Achieve Successful Data Protection

Automate and validate risk reduction when activating more encryption and digital certificates

The Facts

SSL/TLS Comprises 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]

Over 3X Increase in Malware Signed
With legitimate certificates between 2012 and 2013[2]

Almost $600 Million
Is the total possible impact of an attack on trust[3]

Data Protection Challenges

The rampant rise in cyberattacks and the growing concerns (and regulations) over data privacy are combining to compel the increased use of SSL/TLS. And with Google prioritizing search results for sites using HTTPS, the drive to activate and expand encryption is gaining support from all types of business. But turning on SSL/TLS to encrypt data transmission and authenticate web servers, application servers, load balancers, and other applications can be a difficult task for any IT security and operations team.

With the average Global 2000 organization already using almost 24,000 SSL/TLS keys and certificates,[3] managing the deployment of even more SSL/TLS to protect data is challenging for most organizations. System administrators need to generate keys and request certificates, as well as oversee installation and configuration. Yet even more difficult is validating deployment and tracking progress to demonstrate an increase in data protection and reduced risk.

Impacts of More Encryption

More SSL/TLS and digital certificates create new risks and challenges to your business.

- **Expiring certificates:** Digital certificates expire and—and this disrupts the systems they were installed to protect. Expirations create outages which lower productivity and cause lost revenue, profits, and customers.
- **Lack of visibility:** Today's average enterprise holds almost 24,000 certificates, but the real issue is 54% are unaware of how many certificates they have in use, where they are used, and who owns them.[3] These issues will only increase with more use of SSL/TLS.
- **Increase in misuse:** As cyberattacks on certificates escalate, not knowing which certificates are trusted and who is responsible for them is a serious security issue. For four years running, 100% of the Global 5000 surveyed have responded to attacks on keys and certificates.[3]

VENAFI™

To learn more visit
Venafi.com/DataProtection

Pervasive SSL/TLS can address data security and privacy requirements, but only if the SSL/TLS keys and certificates are securely managed and protected.

- **Use of SSL/TLS to exfiltrate stolen data:** Bad guys are using SSL/TLS to cloak their activities with Gartner predicting that by 2017, 50% of network attacks will use SSL/TLS.[1] Turning on SSL visibility and decryption can protect against this, but keys and certificates must be secured and distributed to decryption appliances.

Protecting SSL/TLS Keys and Certificates

With effective key and certificate security and management, organizations can rapidly deploy SSL/TLS to meet data security and privacy goals, while validating that keys and certificates are protected and used correctly across the network.

Complete Visibility

- Continuous detection and monitoring of all keys and certificates
- Single management platform for auditing and reporting

Enforced Policies and Workflow

- Flexible criteria such as certificate lifetime, authorized CA, and more
- Automated workflow for issuance, renewal, installation, and validation

Automated Management and Security

- Policy-enforced, self-service portal for certificate issuance and renewal
- Automated renewal—installation, configuration, and validation in seconds, preventing errors and saving corporate resources
- Quick recovery from CA compromises as per NIST[4]

Venafi Trust Protection Platform

With Venafi TrustAuthority™ and Venafi TrustForce™, Venafi Trust Protection Platform enables you to successfully apply more data protection by securing your SSL/TLS keys and certificates—automating and validating risk reduction in your data security and privacy projects.

Venafi TrustAuthority

Ensures Visibility

- Identifies all keys and certificates across enterprise networks, the cloud, and multiple CAs
- Uses a baseline to identify misuse

Enforces Policies and Workflows

- Provides a policy-enforced, web-based, self-service portal for certificate requests and renewals
- Offers real-time dashboards and detailed reporting to track progress

Venafi TrustForce

Automates Management and Security

- Automates and validates the entire issuance and renewal process
- Replaces certificates in seconds, integrating with dozens of CAs
- Remediates across thousands of certificates in just hours in the event of a CA compromise or new vulnerability such as Heartbleed

SSL/TLS for Data Security

Left unprotected, cybercriminals use keys and certificates to be authenticated, evade detection, and keep their activities cloaked. But with a solution that identifies, continuously monitors, enforces policies, delivers self-service and validates the effective use of keys and certificates—as well as automates remediation—you can safely expand and rely on SSL/TLS to achieve data security and privacy.

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] McAfee. *McAfee Labs Threats Report. Fourth Quarter 2013.*

[3] Ponemon Institute. *2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point.* 2015.

[4] Turner, Paul, Polk, William, and Baker, Elaine. National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL). *Preparing for and Responding to Certification Authority Compromise and Fraudulent Certificate Issuance.* July 2012.

[5] Shey, Heidi, et al. Forrester Research. *Predictions 2015: Data Security and Privacy Are Competitive Differentiators.* November 12, 2014.

Part number: 1-0033-0315

VENAFI

To learn more visit
Venafi.com/DataProtection