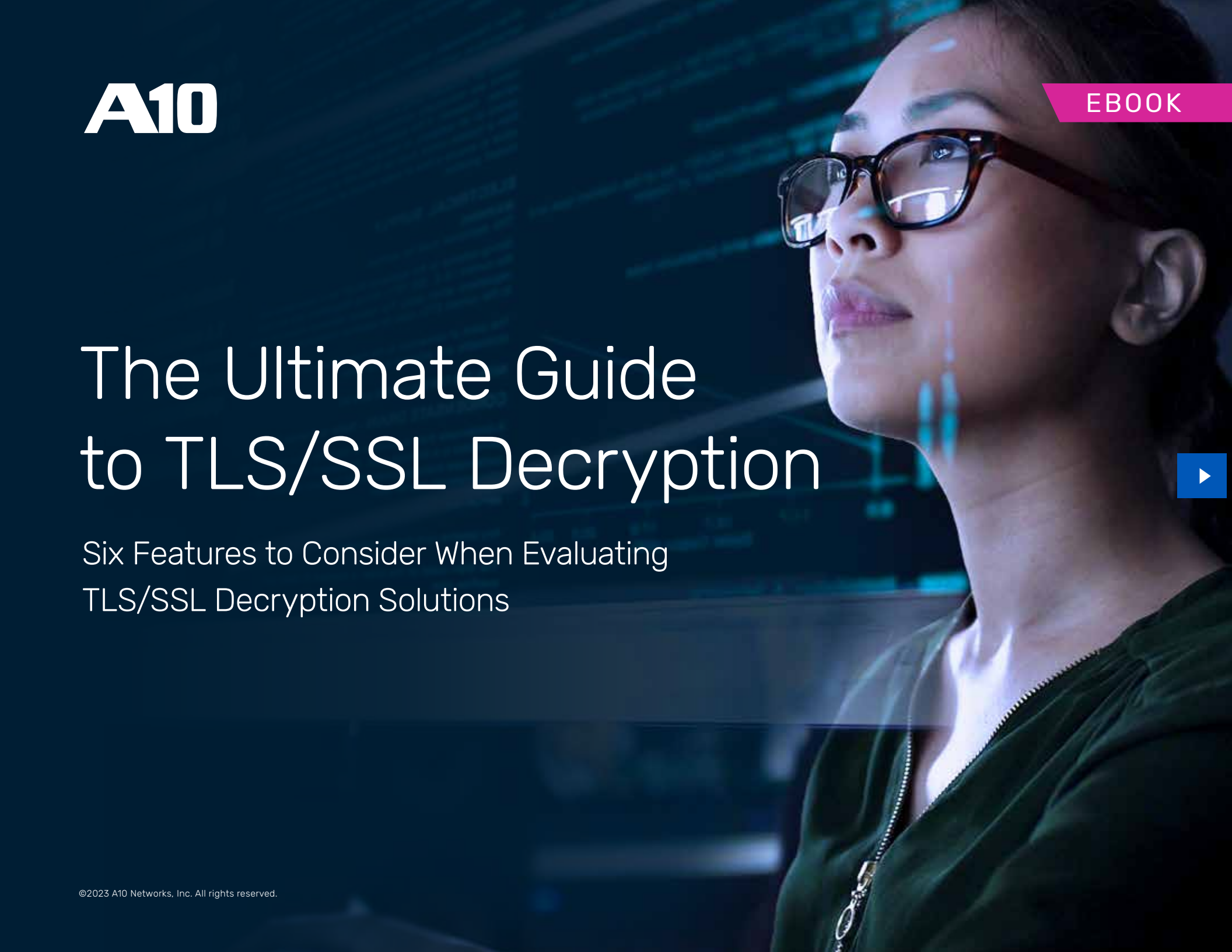


EBOOK

The Ultimate Guide to TLS/SSL Decryption

Six Features to Consider When Evaluating TLS/SSL Decryption Solutions

TABLE OF CONTENTS

THE CURRENT STATE OF INSECURITY

Encrypted traffic accounts for a large percentage of all internet traffic. While the adoption of Transport Layer Security (TLS) and Secure Sockets Layer (SSL), should be cause for celebration—as encryption improves confidentiality and message integrity—these protocols also put your organization at risk as they create encrypted blind spots that hackers can use to conceal their exploits from security devices that are unable to inspect TLS/SSL traffic.

Cybercriminals can use encryption to hide the delivery of malware, as well as the extraction of data, which leaves legacy security devices blind to data breaches. Such breaches can have a disastrous impact on your company's reputation and brand, and you could be subject to disciplinary action and fines. For example, a large-scale z attack targeted and severely affected the Colonial Pipeline, one of the largest pipeline operators in the United States, causing mass panic among consumers, supply shortages and even a rise in gas prices. This just goes to show how impactful modern day cyberattacks can be, bringing critical services to a halt. To prevent cyberattacks, enterprises need to inspect all traffic and encrypted traffic for advanced threats.

Worldwide spending on information security will exceed a staggering $211 billion by 2024 as organizations stack up security products around their network perimeters. Unfortunately, as SSL traffic increases, our collective $211+ billion investment in security is falling far short of protecting all our digital assets.

COLONIAL PIPELINE CO.

Colonial Pipeline paid close to $5 million in ransomware blackmail payment.

Attackers are wising up and taking advantage of this gap in corporate defenses. In fact, as much as 46% of malware attacks are using encryption as part of their delivery and communication mechanisms in 2021. As a result, companies that do not inspect SSL communications are providing an open door for attackers to infiltrate defenses and steal data.

46% OF MALWARE

attacks use TLS encryption to communicate with remote systems over the internet.

$211 BILLION

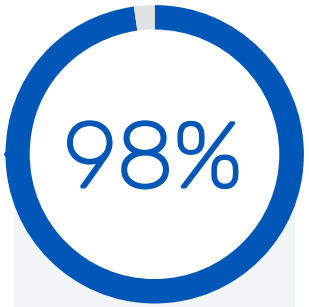
Worldwide spending on information security by organizations by 2024.

EVALUATING TLS/SSL DECRYPTION PLATFORMS SIX KEY FEATURES TO CONSIDER

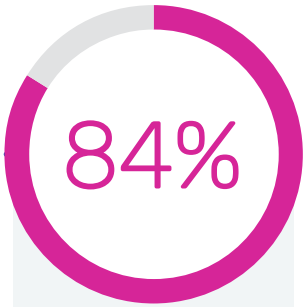
To eliminate the TLS/SSL blind spot in corporate defenses, you should provision a solution that can decrypt TLS/SSL traffic and enable all security products that analyze network traffic to inspect the encrypted data. You must carefully evaluate all the features and performance of your TLS/SSL decryption platform before selecting a solution. If you deploy an TLS/SSL decryption platform in haste, you might be blindsided later by escalating SSL bandwidth requirements, deployment demands or regulatory implications.

Because TLS/SSL decryption potentially touches so many different security products from firewalls and intrusion prevent systems (IPS) to data loss prevention (DLP), forensics, advanced threat prevention (ATP), and more, you should evaluate TLS/SSL decryption platforms against these criteria before selecting a solution. An TLS/SSL decryption platform should meet six key features.

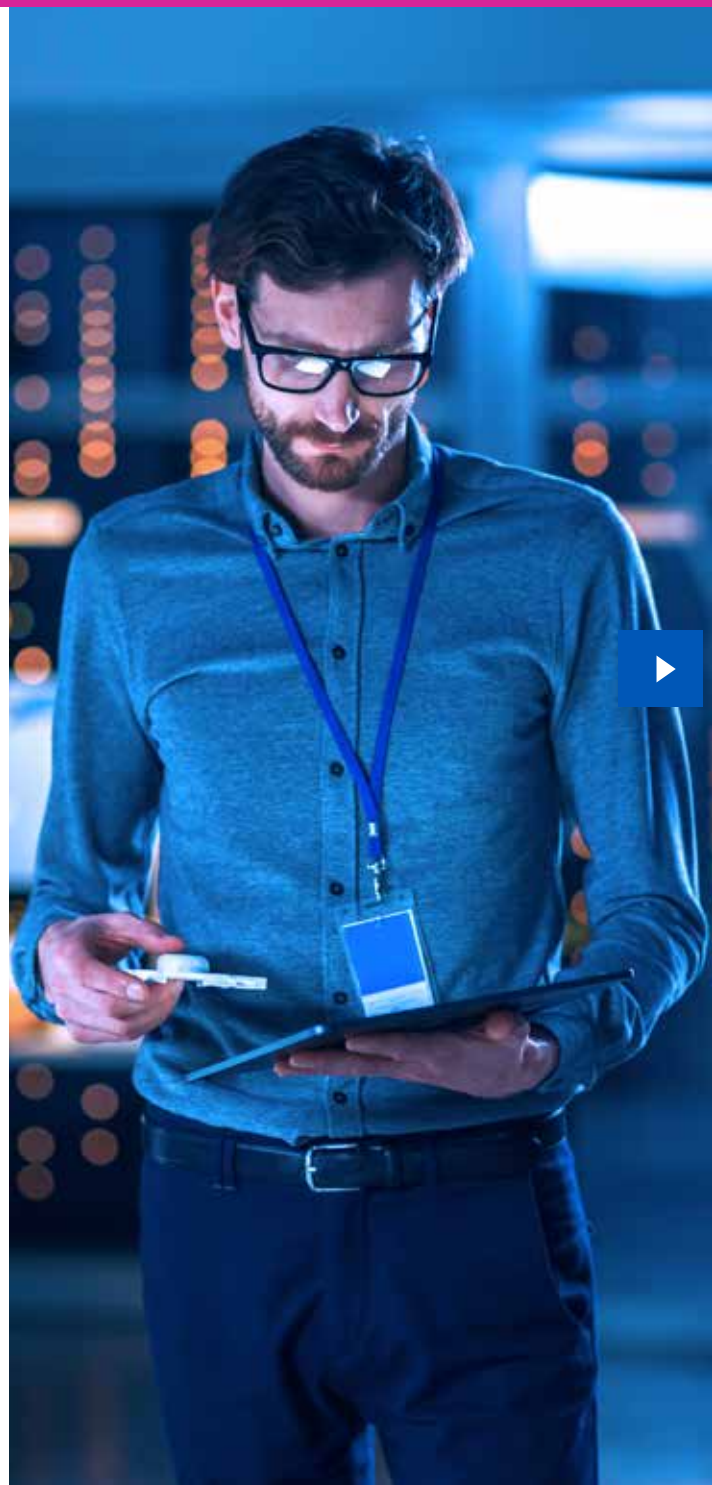
Percentage of internet traffic in North America currently protected by encryption



Percentage of pages loaded by Google Chrome using HTTPS



Percentage of webpages loaded by Firefox using HTTPS

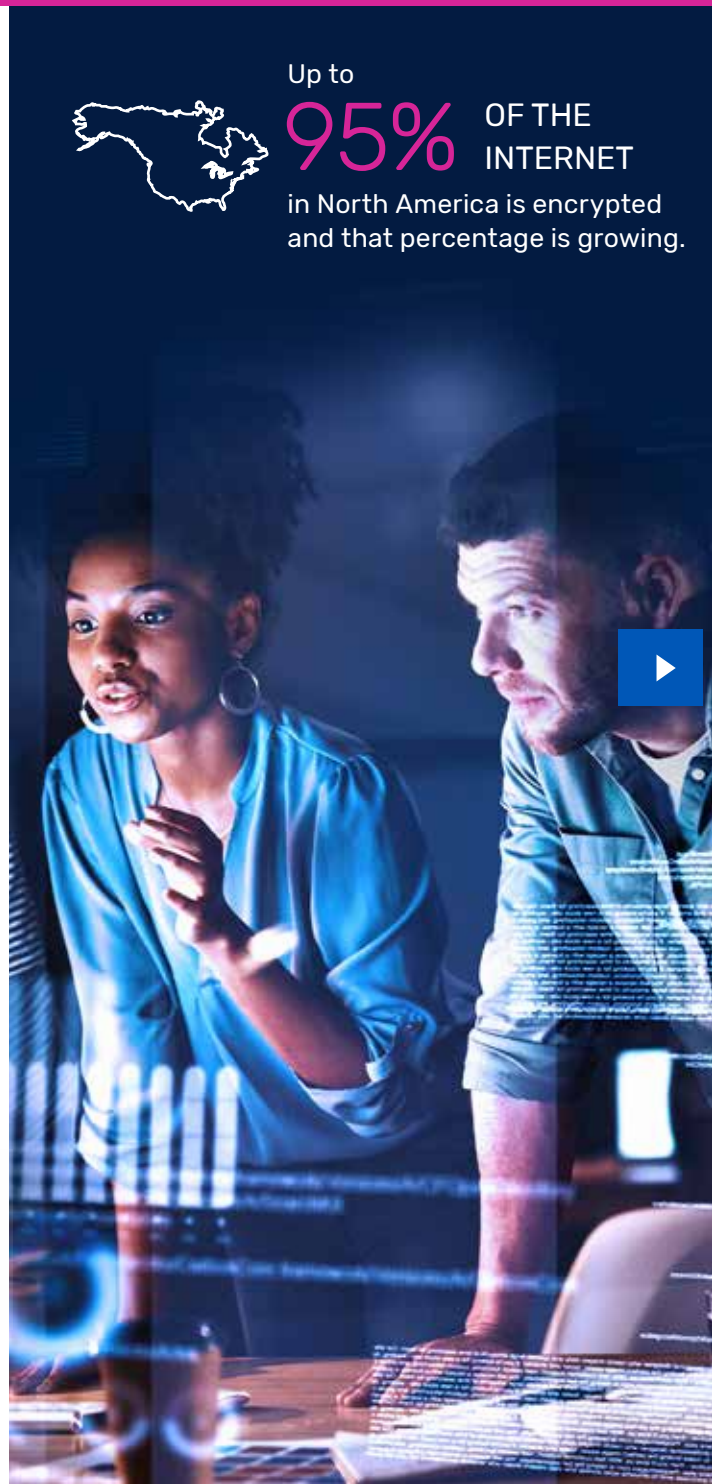


MEET CURRENT AND FUTURE TLS/SSL PERFORMANCE DEMANDS

Performance is one of the most important evaluation criteria for an TLS/SSL decryption platform. You need to assess current internet bandwidth requirements and ensure the decryption platform can also handle future SSL throughput requirements.

- Encrypted traffic is increasing faster than overall IP traffic growth, and more and more sites are using computationally intensive 2084-bit and 4096-bit SSL keys along with complex Elliptic-Curve Cryptography (ECC). Today, up to 95% of the internet in North America is encrypted and that percentage is growing, so you should factor SSL traffic growth into your criteria.
    - Test TLS/SSL decryption speeds with 2048-bit and 4096-bit SSL keys
    - Evaluate your organization's TLS 1.3 and QUIC usage
    - Make sure the TLS/SSL decryption solution has the ability to re-negotiate ciphers, especially weaker or deprecated ciphers to stronger ones, for continued security and availability
    - Ensure the TLS/SSL decryption platform can handle throughput requirements with extra headroom for traffic peaks and decrypt traffic across multiple ports and protocols
    - Analyze appliance performance with essential security and networking features enabled; testing TLS/SSL decryption speeds without considering the impact of deep packet decryption (DPI), URL classification, or other features enabled will not provide a clear picture of real-world performance

Basing an evaluation on these performance benchmarks should prevent surprises in your production environment.



SATISFY COMPLIANCE REQUIREMENTS

Privacy and regulatory concerns have emerged as one of the top hurdles preventing some organizations from inspecting SSL traffic. While your security team may have deployed a wide array of products to detect attacks, data leaks, and malware, and rightfully so, you have to walk a thin line between protecting your company's intellectual property without violating employees' privacy rights.

To address regulatory requirements like GDPR, HIPAA, Federal Information Security Management Act (FISMA), Payment Card Industry Data Security Standard (PCI DSS), and Sarbanes-Oxley (SOX), an TLS/SSL decryption platform should be able to selectively bypass sensitive traffic, such as traffic to banking and healthcare sites. The solution should also be able to track and record all user activity in detail and ensure a valid audit trail is established. Once sensitive traffic is bypassed, you can rest easy knowing that confidential banking or healthcare records will not be sent to security devices or stored in log management systems.

- **Categorize web traffic using an automated URL classification service:** by categorizing web traffic, communications to certain sites can be bypassed to ensure that confidential data remains encrypted
- **Filter traffic based on URL categories** to block access to known harmful websites
- **Support manually defined URL bypass lists** with hundreds of thousands of URL entries
- **Support automated IP reputation services** to block access to known bad resources for added security right off the bat
- **Display a customizable message to users** the first time they access the internet informing them that web traffic and encrypted traffic may be monitored for cyber threats and unauthorized activity

SUPPORT HETEROGENOUS NETWORKS WITH DIVERSE DEPLOYMENT AND SECURITY REQUIREMENTS

You have to contend with a wide array of security threats from external actors, as well as potential malicious insiders. Therefore, to safeguard digital assets, you need to deploy an ever-increasing number of security products to stop intrusions, attacks, data loss, malware, and more.

Decrypt traffic with multiple flexible deployment options.
A decryption platform should be able to support both transparent forward proxy configuration to transparently intercept traffic, as well as an explicit proxy configuration where browsers are explicitly configured to use an upstream proxy.

Intelligently route traffic with traffic steering.
The decryption platform should be able to forward traffic to multiple security devices based on source IP address, protocol, file type, URL, or other parameters. By supporting advanced traffic steering, an TLS/SSL decryption platform can optimize the performance of network security devices and support complex network architectures.

Granularly parse and control traffic based on custom-defined policies.
The support of scriptable, programmatic control over application traffic enables the decryption of request headers and payloads, plus performance of any number of actions, including blocking traffic, redirecting traffic, or modifying content.

Augment growing SaaS adoption.
A modern decryption solution should be able to differentiate between SaaS and non-SaaS traffic while supporting the rising volumes of SaaS traffic. It should have the ability to bypass SaaS traffic from the on-premises security stack, as is recommended by most SaaS vendors, and should be able to modify headers to support access control enforced by these SaaS vendors in the cloud to avoid data exfiltration.

Integrate with a variety of security solutions from leading security vendors.
By validating an decryption platform's interoperability, you can be assured the platform you choose will work seamlessly together with other security solutions and avoid surprises that could delay deployment. Integration with a variety of security solutions will also reduce overall costs and the need to deploy multiple point solutions.

MAXIMIZE THE UPTIME AND OVERALL CAPACITY OF YOUR SECURITY INFRASTRUCTURE

A security infrastructure blocks cyberattacks and prevents data exfiltration. If your security infrastructure fails, threats may go undetected and your company may be unable to perform business-critical tasks, resulting in loss of revenue and brand damage.

Most firewalls today can granularly control access to applications and detect intrusions and malware. Unfortunately, analyzing network traffic for threats is a resource-intensive task. While firewalls have increased their capacity over time, they often cannot keep up with network demand, especially when multiple security features like IPS, URL filtering, and virus decryption are enabled. Therefore, your TLS/SSL decryption platform should not just offload SSL processing from security devices but should maximize uptime and performance of these devices.

- **Scale security deployments** with load balancing
- **Avoid network downtime** by detecting and routing around failed security devices
- **Support advanced health monitoring** to rapidly identify network or application errors
- **Provide better value** by supporting N+1 redundancy rather than just 1+1 redundancy

Your TLS/SSL decryption platform should not be another point product and should not introduce risk to your network. Instead, it should lower risk by maximizing the availability and the overall capacity of your security infrastructure. Only then can the full potential of your TLS/SSL decryption platform be unlocked.

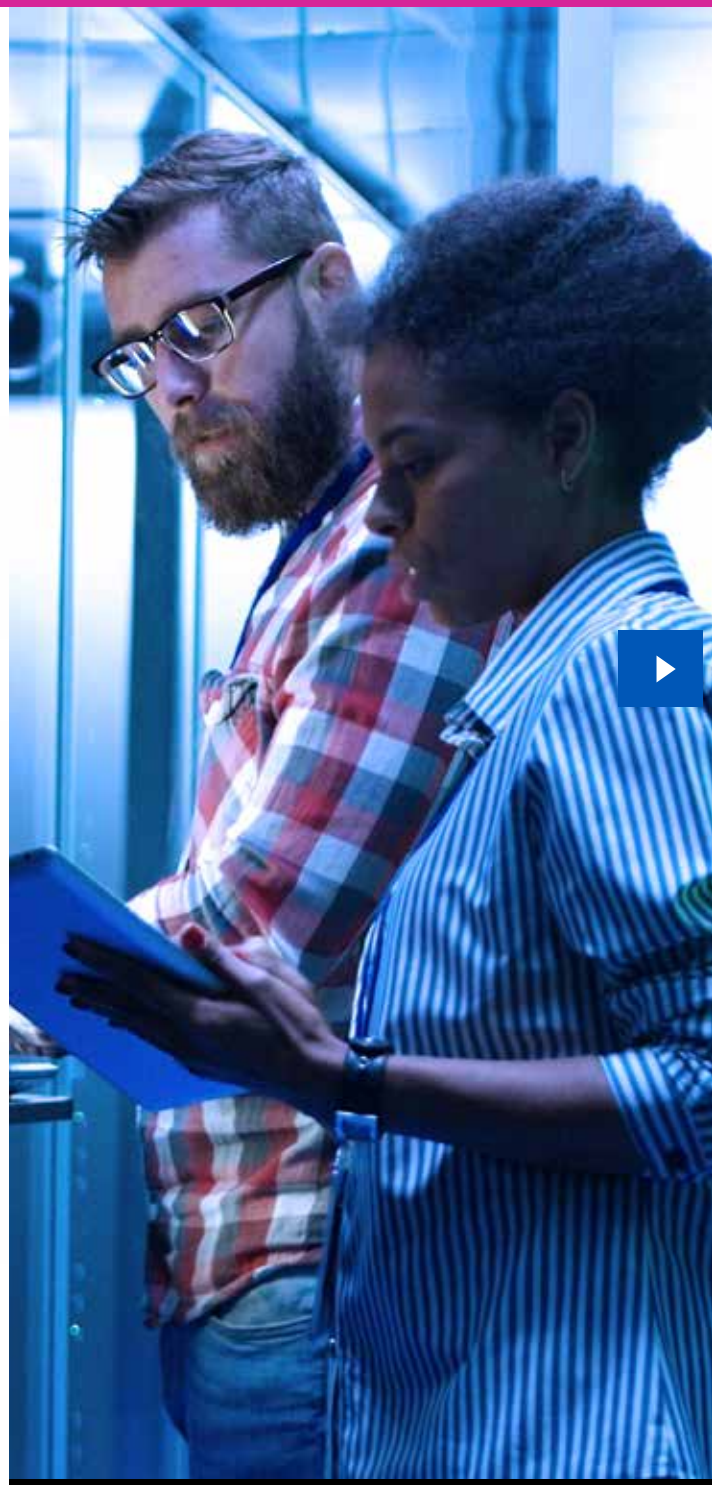
SECURELY MANAGE SSL CERTIFICATES AND KEYS

When providing visibility to SSL traffic, your TLS/SSL decryption solution must securely manage SSL certificates and keys. SSL certificates and keys form the basis of trust for encrypted communications. If they are compromised, attackers can use them for snooping on encrypted traffic and stealing data.

Provide device-level controls
to protect SSL keys and certificates

Integrate
with third-party SSL certificate management solutions to discover, catalog, track and centrally control certificates

Support FIPS 140-2 Level 2 and Level 3
certified equipment and hardware security modules (HSMs) that can detect physical tampering and safeguard cryptographic key



SIMPLIFY MANAGEMENT OF YOUR ENTERPRISE SECURITY SOLUTION

When investing in either a firewall or a decryption solution, two of the biggest problems are the complexity and the lack of rich usable analytics. A solution that can be easily deployed allows your organization to become operational and prevent hidden threats as soon as possible. Unfortunately, most decryption solutions are too complex to be deployed easily. If your solution is deployed quickly, usually after paying hefty professional services fees, more problems can emerge. Are the analytics provided with the solution humanly consumable and useful? Is the solution providing any usable insights?

When managing encrypted traffic, rich analytics with data delivered in an easy-to-consume format is critical in order to free up valuable human analysts to make effective and informed decisions. Real-time analysis provides deep insights into anomalies and threats in encrypted traffic, so adaptive controls and policy updates can be set through behavior analysis. Products from partners like Splunk may be deployed in your security network to capture insights into the traffic flowing through network devices.

Furthermore, as your organization grows and spreads to multiple, geographically distributed deployments, a 'single pane of glass' solution becomes necessary to provide management and analytics available at a single centralized location. Simplicity becomes a must. Make sure the platform:

- **Is easy to use** and can be deployed in minutes
- **Ensures the application of security best practices,** reducing human errors introduced during deployment
- **Provides detailed real-time analytics** that will help in advanced troubleshooting
- **Enables troubleshooting of issues** that you might have with the platform itself, with ease
- **Provides customizable dashboards** that deliver tailored statistics widgets
- **Provides a centralized management option** to support your organization as it grows, allowing all your geographically distributed deployments to be managed and analyzed from a central location

SUMMARY

As privacy concerns are propelling TLS/SSL usage, you face increased pressure to encrypt application traffic and keep data safe from hackers and foreign governments. In addition, because search engines such as Google rank HTTPS websites higher than standard websites, application owners are clamoring to encrypt traffic. At the same time, you face threats like cyberattacks and malware that can use encryption to bypass corporate defenses.

With SSL accounting for nearly 95 percent of enterprise traffic in North America and more applications supporting bigger keys and complex ciphers like ECC for PFS, you can no longer avoid the cryptographic elephant in the room. If you wish to prevent devastating data breaches, you must gain insight into your TLS/SSL traffic. Since legacy firewalls are inefficient at decrypting and inspecting traffic simultaneously, creating bottlenecks in your network, a dedicated TLS/SSL decryption platform that will support your existing security infrastructure is necessary.

Before provisioning an TLS/SSL decryption solution, consider criteria like performance, flexibility, analytics, ease-of-use, and secure key management, which are critical to your organization's success. Armed with this information, you can make a well-informed decision and avoid the deployment pitfalls that TLS/SSL decryption can potentially expose.

Contact us any time or request a free demo.

Read the latest white paper:
Zero Trust is Incomplete without TLS Decryption

Read Now

View the demo:
See the A10 Networks Difference for Yourself

Request a Demo

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

For more information, visit A10networks.com and follow us @A10Networks.

Learn More

About A10 Networks

Contact Us

A10networks.com/contact

Part Number: A10-EB-14146-EN-01 JULY 2023