# Exposing Hidden Threats:

## Why Your Organization Needs SSL Inspection

# Contents

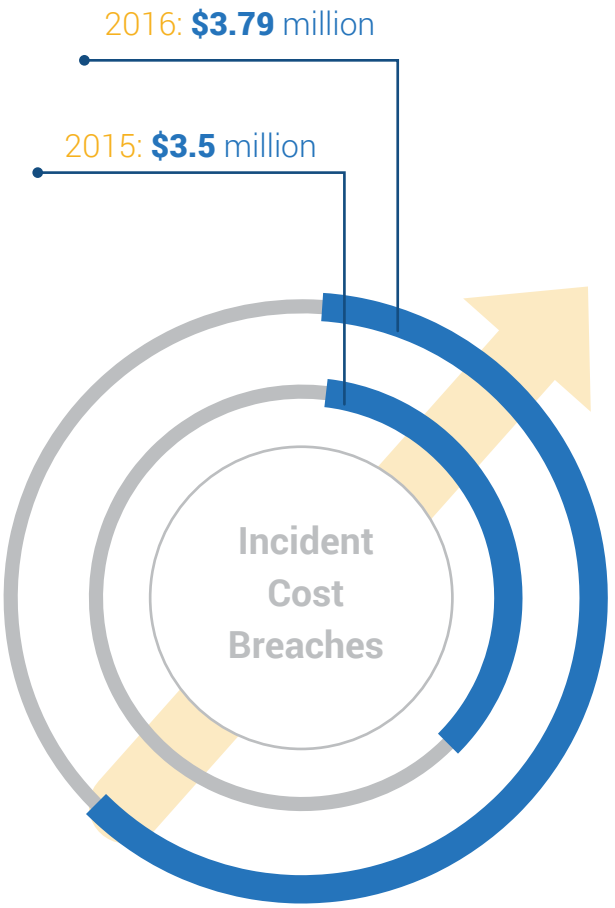


# Introduction: Rising Cost of Breaches and Data Privacy Concerns Are Driving Encryption

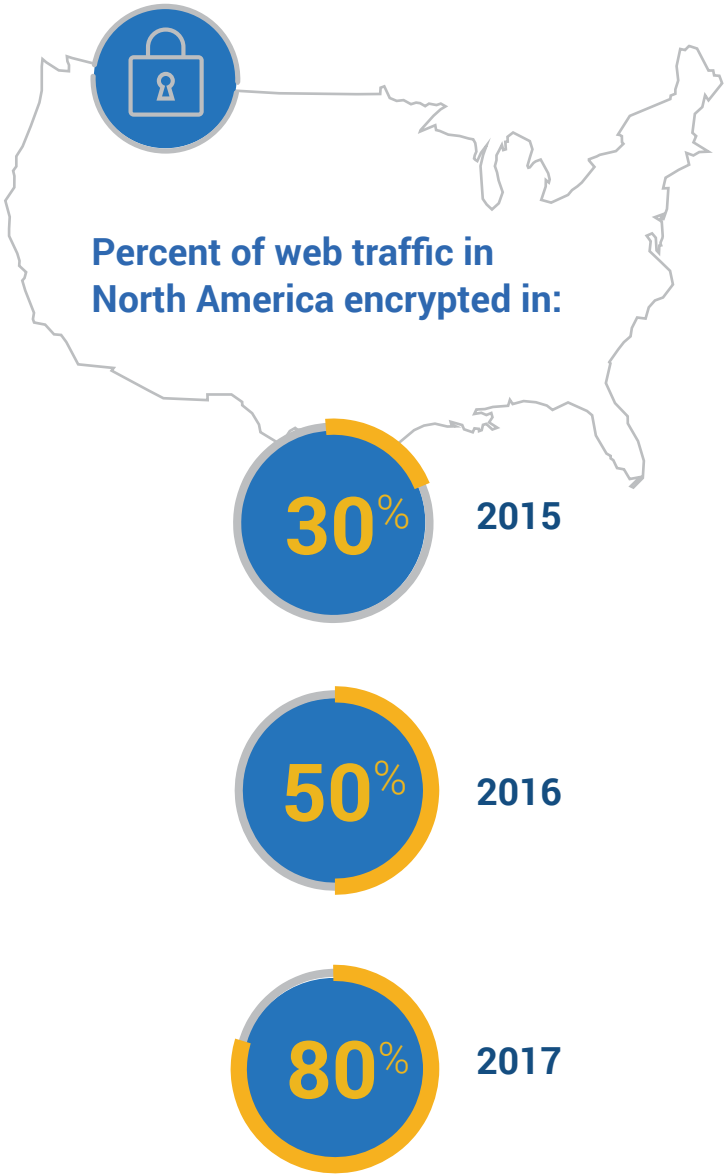
The cost of a data breach has steadily increased over the past several years, hitting $3.79 million, up from $3.5 million in 2015, according to the Ponemon Institute.[1] In response, organizations are stepping up security practices, including data encryption. Encrypting a record can reduce its breach-related costs more than any other measure and extending this to communications is critical.

Interest in encryption is also growing due revelations in recent years about the depth of surveillance by organizations like the U.S. National Security Agency.[2] Protecting data privacy has become a top priority for many organizations.

However, the growing adoption of encryption has created a new set of issues. With the bulk of all web traffic migrating toward SSL/TLS, it is easier than ever for cyberattacks and malware to hide behind the cipher. Security solutions that rely on visibility to monitor web traffic are now blind to a growing number of threats hiding behind encryption.




1: www.csoonline.com/article/2926727/data-protection/ponemon-data-breach-costs-now-average-154-per-record.html
2: whatis.techtarget.com/definition/Snowden-effect




# The Evolution of the Secure Internet

Encrypted web traffic used to be the exception rather than the rule. Over the past few years that trend has reversed, with rapid progress being made toward a fully encrypted internet:

- An estimated 30 percent of web traffic in North America was encrypted in mid-2015. By the start of 2016 that number had grown to 50 percent and as much as 70-80 percent of all web traffic will be encrypted by the start of 2017.[1]
- Google has been leading the charge toward a fully secure internet (including higher search rankings for encrypted websites). By the end of 2013, only 52 percent of requests to its data centers were encrypted; in early 2016, that number had risen to over 70 percent.[2]
- Let Encrypt has removed cost as a barrier to entry for many organizations by providing free SSL certificates. In March of 2016 they issued their one millionth certificate.
- Driven by initiatives like these, the internet is expected to be mostly encrypted as soon as 2017.[3]

While encrypting web traffic is protecting data from breaches and government snooping, it has also introduced a new set of challenges for information security organizations.

1: www.thejakartapost.com/news/2016/03/16/google-reveals-77-percent-its-online-traffic-encrypted.html
2: www.cbronline.com/news/cybersecurity/data/70-percent-of-internet-traffic-to-be-encrypted-as-state-agencies-scramble-to-police-internet-4809408
3: fortune.com/2015/04/30/netflix-internet-traffic-encrypted/

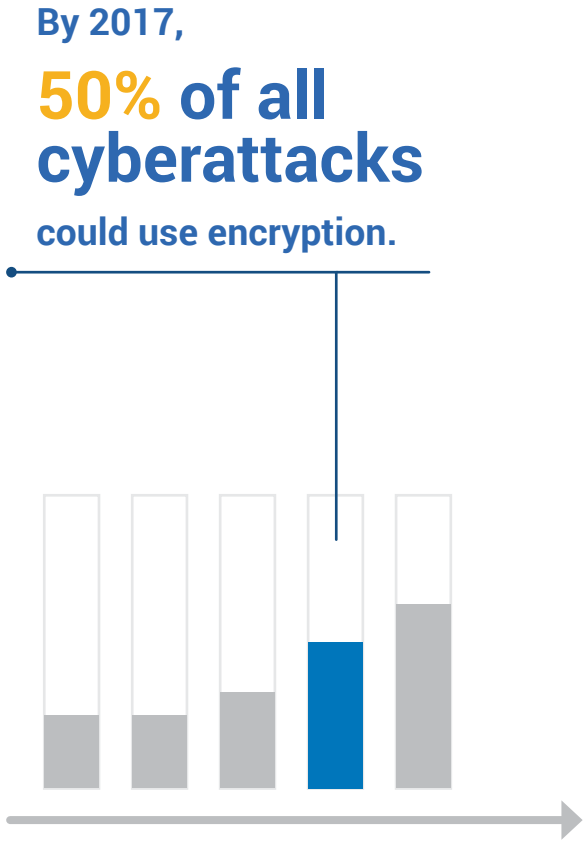
# The Rise of Encrypted Threats

# The Rise of Encrypted Threats

Although SSL is used to protect legitimate communications containing sensitive data, it can also hide more nefarious behavior from inspection. Cyber criminals now use it to hide activities from IT security tools, which typically can't inspect or analyze encrypted communications.

Malicious insiders have been hiding from corporate security measures for years by using encrypted communications. Increasing use of secure, cloud-based storage has made data exfiltration even easier, allowing insiders to exfiltrate sensitive data while evading data loss prevention and other monitoring solutions.

Using SSL is increasingly common for malware as a way to escape detection. Gartner predicts that by 2017, 50 percent of all cyberattacks could use encryption.[1] This prompts the question: What specific types of attacks benefit most from SSL?




1: http://www.securityweek.com/ssl-encryption-keep-your-head-game?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Securityweek+(SecurityWeek+RSS+Feed)

# The Rise of Encrypted Threats: **Malvertising**

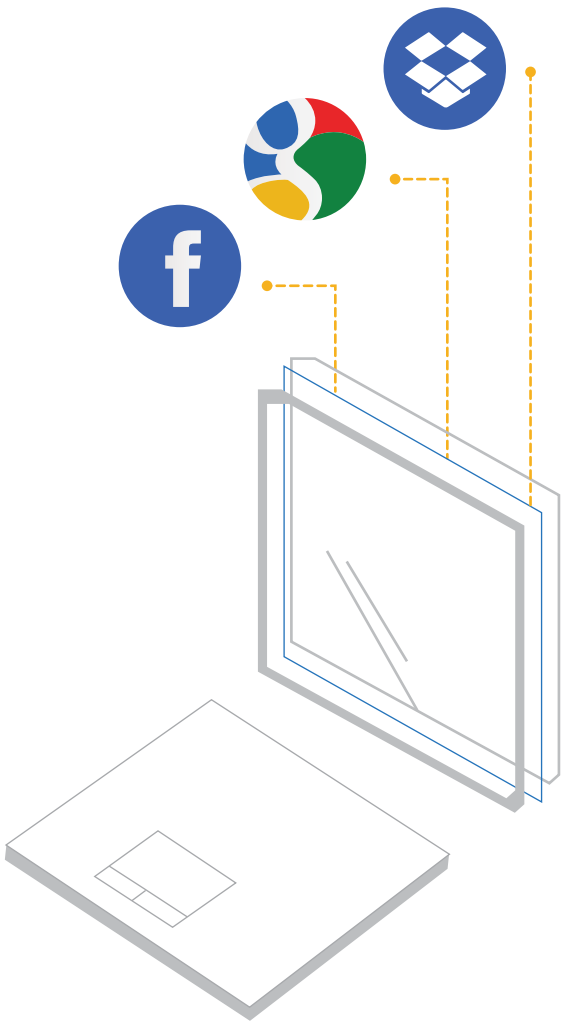
In June and July 2015, malvertising schemes set new records for the number of compromised advertisements served. Yahoo!, which saw around 6.9 billion monthly page views on its main site alone at the time, was the target of a scheme that used HTTPS-protected URLs to deliver malware.[1] These encrypted connections made it difficult to detect the infected traffic at the network layer.

Malware has also capitalized on encryption in other channels such as social media and email, in addition to ad tech networks. For example, Koobface exploited the fact that Facebook encrypts all of its communications, using it to mask the spread of malware that could enlist a PC within a vast peer-to-peer botnet.[2]

**6.9 Billion monthly visitors on Yahoo!**

**were exposed to a malvertising campaign that distributed malicious links**

1: https://blog.malwarebytes.org/threat-analysis/2015/08/large-malvertising-campaign-takes-on-yahoo/
2: http://www.cnet.com/news/koobface-virus-hits-facebook/#!



# The Rise of Encrypted Threats: **Insider Threats**

Insiders have many ways to avoid detection by traditional security monitoring. Widespread use of SSL by instant messaging platforms (Telegram, Facebook Messenger, gchat) and secure, cloud-based storage platforms (Box, Dropbox, Google Docs) makes data exfiltration easy to hide. The average organization will be hit with four incidents a year and 62 percent say that these threats are on the rise.[1]

In one example, a senior IT administrator at a large telecom company was able to upload a significant volume of sensitive data to a personal Dropbox account. The process only took him about 20 minutes.[2] And while this particular attack was successfully detected and stopped before it achieved its goal, most organizations are still struggling to keep up with the rapidly evolving threat landscape. Only 23 percent of organizations are confident that they have done enough to monitor the activities of privileged users.[3]

1: http://www.fiercecio.com/story/companies-averaging-4-insider-threat-attacks-year/2015-06-26
2: http://www.observeit.com/blog/how-major-telecom-company-stopped-data-theft-observeit
3: https://www.netiq.com/communities/cool-solutions/netiq- views/84-fascinating- it-security-

# The Rise of Encrypted Threats: **DDoS & Web Attacks**

Distributed denial-of-service (DDoS) attacks have been climbing for years, reaching an all-time record in Q2 2015. The number of attacks was up 132 percent from the previous year.[1]

SSL/TLS encryption is now commonly used to amplify the power of DDoS attacks such as HTTPS floods.[2] A multi-vector DDoS scheme using encryption puts more pressure on its target. Either the victim's networks have to use up a ton of system resources in the decryption of the incoming traffic or the attack will bypass security controls.

Another spin on encrypted DDoS involves initiating a regular SSL handshake and then requesting immediate renegotiation of the key.[3] The repeated requests ultimately exhaust all available server resources. This approach was once demonstrated as a proof-of-concept by The Hacker's Choice, an international consortium of security researchers.

**The number of attacks was up**

**132 percent**

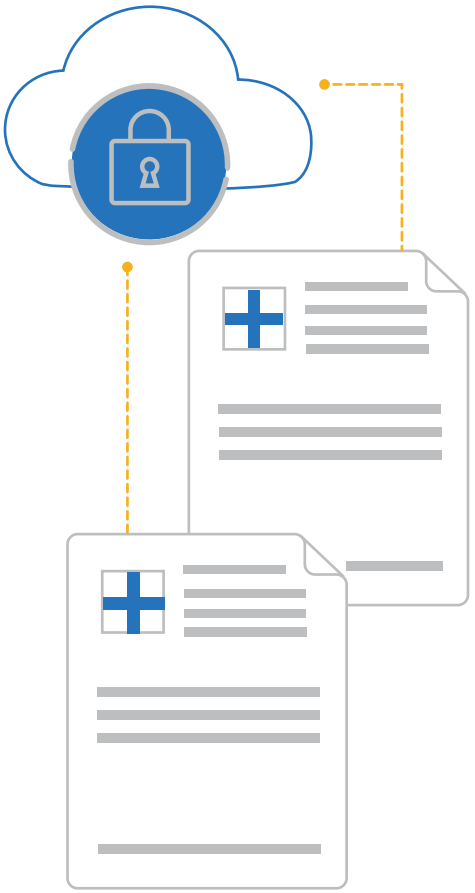
**from the previous year.**

1: http://www.digitaltrends.com/computing/ddos-attacks-hit-record-numbers-in-q2-2015/
2: https://security.radware.com/ddos-threats-attacks/ddos-attack-types/ssl-based-ddos-attacks/
3: http://www.securityweek.com/missing-layer-against-encrypted-attacks

# How to Protect Against Encrypted Threats: **Inline Decryption**

Protection against encrypted threats starts with inline decryption. An SSL inspection appliance decrypts the traffic, sends it to one or more security solutions (UTM, IDS/IPS, firewall, etc) and then passes it back through another partition to encrypting it again.

This process eliminates the well-documented performance degradation that firewalls experience when sorting through encrypted traffic. At the same time, the data in question is only exposed to the security device(s), ensuring that compliance and data privacy requirements are maintained. Policies can even be set up to allow specific data, like patient health records, to remain encrypted to comply with relevant mandates.

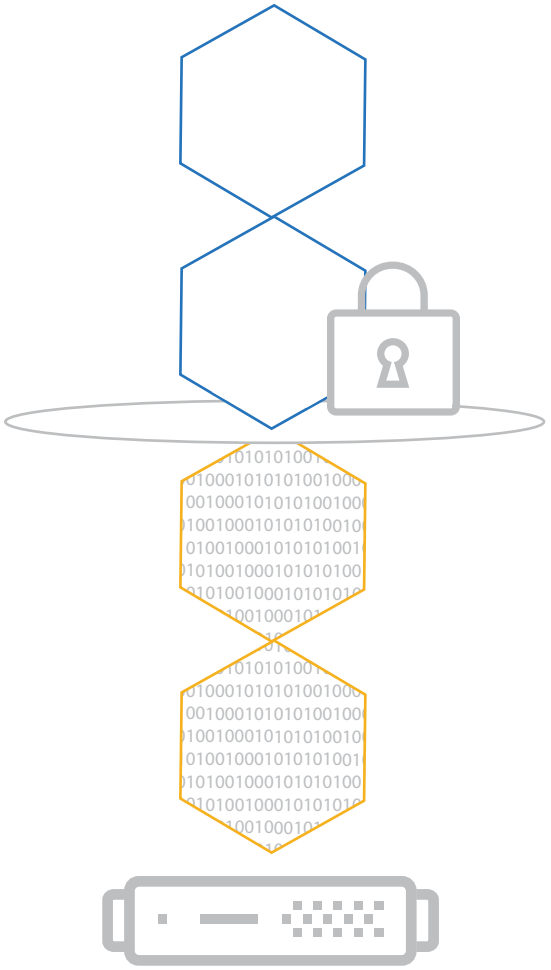


**Patient health records remain encrypted to comply with relevant mandates.**

# Another Way to Protect Against Encrypted Threats: **Out-of-Band Decryption**

Decryption can also be done out-of-band. Again, a dedicated SSL inspection appliance plays a key role, working exclusively with out-of-band security devices or in tandem with one or more inline solutions.

Once data is decrypted, a copy is then relayed to an out-of-band device such as, an advanced threat protection (ATP) platform or a security information and event management (SIEM) solution. The main advantage of leveraging an out-of-band configuration is flexibility, giving visibility to a combination of conventional preventive security devices and advanced detection and response solutions.



# Introducing A10 Thunder SSL Insight

The A10 Thunder® SSL Insight® (SSLi®) appliance provides full visibility into encrypted traffic, including ECDHE ciphers. It helps eliminate blind spots, detect and neutralize potential threats that may be hiding behind encryption such as SSL/TLS and ultimately lower the risk of a costly data breach.

A10 Thunder SSLi can perform both inline and out-of-band decryption. It can perform at 40 Gbps, conduct dynamic port interception of SSL traffic and handle load balancing to scale security infrastructure. Built-in ICAP support can decrypt traffic for tools such as AV scanners.

With A10 Thunder SSLi, it is possible to stay safe from an increasingly common type of cyberattack. Encrypted malware, DDoS and command-and-control infrastructure can all be kept at bay with A10 Thunder SSLi's advanced capabilities.

To learn more about how A10 Thunder SSLi can help your organization detect encrypted traffic threats and protect key data and systems, visit **www.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**



Part Number: A10-EB-14105-EN-01 May 2016