Remediate SSL/TLS Key and Certificate Audit Failures

Achieve audit success, closing security gaps and stopping outages

The Facts

Over 23,000 Keys and Certificates
Are in today's average enterprise[1]

54% Are Unaware
Of where all of their keys and certificates are located[1]

50% of Network Attacks
Will use SSL by 2017 according to Gartner[2]

100% Already Compromised
By an attack on keys and certificates in each G5000 enterprise surveyed[1]

Almost $600 Million
Is the total possible impact of an attack using keys and certificates[1]

2.3 Certificate-related Outages
Is the average per organization over the last 2 years[1]

$15 Million
Is the total possible impact per outage[1]

SSL/TLS Audit Failures

SSL/TLS audits are an organization's opportunity to assess the risk of an SSL/TLS-related outage or compromise and remediate. As SSL/TLS usage increases for privacy and authentication, cybercriminals are exploiting trusted SSL/TLS connections and expired certificates are impacting availability.

Organizations are often unable to demonstrate SSL/TLS compliance to corporate and industry policies and regulations due to a lack of visibility. They don't know where their SSL/TLS keys and certificates are located, how they are used, or who owns them.

Audit findings also commonly indicate an inability to monitor keys and certificates, enforce policy, or maintain effective management. This results in the use of unauthorized certificate authorities (CAs), improper certificate configuration, a lack of rotation, expired certificates, weak key algorithms, the use of self-signed certificates, and more, causing security incidents and outages. And when organizations remediate, they are unable to validate enforcement and report on progress.

Impacts on SSL/TLS Audits

With bugs like Heartbleed, POODLE, and Shellshock eroding the trust established by keys and certificates and outages costing millions, SSL/TLS audit findings have new significance.

Lack of visibility: An average enterprise holds over 23,000 keys certificates and 54% admit to being unaware of where all of their keys and certificates are located.[1]

Expired certificates: All organizations surveyed had 2 or more certificate-related outages over the last 2 years with a total possible impact of $15 million per outage.[1]

Key and certificate misuse: Cybercriminals misuse keys and certificates to hide in encrypted traffic, steal data, and bypass security, and 100% of enterprises surveyed responded to these attacks within the last 2 years with a total possible impact of $600 million per attack.[1]

Unable to veryfiy compliance: Industry regulations and standards, such as PCI DSS and NIST, now explicitly address SSL/TLS security, requiring a complete key and certificate inventory.

VENAFI™

To learn more visit
Venafi.com/SSLAudit

SSL/TLS audit findings provide an opportunity for organizations to assess how they enforce SSL/TLS certificate issuance, renewal, replacement, and authorization to close security gaps and stop outages.

Successful SSL/TLS Audits

For meaningful SSL/TLS audit results, organizations must first have complete visibility into their SSL/TLS key and certificate inventory. From there, an SSL/TLS audit can evaluate certificate ownership and compliance with policies and regulations.

To ensure that audit remediation offers on-going security and availability, organizations must be able to continuously monitor SSL/TLS keys and certificates, enforce policies and workflows, automate certificate lifecycle processes, and deliver on-demand reporting that shows compliance status and remediation progress.

Venafi Trust Protection Platform

The Venafi Trust Protection Platform, with Venafi TrustAuthority™, Venafi TrustForce™, and Venafi TrustNet™, enables SSL/TLS audit success and fast audit remediation to avoid outages and maintain an effective cyberdefense.

Just like the human immune system, an SSL/TLS audit must be able to identify what is "self" and trusted and what is not and dangerous. Venafi is the Immune System for the Internet, identifying what keys and certificates are trusted, protecting those that are trusted, and fixing or blocking those that are not.

Venafi TrustAuthority

Ensures Complete Visibility

- Identifies all keys and certificates across networks, cloud instances, CAs, and trust stores
- Centralizes inventory and management for auditing and reporting
- Responds to audit requests and tracks remediation progress in real-time dashboards and reporting

Enforces Policies and Workflows

- Provides flexible policy criteria
- Issues notifications of expiring certificates
- Enforces configurable workflow capabilities for replacement, issuance, and renewal

Venafi TrustForce

Automates Management and Remediation

- Automates and validates the entire issuance and renewal process
- Replaces certificates in seconds and remediates across thousands of certificates in just hours for fast audit remediation

Venafi TrustNet

Identifies Incidents and Remediates

- Establishes global certificate reputation
- Identifies certificate misuse such as stolen certificates used for spoofed websites
- Remediates immediately through certificate whitelisting and blacklisting

SSL/TLS Audit Remediation Ensures Trust

Organizations rely on SSL/TLS certificates to establish trust in communications, authentication, and authorization. With Venafi, you can secure your SSL/TLS keys and certificates to maintain this trust with your customers and partners. Venafi identifies and fixes SSL/TLS certificate vulnerabilities, enforces enterprise policies, and monitors for certificate misuse. This enables successful SSL/TLS audits and fast, effective remediation, helping to ensure security and availability.

About Venafi

Venafi is the market-leading cybersecurity company that secures and protects keys and certificates so they can't be used by bad guys in attacks. Venafi provides the Immune System for the Internet, constantly assessing which keys and certificates are trusted, protecting those that should be trusted, and fixing or blocking those that are not.

1. Ponemon Institute. *2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point.* 2015.
2. D'Hoinne, Jeremy and Hils, Adam. Gartner. *Security Leaders Must Address Threats from Rising SSL Traffic.* Gartner RAS Core Research Note G00258176. December 9, 2013.

Part number: 1-0044-0615

VENAFI™

To learn more visit
Venafi.com/SSLAudit