6 KEYS TO ELIMINATING SSL BLIND SPOTS:

WHAT YOU NEED FOR SSL INSPECTION

RIGHT NOW, MALICIOUS TRAFFIC COULD BE ACCESSING YOUR SYSTEMS

SSL usage has been steadily increasing each year, with estimates indicating that **67 percent of Internet traffic will be encrypted by 2016.**[1] Unfortunately, it's not just security-conscious organizations and users who are turning to encryption—hackers are using it to conceal their efforts. And although many firewalls and threat prevention solutions are capable of decrypting SSL traffic, they can't keep up with evolving decryption demands.

If hackers are able to get through, the organizations they attack face downtime, lost sales, customer backlash, and loss of intellectual property—plus high costs to remediate breaches and repair the damage to their reputation.

The hard truth is: Without SSL inspection in place, your organization is at risk of an attack. Hackers hiding in encrypted traffic can infiltrate your networks, install malware, and steal data across multiple end-points.

Your best defense against malicious encrypted traffic is an SSL inspection platform that meets 6 key requirements.

1. Sandvine Global Internet Phenomena Spotlight: Encrypted Internet Traffic report, May 2015.

THE 6 KEYS TO KEEPING HACKERS FROM GETTING IN

When evaluating potential SSL inspection partners, businesses should keep performance, compliance, availability and security top of mind. An effective SSL inspection platform should do all of the following:

01.

MEET SSL PERFORMANCE DEMANDS.

Performance is critical in any new solution for your organization, but is particularly so when that solution has **to keep pace with ever increasing loads.** To ensure SSL inspection performance meets current and future needs:

- Test SSL inspection speeds with 2048-bit and 4096-bit SSL keys.
- Evaluate a mix of traffic with Diffie-Hellman and elliptic curve ciphers.
- Confirm that the platform can handle throughput requirements, with extra headroom for traffic peaks.

02.

SATISFY COMPLIANCE MANDATES.

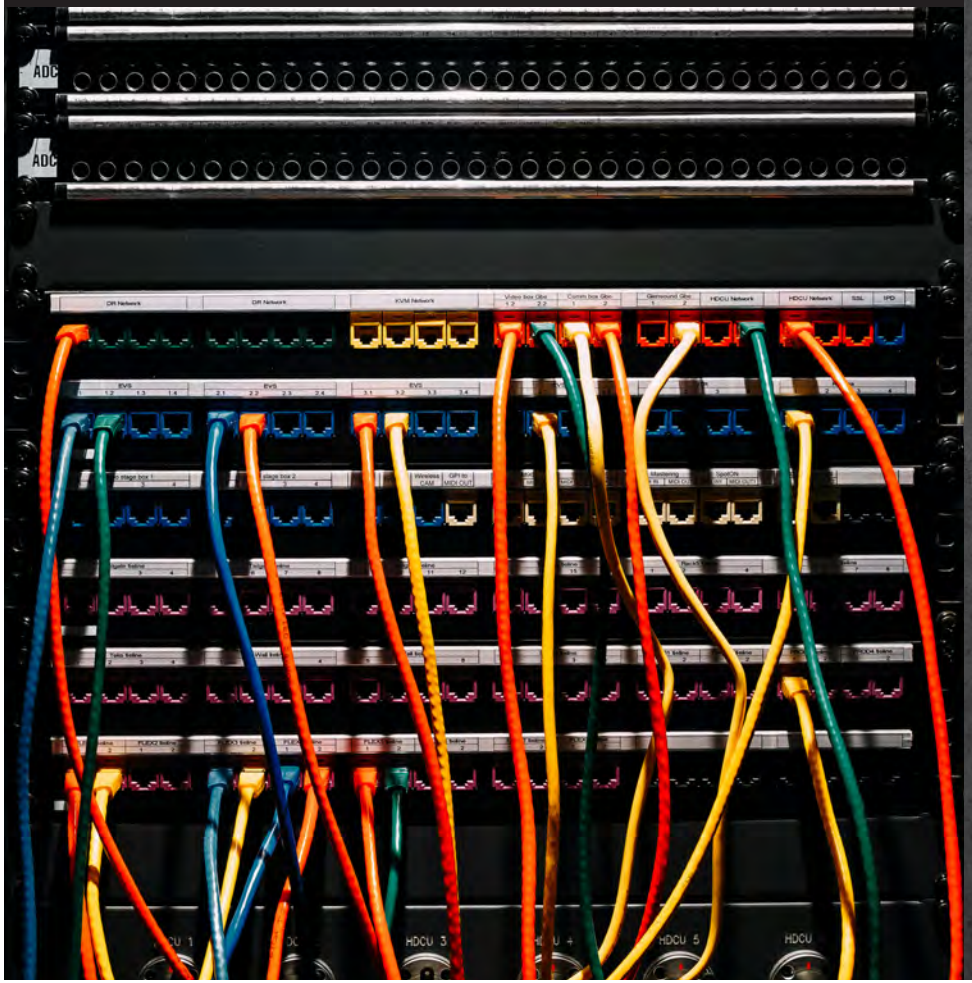
With local laws, regulations like HIPAA and SOX, and the Electronic Communications Privacy Act (ECPA) in place to protect data privacy, **businesses are now tasked with meeting a variety of compliance standards.** Adhering to these laws means that many organizations—such as those in the financial and healthcare industries—must bypass sensitive traffic.

To remain compliant while inspecting SSL traffic, IT security teams should look for platforms that can:

- Categorize web traffic by type, ensuring that confidential data, such as communications directed to healthcare and banking sites, remains encrypted.
- Support automatically-updated as well as manually-defined URL bypass lists.

03.

SUPPORT COMPLEX DEPLOYMENT REQUIREMENTS.



In an effort to cover all security bases, most organizations have deployed a wide range of security devices from multiple vendors. **SSL inspection platforms should be able to decrypt traffic for all of these devices.** To do so, they must:

- Decrypt outbound traffic to the Internet and inbound traffic to corporate servers.
- Intelligently route traffic with advanced traffic steering to multiple security devices.
- Integrate with a variety of security solutions from leading vendors.

04.

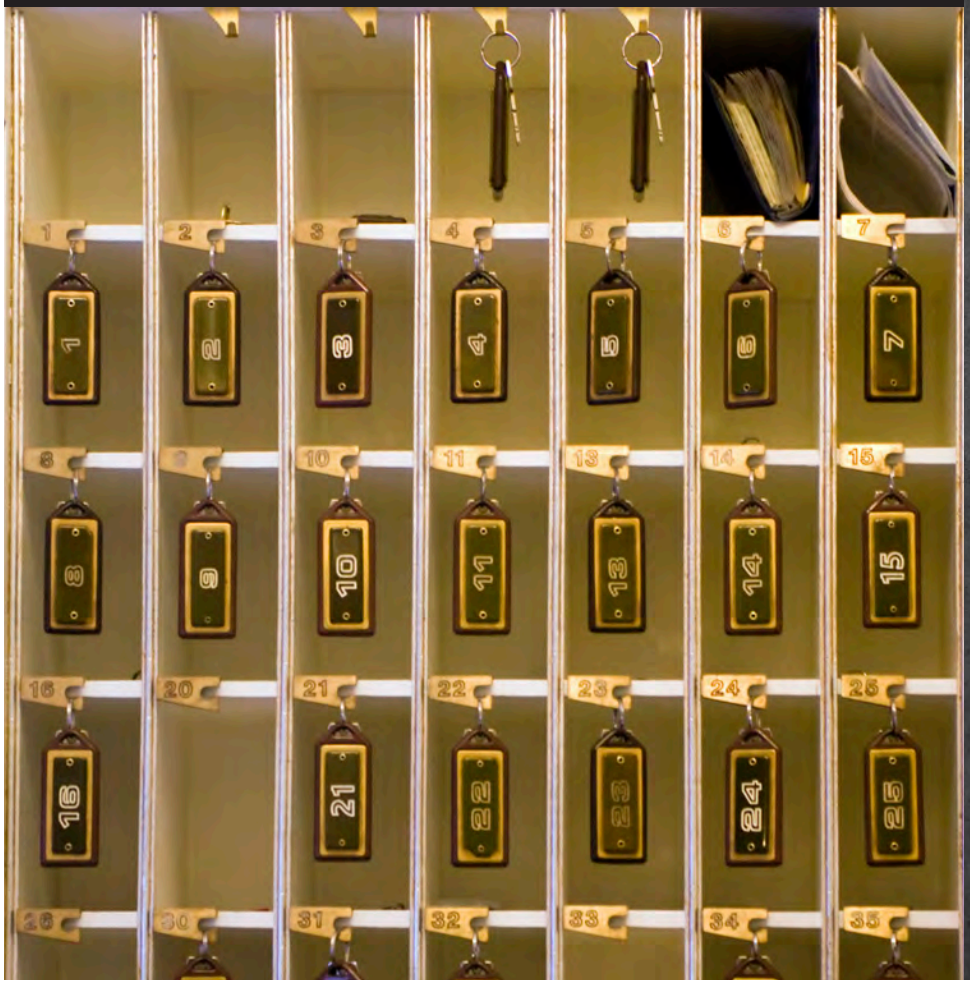
MAXIMIZE SECURITY INFRASTRUCTURE UPTIME AND CAPACITY.

Security infrastructure must be up and fully available in order to block cyber attacks and prevent data exfiltration. If security infrastructures fail, threats may go undetected, leading to devastating attacks, revenue loss, and brand damage. **An effective SSL inspection platform should lower risk by maximizing the uptime of the existing security infrastructure.** Look for a platform that will:

- Scale security deployments with load balancing.
- Avoid network downtime by detecting and routing around failed security devices.
- Support advanced monitoring to rapidly identify network or application errors.

05.

SECURELY MANAGE SSL CERTIFICATES AND KEYS.



SSL certificates and keys form the basis of trust for encrypted communications. If compromised, attackers can use them to steal data. As part of providing visibility into both outbound and inbound SSL traffic, **SSL inspection platforms must be able to securely manage hundreds or thousands of SSL certificates and keys.** An effective SSL inspection platform should:

- Protect SSL keys stored on the SSL inspection platform.
- Integrate with third-party SSL certificate management solutions that discover and control certificates.
- Support FIPS 140-2 Level 2 and Level 3 key management.

06.

DECRYPT ALL STANDARDS-COMPLIANT ENCRYPTED TRAFFIC.

It's not just the volume of encrypted traffic that's increasing—so is the sophistication level of the ciphers organizations and attackers are using. **Techniques like 4096-bit SSL keys, elliptic curve ciphers, Perfect Forward Secrecy (PFS), and others are being put in place to guard against prying eyes.** To keep up, SSL inspection platforms must:

- Support 4096-bit SSL key lengths and advanced SSL and TLS ciphers.
- Decrypt all data, including SSL retransmissions.
- Notify you if traffic can't be decrypted.

Your business's best defense against malicious encrypted traffic is making sure you have an SSL inspection platform in place that meets these 6 critical criteria. Relying on a system that doesn't meet these requirements can open your organization up to deployment pitfalls—and incoming threats.

The SSL Insight™ feature of A10 Networks® Thunder® ADC line of Application Delivery Controllers can provide your business with complete threat protection by analyzing all network data, including encrypted data.

A10's SSL Insight allows your business to:

- **Eliminate blind spots** in corporate defenses by decrypting SSL traffic at high speeds.
- **Maximize uptime** by load-balancing multiple third-party security appliances.
- **Scale performance and throughput** to successfully counter cyber attacks.
- **Prevent costly data breaches and loss of intellectual property** by detecting advanced threats, fast.

IF YOUR SSL INSPECTION FALLS SHORT, YOU COULD BE THE NEXT VICTIM OF AN ATTACK

To learn more about how the A10 Thunder ADC can help your organization detect encrypted traffic threats and protect key data and systems, visit **www.a10networks.com/adc-security** or contact **1-408-325-8616**.

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**

©2015 A10 Networks, Inc. All rights reserved. The A10 logo, and A10 Networks are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners.

Part Number: A10-EB-14101-EN-01 SEP 2015