eBOOK

EXPOSING HIDDEN THREATS:

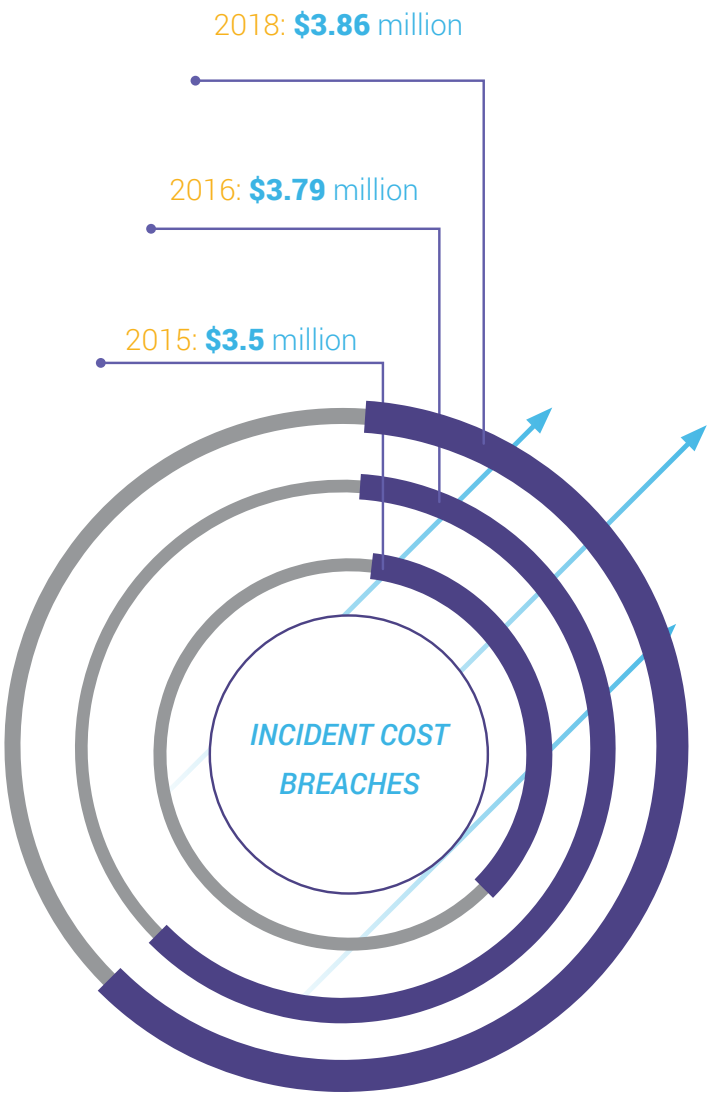
WHY YOUR ORGANIZATION NEEDS DEDICATED DECRYPTION

A10®

Contents

INTRODUCTION

1 The Rising Cost of Data Breaches and Privacy Concerns are Driving Encryption



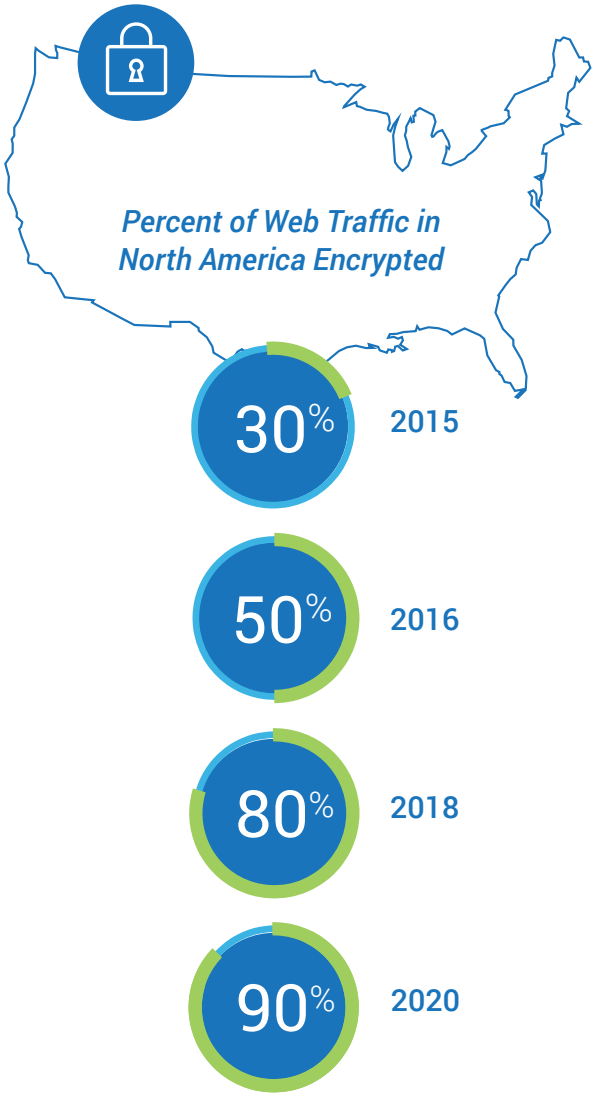
According to the Ponemon Institute, the cost of a data breach has steadily increased over the past several years, hitting $3.86 million in 2018, up from $3.5 million in 2015.[1] In response, the security practices of organizations are evolving, including the increased use of data encryption. Encrypting a data record can reduce the chance of it being modified or stolen more than any other measure, and extending encryption to communications is critical. Reducing the cost of a data breach is more important than ever before as Juniper Research estimates that criminal data breaches will cost businesses a total of $8 trillion over the next four years, due to high levels of internet connectivity and inadequate enterprise wide security![2]

Interest in encryption is also growing mostly because of revelations about the depth of surveillance by organizations such as the U.S. National Security Agency.[3] In light of these developments, 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 now easier than ever for cyberattacks and malware to hide behind encryption. Security solutions that rely on visibility to monitor web traffic are now blind to a growing number of threats using the cover of encryption.

1: https://newsroom.ibm.com/2018-07-11-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses
2: https://www.juniperresearch.com/press/press-releases/cybercrime-to-cost-global-business-over-$8-trn
3: https://whatis.techtarget.com/definition/Snowden-effect

2 The Evolution of the Secure Internet

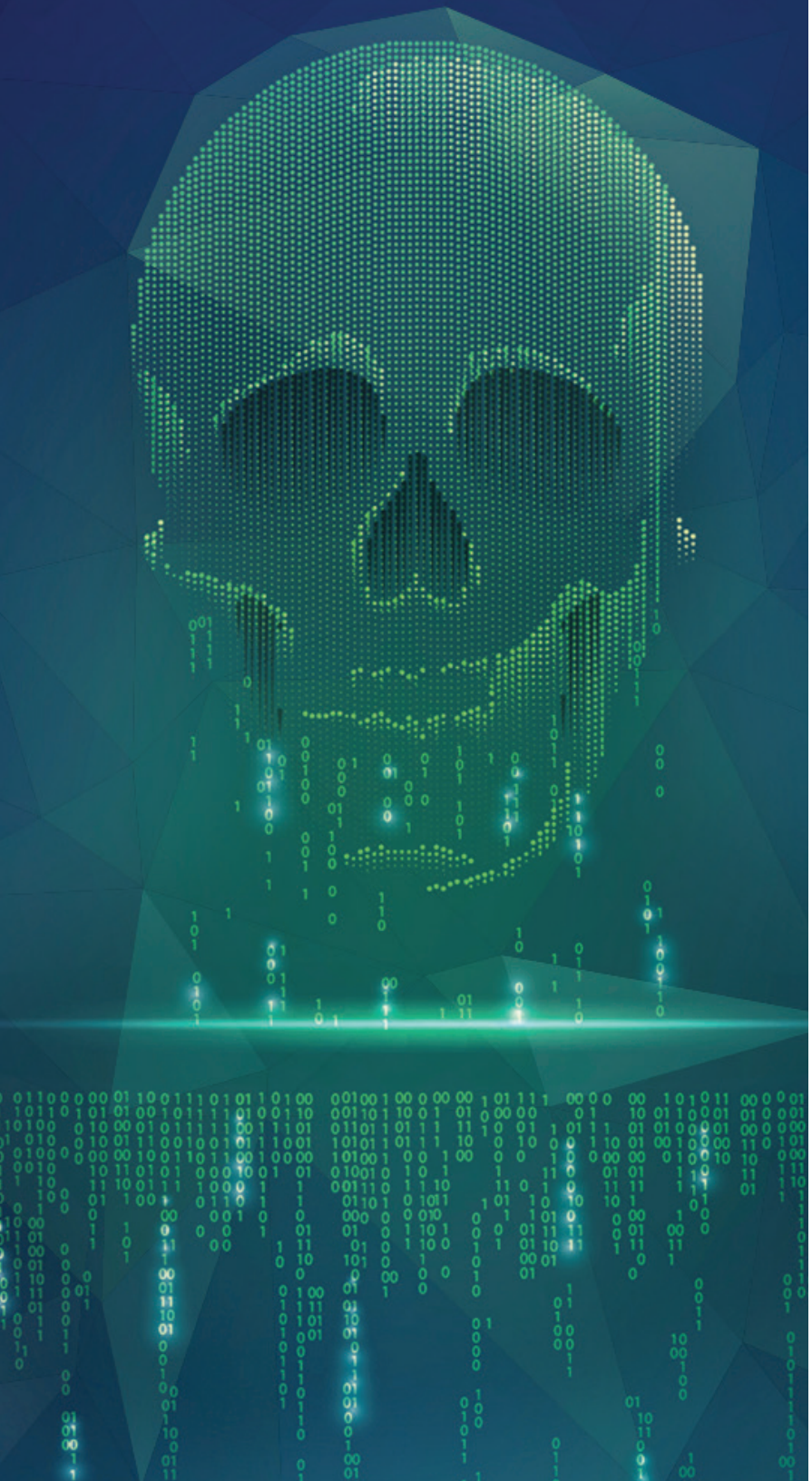


Encrypted web traffic used to be the exception rather than the rule. Over the past few years that trend has reversed, with rapid progress being made toward a fully encrypted internet:

- An estimated 30% of web traffic in North America was encrypted in mid-2015. Towards the end of 2018 that number had grown to over 80% and as much as 90% of all web traffic is expected to be encrypted by the start of 2020.[1]
- Google has been leading the charge toward a fully secure internet (including higher search rankings for encrypted websites). In 2016, only 59% of the HTTPS page loads for Chrome on Windows were encrypted; by September 2018, that number had risen to 87%.[2]
- Let's Encrypt has removed cost as a barrier to entry for many organizations by providing free SSL certificates. In June of 2017, they issued their 100 millionth certificate.[3]
- The web went from 46% encrypted page loads in 2016 to 67% in 2017, according to statistics from Mozilla—a gain of 21 percentage points in a single year.[4]

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

1: https://transparencyreport.google.com/https/overview
2: https://transparencyreport.google.com/https/overview
3: https://letsencrypt.org/2017/06/28/hundred-million-certs.html
4: https://letsencrypt.org/2017/12/07/looking-forward-to-2018.html



THE RISE OF ENCRYPTED THREATS

3

The Rise of Encrypted Threats

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

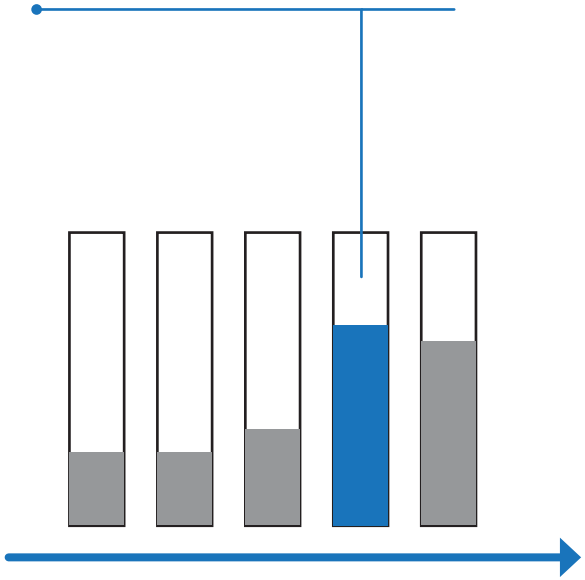
Malicious insiders have been hiding from corporate security measures for years by using encrypted communications. Increasing use of secure, cloud-based storage has made data exfiltration even easier, allowing insiders to smuggle sensitive data out while evading Data Loss Prevention (DLP) and other monitoring solutions.

Using SSL/TLS is increasingly common for malware as a way to escape detection.[1] It is predicted that by 2019 up to 70% of all cyberattacks will use encryption. This prompts the question: What specific types of attacks benefit the most from using SSL/TLS?

By 2019,

70% of all cyberattacks

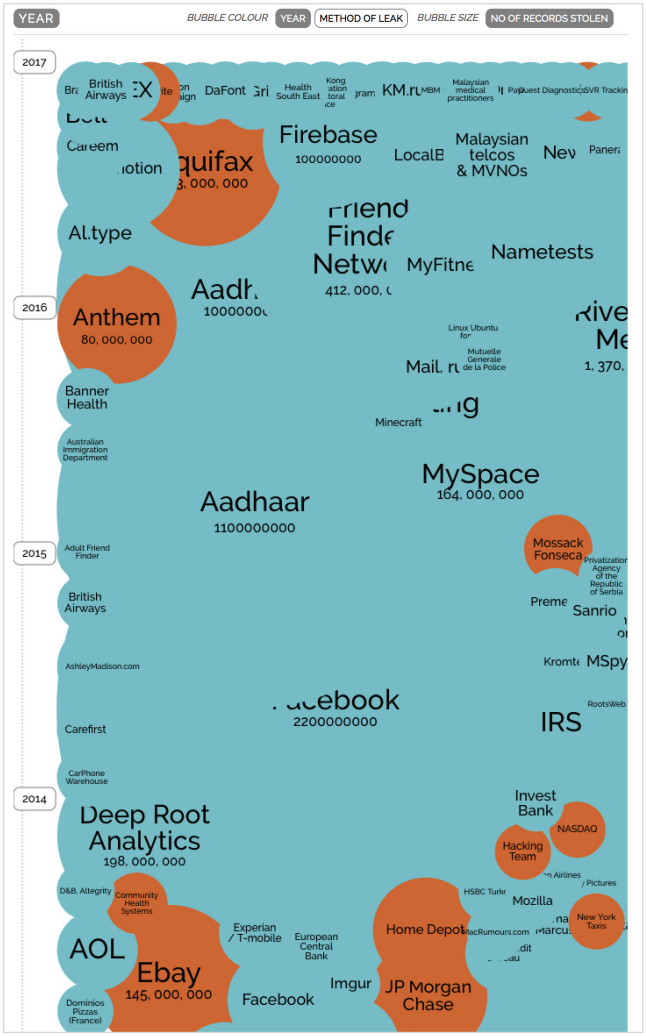
will use encryption.



1: https://blogs.cisco.com/enterprise/a-guide-for-encrypted-traffic-analytics

3.1 The Rise of Encrypted Threats: Data Breaches

Worlds Biggest Data Breaches[4]



Did You Know?

- **85% of the internet** in North America is encrypted[1]
- As much as **70% of cyberattacks** will use encryption as part of their delivery mechanism by 2019[2]
- **Two out of three organizations** are not able to decrypt and inspect their SSL/TLS traffic [3]

Unfortunately, for you it's a catch twenty-two; The more you encrypt the internet to preserve your data integrity and privacy, the more you need to invest in decryption. This is due to cyber criminals now using encryption to hide malware, thereby infecting your systems and having it go undetected. Malware, once enabled and initiated, spreads laterally like wildfire within your network, looking for sensitive assets. Your newly infected systems also begin to "call home" by sending beacons to the Command and Control (C&C) servers, which also use encryption. Once the malware finds the sensitive target data it is looking for, the data exfiltration begins using encryption. This renders your traditional Data Loss Prevention (DLP) systems ineffective, since they can't inspect encrypted traffic. At this point, the cyber criminals have won their game, while your business has lost valuable assets all without your knowledge. And to think you were just trying to protect your assets!

1: https://transparencyreport.google.com/https/overview?hl=en
2: https://blogs.cisco.com/enterprise/a-guide-for-encrypted-traffic-analytics
3: https://www.a10networks.com/sites/default/files/A10-EB-14106-EN.pdf
4: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

3.2 The Rise of Encrypted Threats: Ransomware

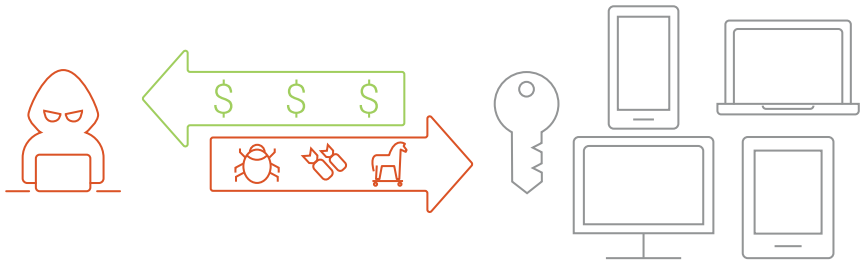
Ransomware is not a new thing; In fact, the first ransomware attack was carried out in 1989.[1] However, within the last few years there has been an increase in the number and scale of these type of attacks where your data is held for ransom. Just in 2018, 6 in 10 malware cybercrimes were ransomware.[2]

Ransomware is a form of malware that infects a target computer, encrypts some or all of the data on it, and gives the victim a message explaining how they can pay to get their data back. Most of the time, these ransomware attackers will use encryption to bypass your security stack, ensuring that the malware is delivered undetected to your network. Highly dangerous, it can be easily stopped by having the right security software block it before it even gets delivered to unsuspecting computers!

One of the largest ransomware attacks was WannaCry[3] in May 2017, that was estimated to have cost organizations as much as $4 billion[4]; over 2.6 times more than the total losses of such malware schemes in the previous year, which was estimated to be $1.5 billion. Included in the losses was lost productivity, and the cost of conducting forensic investigations and restoration of data, but it does not include lost revenue, brand reputation or stock devaluation which would make the losses even higher! With cybercrime damage costs projected to hit $6 trillion annually by 2021[5], you can expect ransomware losses to only increase.

Ransomware will cost the world $6 trillion annually

by 2021, up from $3 trillion in 2015.



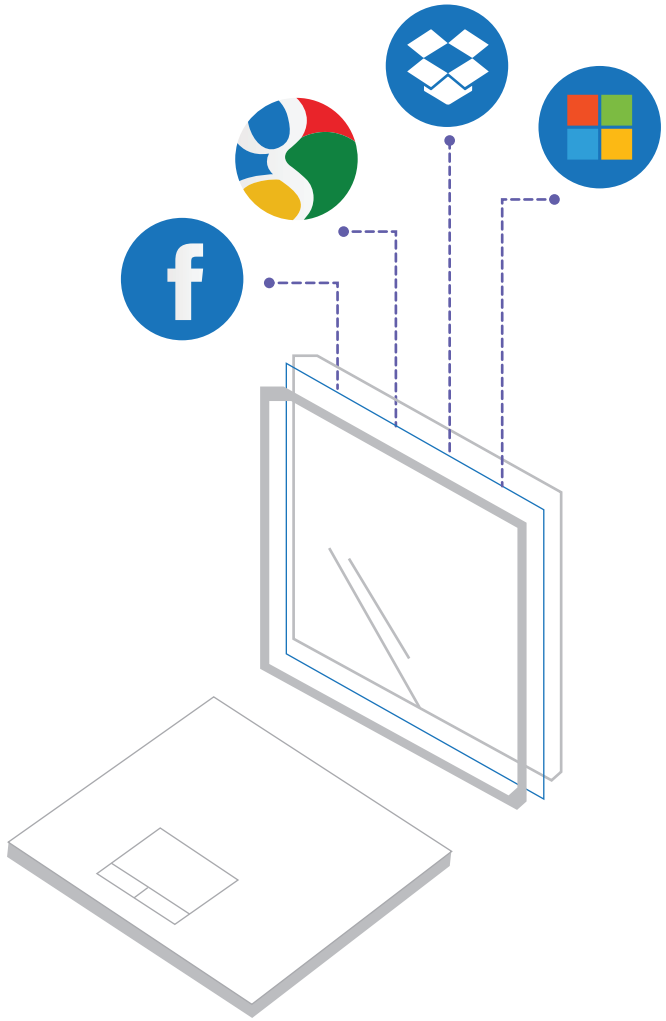
1: https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time#2
2: https://blog.barkly.com/ransomware-statistics-2018
3: https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html
4: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/
5: https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

3.3 The Rise of Encrypted Threats: Insider Threats

Insiders have many ways to avoid detection with 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, Office 365) makes data exfiltration easy to hide. According to a study by Cybersecurity Insiders and Crowd Research Partners, a majority (53%) of organizations where hit by five or less attacks in the previous 12 months and 27% felt that insider attacks have become more frequent.[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]

While that 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. It takes an average of more than 2 months to contain an insider incident and only 16% of incidents are contained in less than 30 days.[3]



1: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf
2: http://www.observeit.com/blog/how-major-telecom-company-stopped-data-theft-observeit
3: https://public.dhe.ibm.com/common/ssi/ecm/55/en/55017055usen/2018-global-codb-report_06271811_55017055USEN.pdf

HOW TO PROTECT AGAINST ENCRYPTED THREATS

4

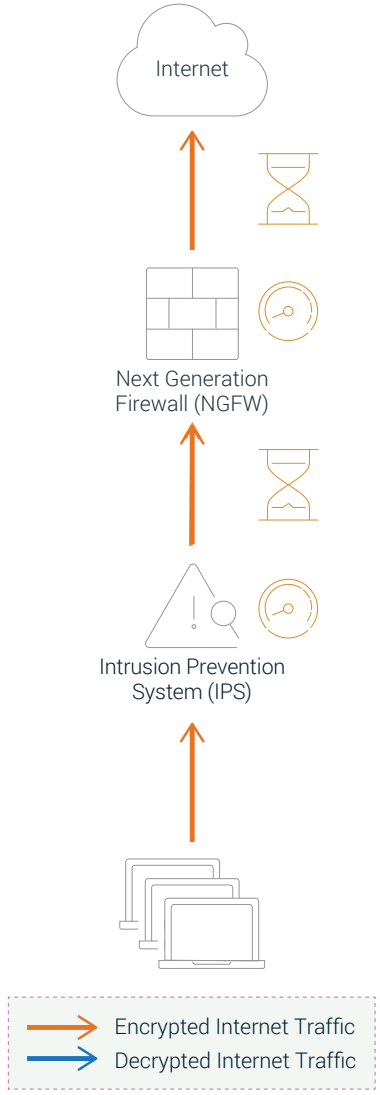
Protecting Against Encrypted Threats: Inline Protection

The most common and effective way of protection against network borne cyberattacks is to deploy an inline inspection solution like a firewall or Intrusion Prevention System (IPS). Since an inline inspection solution sits on the network perimeter, it can look at traffic flowing in and out of the network. This makes it effective at stopping attacks initiated from the outside, while protecting your users from downloading malicious files laced with viruses and malware.

With the rise in encryption, your legacy solutions can be rendered ineffective since they are not designed to decrypt, inspect and then re-encrypt traffic before sending the data on its way. Security vendors either depend heavily on software-based decryption on legacy solutions or produce Next Generation Firewalls (NGFWs) and Next Generation IPSs that support hardware-based decryption.

But the problem remains that these devices will suffer from severe performance degradation[1] when decryption is enabled. This also impedes them from focusing on their main job such as deep packet inspection (DPI) to find malware, etc. And the problem is multiplied if there are several inline inspection solutions deployed in a series on the network, since each device adds latency due to decryption, inspection and re-encryption. Point decryption solutions such as this can severely affect your network's performance and, in turn, your user experience. To address this, security vendors will release more expensive solutions, with higher capacity, to meet increasing decryption needs which may not scale and ultimately effects your return on investment.

Without a dedicated SSL/TLS inspection solution, you will have performance degradation at every appliance.



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

4.1 Protecting Against Encrypted Threats: Data Loss Prevention

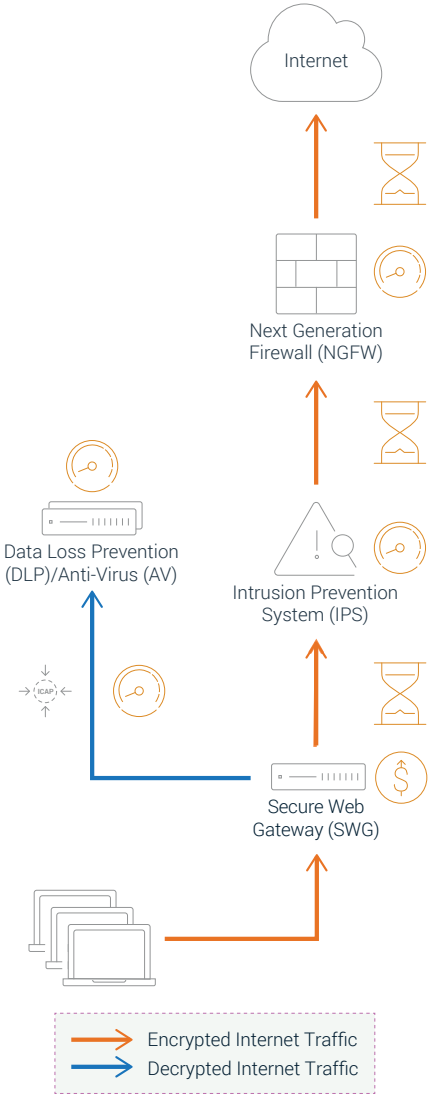
DLP has become one of the most important requirements in enterprise security. With the rise in data breaches, and stricter rules defined by regulations such as the EU's General Data Protection Regulation (GDPR), it is vital that illegitimate data exfiltration is blocked. Since DLP systems have become an essential part of your perimeter security, it is critical to understand the limitations that are introduced by the rise in encryption.

The most common way of deploying DLP systems in a network is by connecting it to a Secure Web Gateway (SWG), which can decrypt traffic for the DLP, enabling it to stop data exfiltration. These DLPs connect to the SWG using the Internet Content Adaptation Protocol (ICAP).

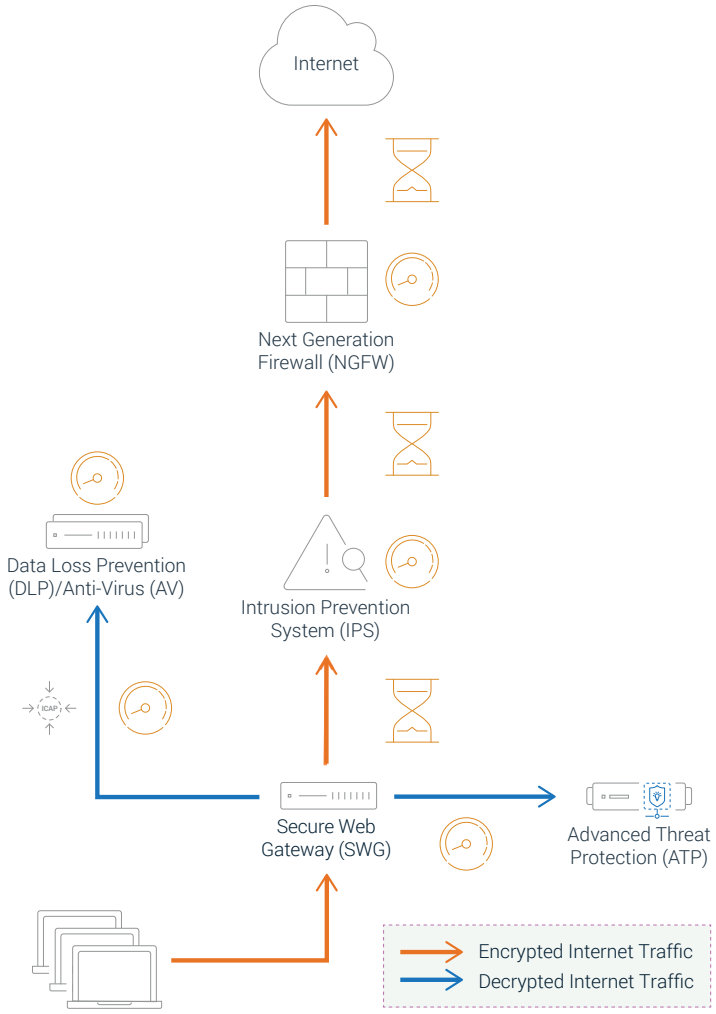
However, such a deployment can introduce several issues into the network. First, you need to have an existing SWG deployed in your network that can decrypt traffic and has the ability to support ICAP. Second, if you don't have an SWG or a decryption device that can support ICAP, you will have to invest in one to make sure that your DLP is not blind to encrypted traffic. Finally, you will have to make sure that your SWG can match your throughput requirements and does not create a bottleneck in the network since these systems are generally not made with a focus on performance, but rather protocol support.

Investing in a decryption solution that not only takes care of inline decryption at high speeds, but also has the ability to support your existing DLP systems using ICAP at no additional cost or with any additional latency just makes sense.

You have to buy an unnecessary SWG just to support ICAP for DLP systems increasing your TCO.



4.2 Protecting Against Encrypted Threats: Passive Inspection



Some network security solutions don't actively take part in threat prevention on the line, but they do play an important role on the side lines. These devices usually perform passive inspection and are deployed out-of-band.

Passive security devices like Advanced Threat Protection (ATP) systems, Security Information and Event Management (SIEM) solutions, or Intrusion Detection Systems (IDS) receive a copy of the traffic that is passing through the network. This traffic is analyzed by these devices and then network administrators are alerted when suspicious activity is detected. An out-of-band configuration does give you flexibility—providing visibility into a combination of conventional preventive security devices in addition to advanced detection and response solutions.

However, ATP systems are used to detect and stop Advanced Persistent Threats (APT) that keep looking for vulnerabilities before striking or malware that stays dormant before executing later at a pre-defined time only once a threat has been delivered into your network.

Therefore, without the ability to decrypt traffic, these passive security devices remain blind to threats that are delivered using the cover of encryption or malware that uses encrypted channels for C&C communications with malware handlers. You really need a solution that enables your security devices to protect your network from these encrypted threats before the threat is delivered to your network.

Passive security devices remain blind to threats that are delivered using the cover of encryption.

DEDICATED DECRYPTION
IS THE ANSWER

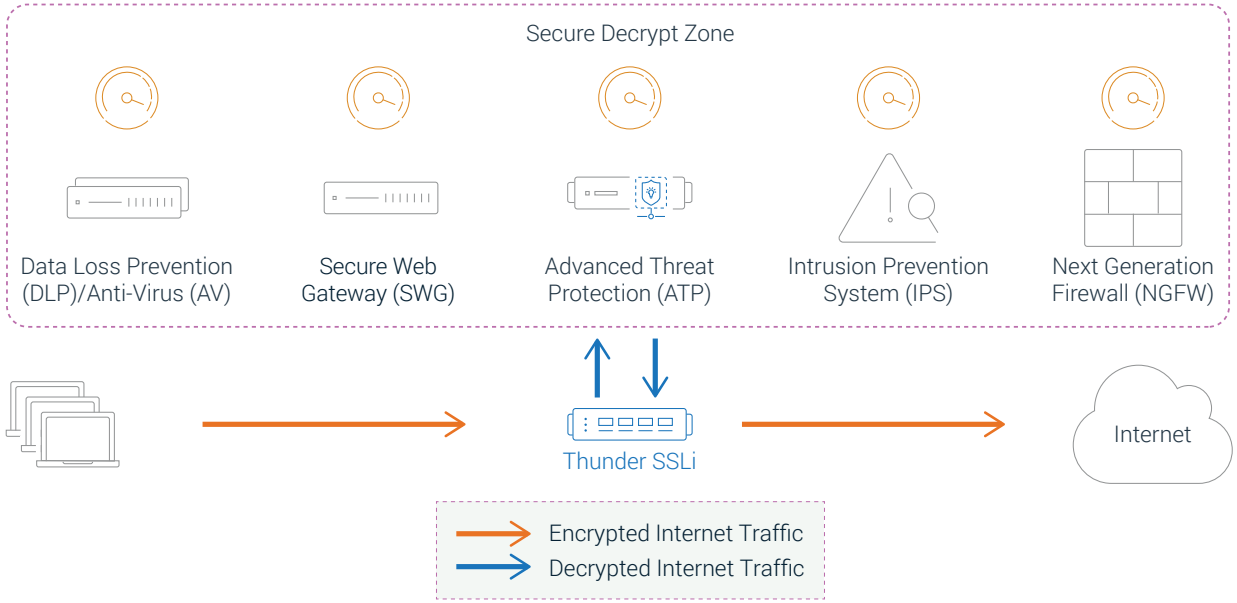
5

Dedicated Decryption: A10 Thunder SSL Insight Advantage

The A10 Thunder® SSL Insight® (SSLi®) appliance provides full visibility into encrypted traffic. It eliminates the blind spot, helping you to detect and neutralize potential threats that may be hiding behind encryption, ultimately lowering your risk of costly data breaches and malware infiltrations. Thunder SSLi also helps you meet your security compliancy with the continually evolving data protection and privacy standards, rules and regulations, such as the EU's GDPR and the healthcare industry's HIPAA Privacy Rule.

With dedicated SSL processors, Thunder SSLi boosts the performance of your security infrastructure, decrypting traffic once, 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. With the intrinsic ICAP support of Thunder SSLi, you can also rest assure your DLP systems are ready to stop data breaches. This dramatically reduces any latency or performance degradation introduced into your security infrastructure.

Thunder SSLi enables your existing security devices to inspect encrypted traffic with optimal performance, minimal latency, advanced analytics and maximizes your ROI.



5.1 Dedicated Decryption: A10 Thunder SSL Insight Advantage (Continued)

To get you up and running as fast and efficiently as possible, Thunder SSLi supports step-by-step configuration and troubleshooting wizards, and customized dashboards so that you can operationalize the device simply and easily, according to A10's recommended best security practices. Using the SSLi app on A10's Harmony Controller provides centralized analytics and a management console for multi-site deployments with rich insights into traffic decryption status, user behavior and traffic pattern analysis, thereby enabling you to take effective action whenever an anomaly is detected. This eliminates any complexity that might have been introduced into the network otherwise.

Thunder SSLi's unique solution provides the most cost-effective, compelling and scalable decryption security solution that will not only arm your existing security infrastructure for today's cyber threat landscape, but will future-proof your enterprise infrastructure to defend against the growth and evolution in cyber threats.

> *"The goal of our research is to demonstrate the value of good data protection practices, and the factors that make a tangible difference in what a company pays to resolve a data breach," said Dr. Larry Poneman, chairman and founder of Poneman Institute. "While data breach costs have been rising steadily over the history of the study, we see positive signs of cost savings through the use of newer technologies as well as proper planning for incident response, which can significantly reduce these costs."*

A10 THUNDER SSLi

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

▶ *LEARN ABOUT A10 Thunder SSLi*

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.

1-888-A10-6363 | a10networks.com

Part Number: A10-EB-14105-EN-02 OCT 2018