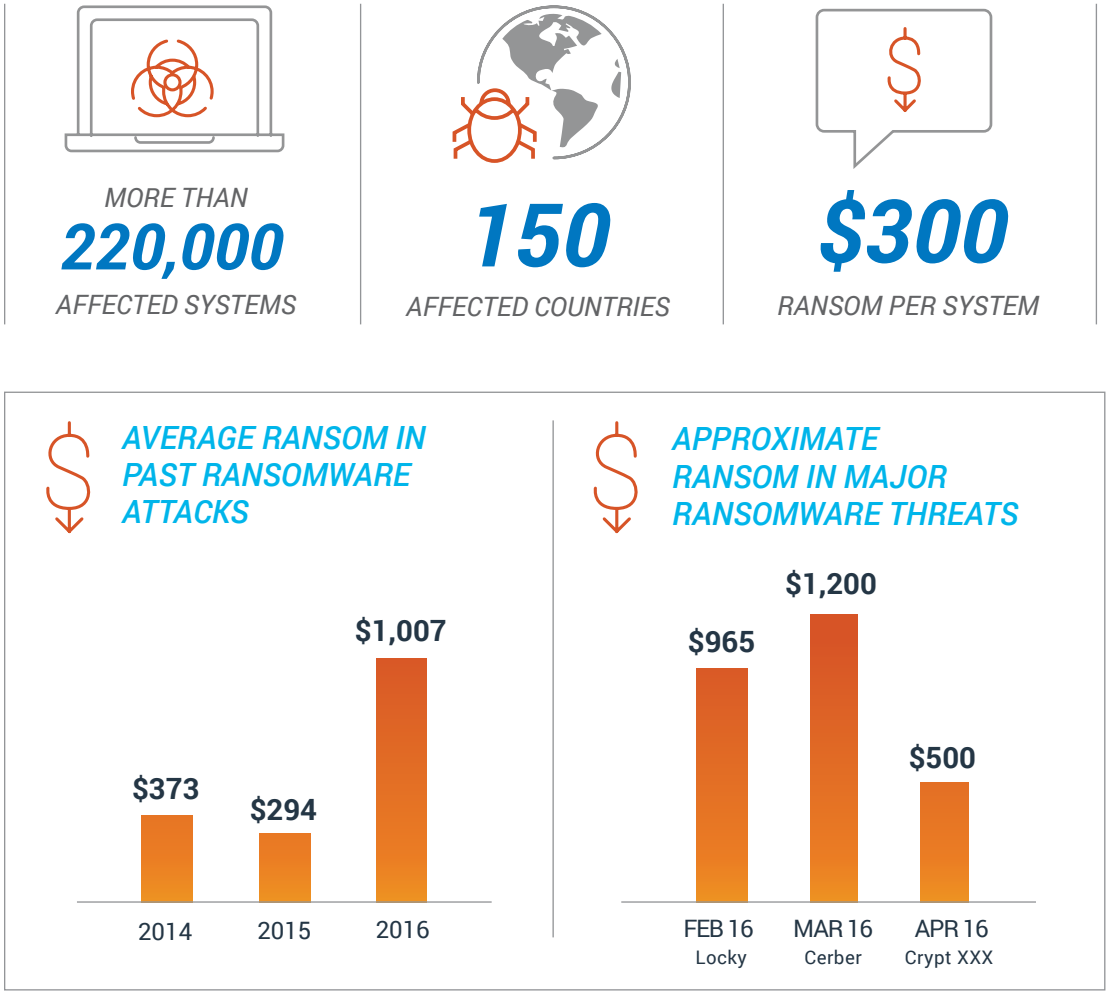


Figure 2. Impact of WannaCry Ransom Attack[2]

► 2. https://www.statista.com/chart/9399/wannacry-cyber-attack-in-numbers/

1 DEFEND AGAINST CYBERATTACKS WITH FULL VISIBILITY INTO ENCRYPTED TRAFFIC

Growth in encrypted traffic, coupled with increasing SSL key lengths and more computationally complex ciphers, makes it difficult for firewalls and other security solutions to scale their decryption and inspection of SSL/TLS traffic. As a result, **many organizations do not have the capacity to scan all encrypted content**, leaving you blind to the threats that may be hidden in that traffic.

You need to invest into a purpose-built, dedicated decryption solution that gives you full visibility into the SSL/TLS blind spot, enabling your existing security infrastructure to protect your assets against encrypted cyberattacks, without the need for costly upgrades.

An effective decryption solution needs to be flexible in many ways, including having the ability to:

- Decrypt traffic across multiple ports and protocols so that attacks using non-standard ports can be stopped.
- Deliver high performance decryption with 2048-bit and 4096-bit key sizes.
- Support most, if not all, modern cipher suites, including Elliptical-Curve Cryptography (ECC) for perfect forward secrecy (PFS) support.
- Maintain full control over the cipher negotiation process so that no weak or deprecated ciphers are ever used.
- Ensure full and continued protection, even if new ciphers or TLS versions are introduced into the network without prior notice.

A10 VIDEO

THE BENEFITS OF A FULL PROXY SSLI ARCHITECTURE

WATCH IT NOW

2 DETECT DATA BREACHES WHILE ENFORCING SECURITY AND REGULATORY COMPLIANCE

In a study by **Ponemon Institute**, 36 percent of surveyed organizations said compliance/regulatory failure was a major factor in justifying funding for their IT security budgets. But while they see compliance as important, 58 percent of US companies lack confidence in their ability to comply with the European Union's General Data Protection Regulation (GDPR). Forrester Research also **recently reported** that as many as "80 percent of companies will fail to comply with GDPR."

For healthcare providers compliance is a must. Failure to comply with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rules can put patients' health information at risk.

To help you ensure your security deployment meets your regulatory compliance with the continually evolving data protection and privacy standards, rules, and regulations, your decryption solution needs to provide you with granular control, to specify which SSL/TLS traffic needs to be decrypted and inspected and which needs to be bypassed. For instance, your decryption solution needs to have a URL classification service that classifies and maintains millions of domains in multiple categories to selectively bypass traffic so that private or sensitive data (e.g., medical or financial) is not decrypted in adherence with your specific compliance standards, such as the HIPAA Privacy Rules.

CONFIDENCE IN ORGANIZATIONS' ABILITY TO COMPLY WITH THE EU GDPR

1 = low ability to 10 = high ability, 7+ responses reported

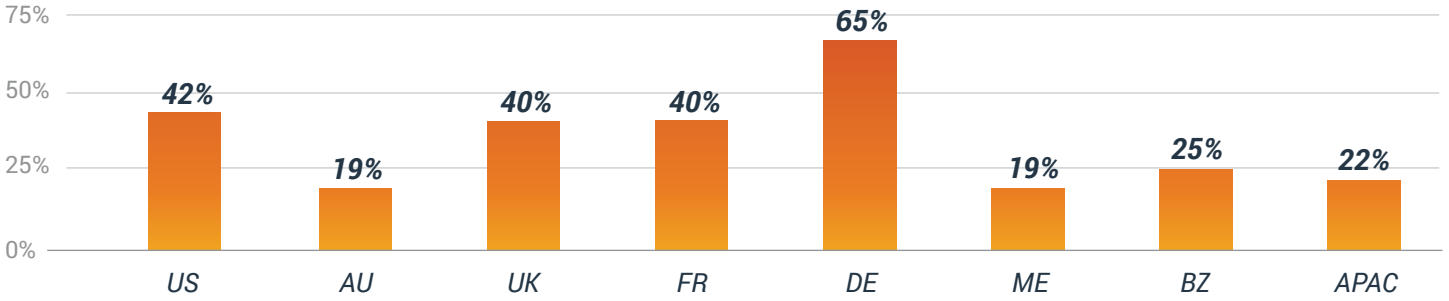


Figure 3. Confidence in organizations' ability to comply with the EU GDPR[3]

► 3. https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2018_Cyber_Resilient_Organization_Study.pdf

3 DELIVER RELIABLE, FAST, AND VERSATILE SSL DECRYPTION WHILE MAXIMIZING PERFORMANCE

Turning on SSL/TLS inspection often severely degrades the performance of legacy security devices, such as next generation firewalls (NGFW). NSS Labs looked at how much performance was impacted in their **2018 SSL/TLS Performance Tests**.

When measuring product performance with a NGFW with SSL/TLS turned on versus turned off, NSS Labs found significant performance degradation and increased latency in the tested products.

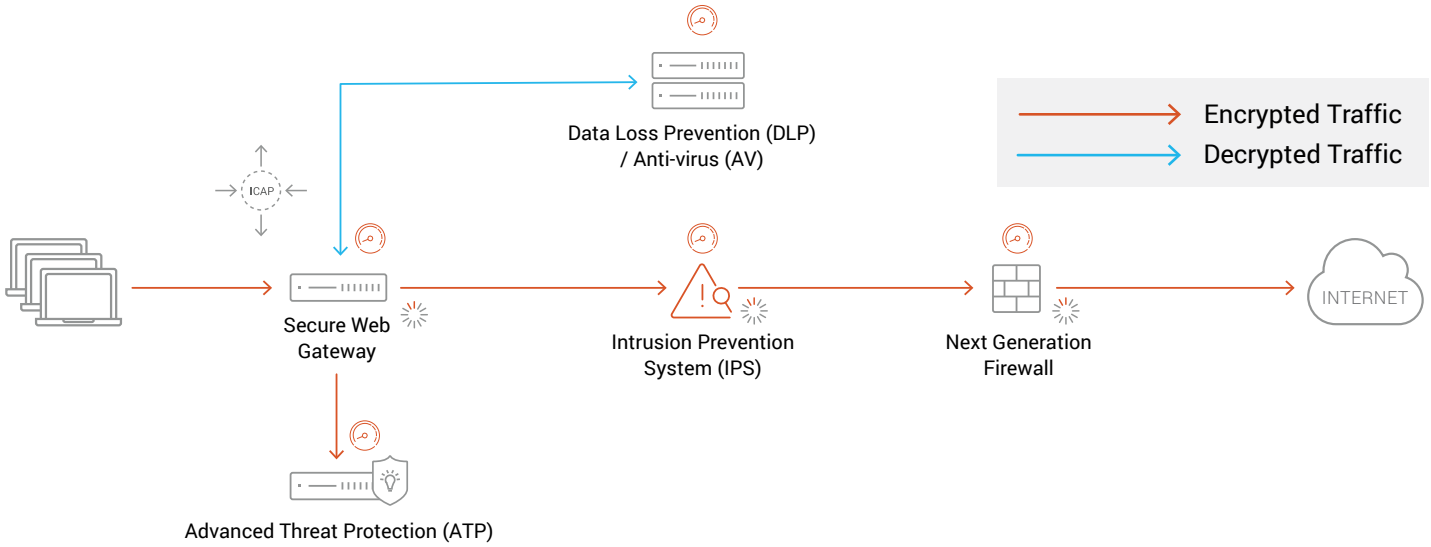
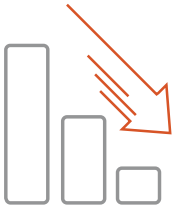


Figure 4. Your legacy security devices remain blind to threats that are delivered using the cover of encryption.

Because most legacy security solutions are not able to send decrypted traffic to other devices, each device must decrypt, inspect, and re-encrypt traffic before sending it to the next device in the security stack.

This results in a lot of wasted time, cost, and effort. And the more devices in your network stack, the more latency that is introduced. **Gartner believes that by 2020 more than 60 percent of organizations will fail to decrypt HTTPS traffic efficiently**, missing most targeted web malware.

With a purpose-built and dedicated hardware-based decryption solution, you can avoid creating network bottlenecks due to performance degradation. Such solutions need to provide real-time decryption at high speeds. They also need to adhere to the "decrypt once inspect many times" approach of decryption, enabling your entire security infrastructure to maintain optimal performance.



60%

DROP

IN THE AVERAGE THROUGHPUT

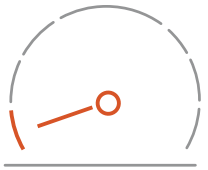
Throughput degradation ranged from 13% to 95%[4]

92%

DROP

IN THE AVERAGE CONNECTION RATE

Connection degradation ranged from 84% to 99%[3]



672%

INCREASE IN LATENCY

IN THE AVERAGE APPLICATION RESPONSE TIME

Latency ranged from 99% to 2,910%[3]

4. https://www.nsslabs.com/company/news/press-releases/nss-labs-expands-2018-ngfw-group-test-with-ssl-tls-security-and-performance-test-reports/

4 MAXIMIZE THE ROI OF YOUR EXISTING SECURITY INFRASTRUCTURE

Security devices like firewalls are primarily designed to inspect traffic, not decrypt it. To maximize the return you get on your security investments, make sure they are focused on what they do best enforcing policies that restrict access and protect your resources from violations and attacks.

According to an **NSS Labs report**, buying a larger, more expensive firewall dedicated to SSL/TLS decryption can cost you tens of thousands to hundreds of thousands of dollars. Getting the capacity you need to decrypt all your SSL/TLS traffic just isn't practical. Buying an SSL/TLS security solution that is designed specifically to decrypt this traffic for your security devices offers a much better value.

Another alternative is to not decrypt your enterprise traffic at all, but with the rising trend of encryption across the internet, you will be blind to most of the traffic passing through your network. This means the cost of not decrypting can potentially have significant financial and operational consequences for your organization, as well as a negative impact on your brand, reputation, and stock. **The average cost** of a cyberattack on a company is $3.9 million, and the **average cost in time** of a malware attack is 50 days. Can you afford to not protect your organization from encrypted malware?

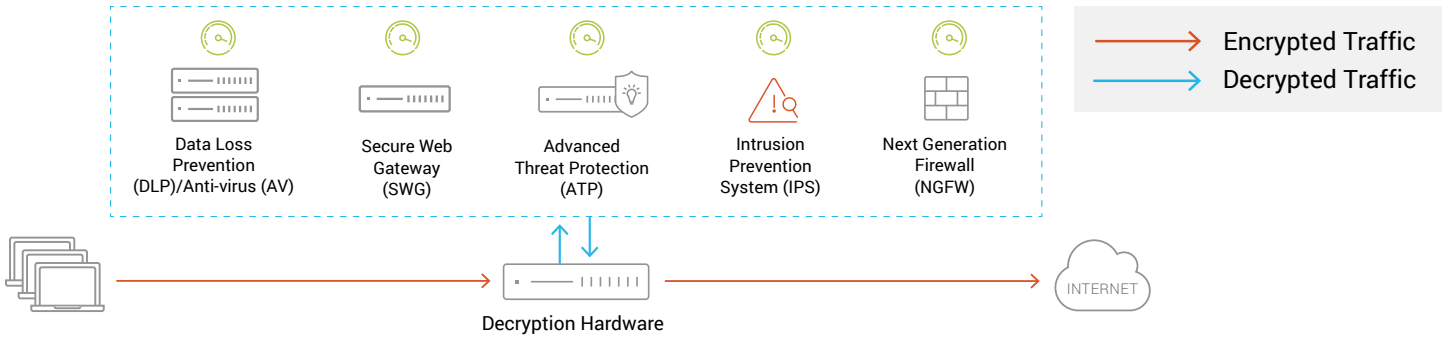


Figure 5. Enable your existing security devices to inspect encrypted traffic with optimal performance

CALCULATE YOUR ROI

See How Much You Could Save With A Dedicated Decryption Solution

CALCULATE NOW

5 DEPLOY AND MANAGE YOUR ENTERPRISE SECURITY SOLUTION SIMPLY AND EASILY

Two of the biggest problems you can face when investing in a decryption solution, whether in a firewall or a decryption solution, are the complexity and the lack of rich, usable analytics. Once you have invested in a solution that provides easy deployment and troubleshooting, you want to be operational as soon as possible to prevent any hidden threats that might come your way. Unfortunately, most of the decryption solutions are too complex to be deployed easily. If you somehow get your solution deployed, usually after paying hefty professional services fees, you are faced with more problems: are the analytics provided with the solution humanly consumable and useful, and is the solution even providing any usable insights?

Rich analytics with data delivered in an easy-to-consume format, that enables human analysts to make effective and informed decisions, are critical when you have encrypted traffic. Real-time analysis is essential to capturing deep insights into anomalies and threats in encrypted traffic, so you can set adaptive controls and policy updates through behavior analysis.

You may have products from partners like Splunk already deployed in your security network to help with gaining insights into the traffic flowing through your network devices. However, as your organization grows, and you have multiple geographically distributed deployments, a 'single pane of glass' solution becomes a necessity, so you can have management and analytics available at a single centralized location.

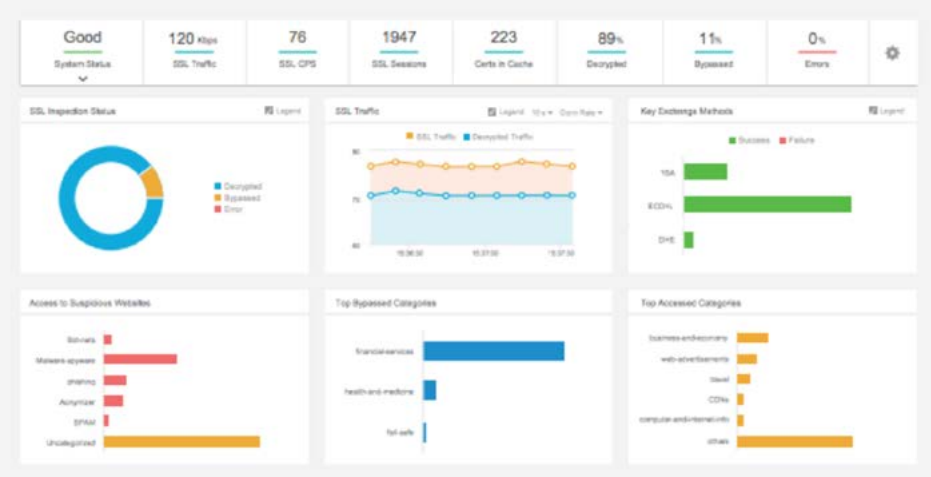
What you need is a centralized management and visibility solution that can manage multiple decryption solutions deployed in different branch offices, and provide rich analytics on a consolidated console. Such a solution should enable you to configure and manage all of your geographically distributed devices, individually or collectively, from a central location. It should also provide access to individual device statistics as well as aggregated analytics across multiple devices and locations. Additionally, the dashboards that these statistics are displayed on should be intuitive, making the data more digestible and troubleshooting faster.

YOUR DECRYPTION SOLUTION SHOULD

- Enforce **recommended security best practices,** eliminating human errors and oversights
- Provide a detailed troubleshooting wizard that helps you pinpoint cyber issues
- Provide dashboards that present you with detailed insights and actionable analytics that help you track anomalies

However, a centralized management solution should not interfere with your local management needs. Your decryption solution should also be able to host its own local management application that provides you with easy, wizard-driven configuration options that facilitates quick and accurate deployment. You should also have access to dashboards on your local machines that can help you analyze the traffic flowing through your network easily.

Centralized management and analytics provide full visibility into all SSL/TLS traffic across multi-site deployments



Easy-to-use configuration and troubleshooting wizards, and customizable dashboards

A10 THUNDER SSLI INSPECTION ADVANTAGE

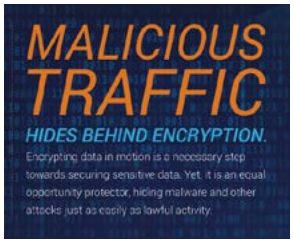
A10 Thunder SSLi is a purpose-built solution that eliminates the SSL/TLS blind spot, providing full visibility into encrypted traffic. Thunder SSLi increases your security effectiveness at a fraction of the cost by offloading CPU-intensive SSL/TSL operations from existing security solutions and eliminates the need for purchasing expensive added capacity and capabilities on many alternative security devices. Thunder SSLi also helps you meet your specific regulatory compliance requirements with continually evolving data protection and privacy standards, rules, and regulations such as the GDPR and HIPAA, thereby avoiding hefty fines.

With dedicated SSL processors, Thunder SSLi boosts the performance of your security infrastructure by decrypting traffic and forwarding it to one or more of your security devices, such as a firewall for deep packet inspection (DPI), allowing each of your security devices to operate at their peak performance.

This dramatically reduces any latency or performance degradation introduced into your security infrastructure.

Thunder SSLi supports step-by-step configuration and troubleshooting wizards and customized dashboards, so you can operationalize devices simply and easily. Using the Harmony Controller SSLi app also provides a centralized analytics and management console for multi-site deployments with rich insights into traffic decryption status, user behavior, and traffic pattern analysis.

Thunder SSLi's unique solution provides the most cost-effective, compelling, and scalable enterprise security solution that will not only arm your security infrastructure against today's cyber threat landscape, but will also future-proof your enterprise infrastructure to defend against growing cyber threats without compromising your network's performance.



TO LEARN MORE

For more information, check out A10's Malicious Traffic Hides Behind Encryption Infographic.

READ IT NOW

REQUEST A FREE EVALUATION TO DETERMINE YOUR RISK LEVEL

REQUEST DEMO

SOURCES

- https://www.gartner.com/en/conferences/na/security-risk-management
- https://www.a10networks.com/blog/takeaways-gartner-security-summit
- https://transparencyreport.google.com/https/overview?hl=en
- https://blogs.cisco.com/enterprise/a-guide-for-encrypted-traffic-analytics
- https://www.nsslabs.com/company/news/press-releases/nss-labs-predicts-75-of-web-traffic-will-be-encrypted-by-2019/
- https://go.forrester.com/wp-content/uploads/Forrester-2018-Predictions.pdf?utm_source=forrester_lp_capstone&utm_medium=web&utm_campaign=predictions_2018&utm_content=button
- https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html
- https://www.nsslabs.com/company/news/press-releases/nss-labs-expands-2018-ngfw-group-test-with-ssl-tls-security-and-performance-test-reports/
- https://www.sonicwall.com/en-us/asset-lp-show?asset=239552&hash=f1a4866ff96eb31a2a8f099f776f778e95dc9136d739dfddc9a98309dfb7fe02
- 2018 Cost of a Cyber Breach by Ponemon
- https://www.accenture.com/us-en/event-cybertech-europe-2017?src=SOMS#block-insights-and-innovation
- https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2018_Cyber_Resilient_Organization_Study.pdf
- https://go.forrester.com/2018-predictions/
- https://go.recordedfuture.com/buyers-guide

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information visit: **a10networks.com**
or tweet **@A10Networks**.

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-EB-14112-EN-02 DEC 2018