

## The SSL Store™ Venafi Driver

### PKI Certificate Management powered by The SSL Store™



As a leader in web-security, The SSL Store™ is the first ever SSL reseller to partner with the Venafi Trust Protection Platform to bring automated SSL encryption to enterprises. Venafi's secure communication platform, powered by The SSL Store™ driver, gives enterprises the ability to automatically update and replace weak or fraudulent keys and certificates to avoid unplanned security outages at a fraction of the cost of a traditional MPKI platform.

## Discover, automate and continuously monitor your entire SSL network

### Visibility



- ✓ Discover the configuration, location, and use of every key and certificate
- ✓ Quickly create an accurate inventory with cloud-based, agentless scanning
- ✓ Achieve compliance and audit success
- ✓ View internal and external certificates from all Certificate Authorities
- ✓ Analyze your network by integrating with multiple SIEM systems

### Automation



- ✓ Automatically correct vulnerabilities, misconfigurations, and CA errors
- ✓ Manage certificate lifecycles across all six leading certificate authorities
- ✓ Automate certificate remediation
- ✓ Define your own workflows and change certificate management controls
- ✓ Automate certificate replacement and key rotation to prevent outages

## Accelerate Network Protection



Quickly find network weaknesses



Simplify certificate/key management



Rapidly procure new certificates



Automate certificate requests



Instantly blacklist untrusted CA's



Enable bulk certificate remediation

## Optimize

- ✓ Improve operating efficiency
- ✓ Reduce labor expenses
- ✓ Access the lowest PKI pricing on the market
- ✓ Recover data storage space

The Venafi Trust Protection Platform, in partnership with The SSL Store™, provides enterprise-wide visibility of all keys and certificates regardless of the issuing CA. Using advanced automation protocols, the Venafi PKI management system allows businesses to comprehensively manage all SSL certificates and identify malicious activity within their network.



## Automate crucial SSL workflows

- ✓ Automatically find, revoke, or change and re-validate compromised certs
- ✓ Automate requests for security certificates and certificate renewals



## Improve network control and visibility

- ✓ Scan local systems to retrieve certificates in file systems and key stores
- ✓ Issue, manage, and renew certificates with certificate monitoring tools



## Establish certificate reputation

- ✓ Reveal the misuse of keys and certificates through reputation scores
- ✓ Establish and maintain certificate trust created by keys and certificates



## Maintain organizational compliance

- ✓ Apply security guidelines to validate key or certificate trustworthiness
- ✓ Ensure your certificate environment remains organized and audit-ready



## Secure numerous digital assets

- ✓ Secure your inward and outward facing domains with SSL/TLS certificates
- ✓ Protect communications through mobile devices and remote access points



## Continuously monitor your SSL network

- ✓ Alert admins to important events such as future certificate expirations
- ✓ Receive notifications if/when a rogue key or certificate is discovered



## Ensure Enterprise-wide security

- ✓ Create situational awareness of cryptographic security risk posture always
- ✓ Enable quick response with automated remediation in the case of a breach

**Schedule a quick call for a detailed savings assessment**

Call **+1 (727) 565-4251** or email **[enterprise@theSSLstore.com](mailto:enterprise@theSSLstore.com)**

