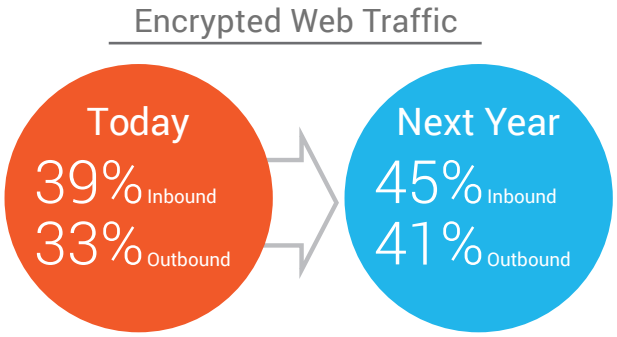
A10 Thunder SSLi Enables Organizations to Protect Themselves from Threats Hidden in Encrypted Traffic

The Risks in Encrypted Traffic

The Ponemon Institute conducted a survey, "The Hidden Threats in Encrypted Traffic: A Study of North America and EMEA," sponsored by A10 Networks, to investigate the challenges organizations face trying to detect and prevent Web-based threats.

Organizations are increasingly using SSL encryption, as they look to prevent costly cyberattacks and maintain compliance with relevant regulations, to protect the privacy and integrity of their sensitive data in transit. According to survey respondents, **45 percent** of inbound Web traffic and **41 percent** of outbound Web traffic are expected to be encrypted within the next 12 months.



Although it is a powerful security measure, SSL encryption is increasingly being used by attackers to hide malicious activity from detection. **79 percent** of the survey participants indicated they had been the victim of a cyberattack or malicious insider abuse in the past 12 months; **41 percent** of those attacks used encryption to evade detection. **54 percent** thought network attackers will increase their use of encryption (to evade detection and bypass controls) over the next 12 months.

As a result, it's not surprising **75 percent** believe that compromised insider credentials due to malware hiding inside encrypted SSL traffic could cause a data breach.

The Problem with Inspecting Encrypted Traffic

While **89 percent** of respondents recognize it is "Important"/"Essential" to inspect SSL traffic, the majority (**53 percent**) do not decrypt Web traffic to detect attacks, intrusions and malware, leaving them blind to the threats that may be hiding in it. The reasons organizations give for not inspecting encrypted traffic are centered around a lack of enabling security tools (**47 percent**), performance degradation (**45 percent**) and insufficient resources (**45 percent**).

89% Agreed it is essential to inspect SSL traffic

Performance Degradation

53%

Agreed security solutions are collapsing under growing SSL bandwidth demands.

Most existing security solutions are unable to effectively handle the CPU-intensive decryption and re-encryption of SSL traffic. Independent tests show most security devices experience an 80 percent performance degradation.

The problem is compounded when Elliptic Curve Cryptography (ECC), a.k.a. Diffie Hellman, is used to encrypt the session (a method increasingly employed by Apple and Google). **53 percent** of respondents agreed their organization's security solutions are collapsing under growing SSL bandwidth demands and SSL key lengths.

As a result, organizations are often forced to forgo or only selectively inspect encrypted traffic, leaving them vulnerable to attacks. **39 percent** of the organizations surveyed agreed their enterprise perimeter security investment is ineffective because of inbound and outbound encrypted traffic (**31 percent** were unsure). **52 percent** agreed that the inability of their organization's current security infrastructure to inspect encrypted traffic compromises their ability to meet existing and future compliance requirements.

Requirements for an SSL Inspection Solution

Organizations require a solution that can help them detect abuse in encrypted traffic without impacting the performance of their traffic. Specifically, respondents to the Ponemon study indicated it was important for a solution to:

- Securely manage SSL certificates and keys — 88%
- Scale to meet current and future SSL performance demands — 87%
- Maximize the uptime and performance requirements of the overall capacity of the security infrastructure — 82%
- Satisfy compliance requirements — 80%
- Interoperate with a diverse set of security products from multiple vendors — 77%
- Categorize Web traffic to ensure confidential or sensitive data remains encrypted (satisfy regulatory requirements) — 76%
- Granularly parse and control traffic based on custom-defined policies — 75%
- Intelligently route traffic to multiple security devices — 73%

A10 Networks Thunder SSLi

The Answer to an Organization's Encrypted Traffic Problems

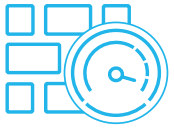
A10 Networks Thunder® SSLi® enables organizations to quickly detect malware and insider threats in encrypted traffic. A10 Thunder SSLi offloads SSL decryption and re-encryption from third-party security devices and enhances the efficiency and performance of the overall infrastructure.

Thunder SSLi is purpose-built to quickly decrypt SSL traffic and then forward it to one or many dedicated security devices. Once the traffic has been inspected, Thunder SSLi can re-encrypt the data and forward it to the appropriate destination. With Thunder SSLi, organizations can:

- **Eliminate security blind spots** – Ensure security tools can detect malware, breaches, abuses and insider threats in encrypted traffic to keep ongoing operations and sensitive information safe.
- **Lower TCO and improve overall network performance** – Offload SSL decryption from security devices to boost the overall effectiveness and performance of the infrastructure. Thunder SSLi's high-speed decryption delivers near-parity performance between 1024-bit and 2048-bit key sizes and the extreme power needed to handle 4096-bit keys at high-performance production levels to minimize any impact on the network.
- **Protect sensitive data and adhere to regulatory requirements** – Leverage granular controls to dictate which SSL traffic needs to be decrypted and inspected and which needs to be bypassed to meet compliance requirements and ensure data privacy.

Eliminate Security Blindspots

Improve Network Performance



Protect Sensitive Data

For more information on A10 Thunder SSLi, please visit **a10networks.com/SSLi**.

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Hong Kong
hongkong@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
Japan South Asia
jinfo@a10networks.com
southasia@a10networks.com
China/Australia/New Zealand
china_sales@a10networks.com
anz_sales@a10networks.com

To discover how A10 Networks products will enhance, accelerate and secure your business, contact us at a10networks.com/contact or call to speak with an A10 sales representative.

Part Number: A10-SB-19159-EN-01 Aug 2016