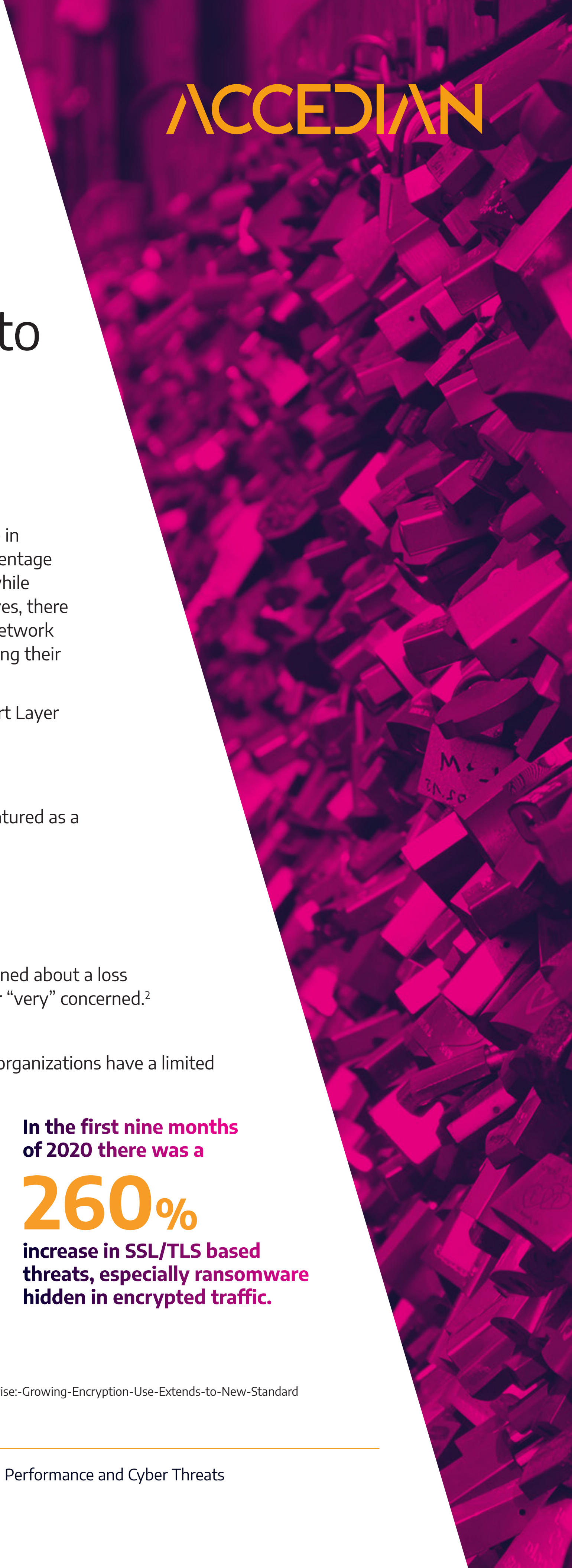


Solution Brief

Skylight TLS Decryption for Enhanced Visibility into Application Performance and Cyber Threats

Encryption is an unstoppable force. It's recommended as a best practice in leading privacy regulations, such as GDPR and CCPA, and the total percentage of encrypted web traffic is already estimated at over 90% today.[1] But while there are very good reasons to keep traffic flows hidden from prying eyes, there are also dangers. Without visibility, enterprises are unable to monitor network and application performance, or investigate if threat actors are also hiding their activity in encrypted tunnels.

That's why Accedian Skylight is evolving. We can now decrypt Transport Layer Security (TLS) to analyze everything, everywhere.

The pros and cons of TLS

TLS has been around for over two decades and over that time it has matured as a technology. Today, version 1.3 of the protocol offers users:

- **Confidentiality** – no-one can view the data
- **Integrity** – no-one can alter the data
- **Authentication** – to verify the legitimacy of clients/servers

In 2019 research, it was revealed that 91% of organizations were concerned about a loss of visibility related to encryption, with over a third (35%) "extremely" or "very" concerned.[2] What's driving this unease? Three key factors:

Application security monitoring – Without insight into traffic flows, organizations have a limited ability to spot and stop threats targeting critical applications.

Threat detection – As above, network detection and response (NDR) tools need visibility into traffic to work properly. The longer attackers are allowed to dwell inside networks without being spotted, the more damage they can do. It takes on average 280 days to identify and contain a breach today, with the average incident costing almost $3.9 million.[3] In the first nine months of 2020 there was a 260% increase in SSL/TLS based threats, especially ransomware hidden in encrypted traffic.[4]

In the first nine months of 2020 there was a

260%

increase in SSL/TLS based threats, especially ransomware hidden in encrypted traffic.

[1] Google, https://transparencyreport.google.com/https/overview
[2] EMA, https://www.enterprisemanagement.com/research/asset.php/3700/TLS-1.3-Adoption-in-the-Enterprise:-Growing-Encryption-Use-Extends-to-New-Standard
[3] IBM, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] ZScaler, https://info.zscaler.com/resources-industry-reports-state-of-encrypted-attacks

Skylight's decryption approach is focused on your security

Accedian has taken care to ensure that our decryption capabilities present no additional cyber risk to customer organizations. In fact, Skylight TLS decryption:

- Requires the permission of the network owner before it can start decrypting traffic
- Will ensure traffic remains encrypted right up to the decryption box, for maximum security
- TLS keys expire very quickly (minutes or hours), after which time they will no longer be usable

Application performance troubleshooting – It's not just a case of managing cyber-risk. TLS encryption means organizations are also flying blind with regards to the performance of critical applications. Without visibility at this layer, they're unable to manage Quality of Experience (QoE) for end customers or fix problems proactively.

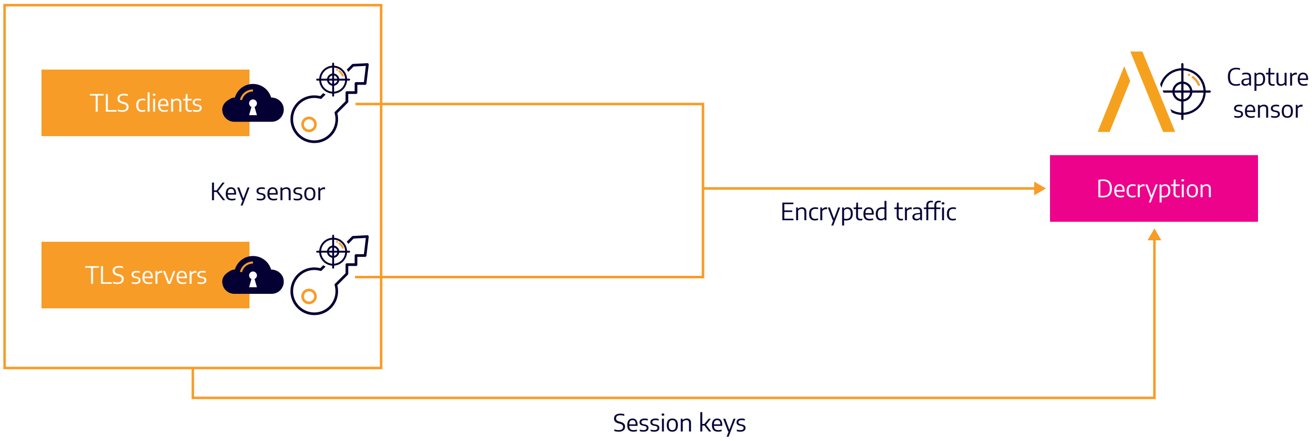
In short, a lack of visibility into TLS traffic could lead to:

- Customer churn
- Increased breach costs – IT forensics and remediation, legal, regulatory fines, etc.
- Reputational damage – from poorly performing apps and over-notification of breaches to regulators
- Ransomware costs – unable to clarify what was stolen, victim organizations would have to 'trust' the threat actors' claims

Skylight TLS decryption: how it works

Accedian Skylight can restore full visibility into traffic at the network and application layer for any TLS version. The secret is a key sensor, a small software-based agent that can sit on any client or server. For every TLS session, this sensor will monitor memory and pick out the symmetric encryption key. A decryption box receives the still-encrypted traffic and these keys to decrypt the whole TLS communication from the payload. It's fast, efficient, and made possible with only a small CPU footprint.

The traffic is then sent to the Skylight capture sensor for analysis, where intelligent algorithms are applied to unlock insight into application and network performance, and security risk.



The advantages of Skylight TLS decryption

With these new decryption capabilities, Skylight users gain the following benefits:

- Decryption functionality works for all TLS versions
- Supports major platforms: Windows server and desktop, Linux server, Kubernetes, Docker containers
- Capturing of symmetric session keys is fast and efficient (just picking keys from memory) with a small CPU footprint
- Free from certificate or server key dependency – key sensors can be installed on the server or client side, so even if you don't control the server you can still decrypt and monitor all traffic
- Enhanced security through limited lifespan of the session keys, and the fact that traffic remains encrypted until it reaches the decryption box
- Decryption of traffic is fast and efficient – and can be scaled to hundreds or thousands of sensor instances and hundreds or thousands of applications
- Capture performance is on par with Skylight performance without decryption (around 10Gbps)

Driving performance assurance and enhanced security

With TLS decryption, customers get the best of both worlds: all the security of TLS encryption plus enhanced insight into traffic to improve risk management and performance monitoring.

The business value of this approach drives:

- Low operational cost – simple to deploy and manage
- High scalability – can grow with your company's needs
- Flexibility of management – in the cloud, on-premises, or in hybrid environments
- Greater visibility means best-in-class insight into traffic performance for QoE and effective troubleshooting
- Visibility into TLS traffic unlocks threat detection and application security capabilities to minimize cyber risk

Despite their concerns over visibility, 97% of organizations said in 2019 they would implement TLS 1.3 within 18 months.[5] Now they can do so whilst maintaining application performance and security.

[5] EMA, https://www.enterprisemanagement.com/research/asset.php/3700/TLS-1.3-Adoption-in-the-Enterprise:-Growing-Encryption-Use-Extends-to-New-Standard

About Accedian

Accedian is the leader in performance analytics, cybersecurity threat detection and end user experience solutions, dedicated to providing our customers with the ability to assure and protect their digital infrastructure, while helping them to unlock the full productivity of their users.

Learn more at accedian.com

Accedian | 2351 Blvd. Alfred Nobel, N-410 | Saint-Laurent, QC H4S 2A9 | 1 866-685-8181 | **accedian.com**