The number of devices and applications continues to grow at an exponential rate—on-premises, mobile, IoT, cloud, virtualization and container environments. The scale of machine adoption creates an overwhelming challenge for security teams to keep pace. They need to authenticate machine identities to ensure machine-to-machine communications are secure, but the number of machines that need to be authenticated is creating a machine identity crisis for enterprises. Of the nearly 30 billion connected devices that are expected by 2023, more than 20 billion will be connected to machine-to-machine devices.

These automated machine-to-machine connections rely on SSL/TLS certificate machine identities to authenticate, encrypt and decrypt communications. But as organizations increase their reliance on encryption and expand Encryption Everywhere strategies, the scalability of machine identity issuance, installation and management quickly becomes untenable when using traditional manual, homegrown and siloed Certificate Authority (CA) management tools.

Venafi TrustForce eliminates these SSL/TLS challenges, delivering automated, intelligence-driven actions that securely scale encryption, remove error-prone manual installation and remediate vulnerabilities and weaknesses. It also conducts rapid bulk replacement in response to security events that impact keys and certificates.

To enable intelligence-driven action, TrustForce leverages the global visibility and intelligence on SSL/TLS provided by Venafi TrustAuthority™. Through policy-enforced automated installation of keys and certificates, Venafi TrustForce™ automates the installation of digital certificates and private keys which serve as machine identities.

To ensure the security of SSL/TLS communications, Venafi TrustForce™ automates the installation process.

- Applies automated policy enforcement to the installation process
- Replaces vulnerable or weak keys and certificates automatically
- Delivers crypto-agility, replacing a large number of certificates in response to security incidents

**Prerequisite:**

- Venafi TrustAuthority™

**Benefits**

- Eliminate resource-intensive manual certificate installation
- Remove human error—once set up correctly, the implementation is the same every time
- Scale Encryption Everywhere projects safely and quickly
- Improve security with automatic replacement of vulnerable keys and certificates
- Speed incident response with automated bulk certificate replacement
- Demonstrate compliance with ongoing validation of policy-enforced installation
certificates, TrustForce enables organizations to build and maintain sustainable and scalable machine identity protection for SSL/TLS. Organizations can keep up with the growing and changing nature of machines, improving efficiencies and increasing security—all at machine speed and scale.

**Challenges**

The global visibility and machine identity intelligence gathered by Venafi TrustAuthority, including automated certificate issuance, is critical for machine identity protection. But if organizations are still using manual methods to install and configure SSL/TLS keys and certificates, inherently error-prone and resource-intensive processes will cripple them. Without automation, organizations are faced with a trade-off between machine scalability and machine identity protection.

Over 50 percent of organizations are using manual certificate management processes, while others are using ineffective homegrown solutions or siloed certificate management tools provided by CAs. None of these methods provides automated installation of keys and certificates.

**Outages.** Without the automation of the entire certificate life cycle, the risk of certificate-related outages increases. Keys and certificates need to be properly installed and configured, often on multiple systems when clustering or load balancing. Yet, in certificate life cycles, installation and configuration tend to be the most error-prone tasks. If they are misinstalled or misconfigured, certificate-related outages can bring down the systems that they are meant to support.

**Breaches.** While the automated detection of policy violations is critical, the risk of breach is mitigated only through policy enforcement. The best machine identity protection includes the automated replacement of weak or vulnerable keys and certificates, as well as the decommission of unused or old machine identities. Automation also prevents the use of poor security practices, which are frequently used in manual approaches, such as the cloning of private keys.

**No Crypto-Agility.** When there is a security event, time is critical. The longer a security threat, outage or breach continues, the greater the potential damage. Crypto-agility is the ability to quickly replace encryption certificates and keys in response to security events, especially when bulk replacement is required. Without automated installation and validation, crypto-agility is impeded, delaying incident response and increasing the risk of damage.

**Negative Compliance Findings.** In most organizations, administrators perform key and certificate installation and configuration for the systems that they control. With this approach, auditors often find inconsistent security practices, are unable to validate installation and configuration, and discover administrators with direct access to private keys, which increases the possibility of compromise.

**Lack of Scalability.** Installation of certificates and keys can be one of the most resource-intensive tasks in machine identity protection. When conducted manually, the scalability of machine identity protection is dramatically limited. As organizations increase their reliance on SSL/TLS, including Encryption Everywhere projects, they need to be able to quickly scale and secure the use of keys and certificates, which can only be achieved through automation.

**The Solution: Venafi TrustForce**

Venafi TrustForce for SSL/TLS automates every step in the key and certificate life cycle, eliminating human error and automatically renewing expiring certificates to prevent outages. TrustForce also safeguards organizations against exploits and data loss by automatically discovering machine identity weaknesses and applying defined security policies to remediate them. With the automation that TrustForce delivers, organizations can sustain crypto-agility, validate compliance, and scale machines and encryption safely to meet business demand.

**Automate Installation and Configuration.**

TrustForce provides automated certificate installation with integration across hundreds of applications, devices, services, and CAs. This includes out-of-the-box integration with load balancers, web applications and network traffic inspection devices. TrustForce can also integrate automated certificate installation with any system that allows APIs using custom scripts.
still correctly installed, ensuring that out-of-band misconfigurations are detected after installation.

**Speed Remediation.** TrustForce goes beyond identifying policy violations and enables organizations to apply automated policy enforcement. In addition, organizations can identify keys and certificates that have been impacted by security events, such as CA compromises, vulnerable algorithms or cryptographic library bugs. With the impacted keys and certificates identified, they can then be automatically replaced, drastically improving crypto-agility and closing the window of exposure.

**Scale Encryption.** With the use of encryption expanding, TrustForce enables safe scalability of SSL/TLS use to meet elastic demands for services. Whether automating the installation, configuration and validation of new SSL/TLS services, or decommissioning unused or old machine identities, TrustForce delivers safe, adaptable usage of SSL/TLS services to meet the business need.

**How It Works**

**Prerequisite: Venafi TrustAuthority for TLS**

### Machine Identity Intelligence

| Intelligence Used to Drive TrustForce Actions | • Gain global visibility using network, agent-based and onboard discovery, CA import, dashboard, certificate operation validation and reporting  
|                                               | • Enforce policies based on security and operational parameters, granular access controls, expiration monitoring, SIEM/alerts and custom metadata  
|                                               | • Streamline certificate installation with CA integration, a self-service portal, workflow controls, revocation monitoring, standards-based protocol support and RESTful APIs to automate requesting certificates, searching, importing, reporting, exporting, etc. |

### Product Features: Venafi TrustForce for TLS

| Automated Certificate Installation | • Automate the full certificate life cycle from generating keys and certificate signing requests (CSRs) to securely installing those keys and certificates on all required systems  
|                                  | • Schedule certificate installation to occur at specific dates/times in the future  
|                                  | • Execute commands or scripts during automated installation (for configuration, restarting apps, etc.) |

---

“I would highly recommend Venafi for its automation capabilities in general. Once it has been set up, it is pretty slick.”

Large Enterprise Health Care Company  
<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
</table>
| Remote Key Generation | - Automatically and remotely create the private key and CSR on the application  
- Automatically bring the CSR into the Venafi Platform, submit it to the CA and install the certificate |
| Automated Renewal | - Employ a configurable trigger (by folder) to begin automated certificate renewal  
- Be able to set the trigger based on the number of days before certificate expiration |
| Flexible Infrastructure & Application Support | - Use agentless or agent-based installation and management of certificates and keys  
- Support SSH jump servers to traverse network zones for agentless certificate provisioning  
- Leverage support for numerous operating systems, applications, appliances and cloud services |
| Workflow / Dual Control | - Enable reviews on certificate and private key installation requests via configurable workflows to ensure the security of all cryptographic assets  
- Assign one or more individuals or groups as approvers to one or more stages in the installation cycle as needed |
| Ongoing Validation of Certificate Installation | - Validate that certificates and keys are properly installed in keystores  
- Configure validation error alert notifications  
- Monitor for terminated cloud instances to ensure certificates are cleaned up |
| Application Integration | - **Web Servers**: Microsoft IIS 6.0 - 10.0, Apache HTTP server, Apache Tomcat  
- **Application Delivery Controllers**: AWS IAM/ELB, F5 Big-IP LTM, Citrix NetScaler, A10 Networks, Avi Networks  
- **Application Servers**: IBM WebSphere, JBoss, Oracle WebLogic  
- **Keystores**: IBM GSK, Java KeyStore, Microsoft CAPI, PEM, PKCS12  
- **Appliances**: IBM DataPower, Imperva, Juniper, Riverbed, Radware, Compuware, IBM Tealeaf and more  
- **Automated Life Cycle Remediation**: Demisto, Morpheus Data  
- **SSL/TLS Visibility**: Symantec SSL Visibility Appliance, Palo Alto Networks, Arbor Networks  
- **Cloud**: AWS ACB/ALB/IAM/ELB/CloudFront, Microsoft Azure Key Vault  
- **Other**: IBM Sterling Connect:Direct, Dell iDRAC, HP iLO and more |
| Adaptable Certificate Installation Framework | - Easily create custom modules for the installation and management of certificates and private keys on systems that require unique handling or configuration |
| API Integration | - Leverage REST APIs to programmatically configure large numbers of systems and certificates for automated installation and monitor status |
The Venafi Platform

The Venafi Platform delivers the machine identity and risk intelligence necessary to automatically safeguard machine-to-machine communications. It secures keys and certificates that serve as machine identities—such as SSL/TLS, SSH, IoT and mobile—and continuously collects the comprehensive intelligence needed to accurately assess security and availability risks and apply remediation.

On the Venafi Platform, TrustAuthority and TrustForce are complementary products. TrustAuthority delivers visibility, policy enforcement, and simplified and integrated enrollment. TrustForce automates the installation and configuration of keys and certificates, reducing labor and resource costs and greatly improving security and incident response.

The Venafi Platform is a mature solution:

- Scalability up to 1 million certificates with load-balanced architecture
- Over 30 patents related to machine identity protection
- Common Criteria Certified
- Network zone partitioning
- Multifactor authentication and single sign-on

As the foundation of Venafi products, the platform delivers permissions, logs, notifications, integrations and many other capabilities that align Venafi products with existing security and operations systems.

Next Steps

If you would benefit from automated, end-to-end provisioning of SSL/TLS keys and certificates—even if you have a complex, load-balanced encryption environment—contact Venafi to learn more about how TrustForce can automate your machine identity protection. With TrustForce, you can automate your entire key and certificate life cycle, speed remediation, validate compliance and safely scale your SSL/TLS encryption.

Would you recommend Venafi automation?

“Yes, definitely! We have an automated process with self-service so that users can generate their own keys and we use automated renewals, so keys don’t expire.”

Global 500 Industrial Manufacturing Company
Source: TechValidate. TV: D04-D99-4DC

Trusted by:

5 OF THE 5 Top U.S. Health Insurers
5 OF THE 5 Top U.S. Airlines
3 OF THE 5 Top U.S. Retailers
4 OF THE 5 Top U.S. Banks
4 OF THE 5 Top U.K. Banks
4 OF THE 5 Top S. African Banks
4 OF THE 5 Top AU Banks

About Venafi

Venafi is the cybersecurity market leader in machine identity protection, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.

To learn more, visit www.venafi.com

2. Source: TechValidate. TVID: 180-783-238