Eliminate Blind Spots in SSL Encrypted Traffic

Your Threat Detection Can Miss Up to 50% of Network Attacks If All Keys and Certificates Are Not Delivered for SSL Traffic Decryption

The Facts

SSL/TLS Makes Up 15% to 25%

Of the total web traffic[1]—for many businesses its over 50%

50% of Network Attacks

Will use SSL by 2017 according to Gartner[1]

51% of Organizations

Are unaware of how many keys and certificates are in use[2]

700% Growth

In certificate-enabled malware from 2012 to 2015 according to Intel Security[3]

Almost $400 Million

Is the total possible impact of an attack on trust[2]

SSL Visibility Challenges

While SSL/TLS provides privacy and authentication, it also creates a blind spot for enterprise security. Cybercriminals can use SSL to hide their exploits from an organization's security controls, including Next Generation Firewalls (NGFW), Intrusion Prevention Systems (IPS), Unified Threat Management (UTM), secure gateways, Data Loss Prevention (DLP), anti-malware solutions, and more. Cybercriminals use SSL/TLS to hide attacks, evade detection, and bypass critical security controls.

Gartner estimates that by 2017, more than 50% of network attacks will use SSL/TLS.[1] Most organizations lack the ability to decrypt and inspect SSL communications to detect these threats. This blind spot undermines traditional layered defenses and creates an unacceptable risk of breach and data loss. For example, less than 20% of organizations with a firewall, IPS, or UTM appliance decrypt SSL traffic.[1] That means 80% of these organizations might be allowing cybercriminals to leverage SSL tunnels to sneak malware into their network, hide command-and-control traffic, and pilfer sensitive data.

Impact of SSL Blind Spots

With no visibility into encrypted SSL traffic, organizations are at risk of attacks that can result in stolen data, compromised systems, lost revenues, and long-term damage to business reputation.

- **No key and certificate discovery.** Today's average enterprise holds over 17,800 certificates, but over 50% of organizations are unaware of how many certificates they have in use.[2] The inability to find and access all keys and certificates restricts the ability to decrypt SSL traffic and inspect for malicious content.
- **No way to distribute keys.** The scope and size of distributing keys and certificates have put off many administrators trying to setup decryption systems. And the process of collecting and distributing keys can introduce new security and compliance risks if not handled properly.
- **No way to stay updated.** Decryption systems must be kept up to date as certificates expire or are renewed or replaced. Otherwise, the amount of decrypted traffic will decrease and blind spots and risk will grow.

VENAFI

To learn more visit
Venafi.com/SSLVisibility

Maximizing the SSL/TLS traffic that can be decrypted and inspected eliminates blind spots, strengthening your layered security defenses and protecting your business against trust-based attacks.

Maximize SSL Decryption

Bad guys are increasing their misuse of SSL/TLS, but most organizations have not calculated this into their planning. The ability to quickly decrypt and inspect SSL traffic in real time and detect threats is imperative.

Many security systems now perform high speed SSL/TLS decryption. But these systems cannot decrypt traffic if they don't have access to keys and certificates. To eliminate blind spots in encrypted traffic, you need to secure your keys and certificates. Otherwise, your other security controls become less effective and leave the door open to cybercriminals.

Complete Visibility

- Detection of all keys and certificates
- Established ownership and control

Enforced Policy and Monitoring

- Flexible criteria such as certificate lifetime, authorized CA, and more
- Continuous monitoring for updates

Automated Distribution

- Automated, secure distribution of key and certificates to decryption systems
- Automated validation that keys are working and enabling decryption

Decrypting SSL/TSL traffic gives security tools the clear-text visibility they need to enforce protection. This strengthens security controls such as NGFW, IDS/IPS, and DLP, and increases their effectiveness and value.

Venafi Trust Protection Platform

Deployed with Venafi TrustAuthority™ and Venafi TrustForce™, the Venafi Trust Protection Platform™ works to eliminate blind spots from encrypted threats by safely delivering trusted keys for SSL decryption and threat protection.

Venafi TrustAuthority

Enables Complete Visibility

- Identifies all keys and certificates across enterprise networks, the cloud, and across multiple CAs
- Monitors continuously for updates and misuse

Enforces Policies & Workflows

- Provides flexible criteria such as certificate lifetime, authorized CA, and more
- Enforces configurable workflows for replacement, issuance, and renewal
- Provides a policy-enforced, web-based, self-service portal for SSL certificate requests and renewals

Venafi TrustForce

Automates Policy & Remediation

- Automates the entire issuance and renewal process
- Distributes keys and certificates to decryption systems automatically
- Validates certificates are installed and working for decryption
- Integrates with leading decryption systems, including A10, Blue Coat, and Palo Alto networks
- Replaces SSL certificates in seconds, integrating with dozens of CAs

Eliminate Blind Spots

To combat the threat of SSL/TLS encryption blind spots, companies need to decrypt SSL traffic and pass the content to security devices for further processing, analysis, and policy administration. With Venafi, robust key and certificate management maximizes the encrypted traffic that can be decrypted and inspected. Venafi integrates with leading SSL decryption systems, NGFW, IPS, UTM, secure gateways, DLP, anti-malware solutions, and more, to automate the entire process of distribution, installation, and validation, eliminating the blind spots in your threat detection strategy.

About Venafi

Venafi is the leading cybersecurity company in Next Generation Trust Protection. Venafi delivered the first trust protection platform to manage, secure, and protect keys and digital certificates that every business and government agency depends on for secure communications, commerce, computing, and mobility.

1. D'Hoinne, Jeremy and Hills, Adam. Gartner. *Security Leaders Must Address Threats from Rising SSL Traffic*, December 9, 2013. Gartner RAS Core Research Note: G00258176.
2. Ponemon Institute. *2013 Annual Cost of Failed Trust Report: Threats & Attacks*. 2013.
3. Intel Security. *McAfee Labs Threats Report*. November 2014.

Part number: 1-0036-0215

VENAFI

To learn more visit
Venafi.com/SSLVisibility