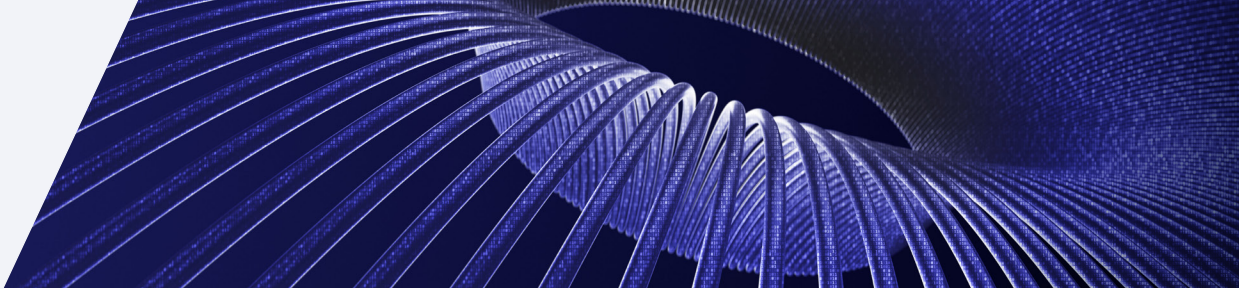
Venafi



DATA SHEET

Venafi TLS Protect

Protect TLS Machine Identities and Prevent Certificate-Based Outages

Venafi TLS Protect at a Glance

Delivers the visibility, intelligence and automation to manage the TLS certificates and digital keys that protect machine-to-machine connections and communications.

- Rapidly identifies all TLS keys and certificates
- Continually validates that certificates are installed and operating properly
- Automates the entire key and certificate management lifecycle
- Integrates with an unparalleled ecosystem of technologies

TLS Protect allows multiple teams to effectively keep up with the rapid growth of TLS machine identities, while at the same time improve security by minimizing risks introduced by humans.

Benefits

- Prevent certificate-related outages and security breaches
- Eliminate resource-intensive manual certificate orchestration tasks
- Enable certificate owners to easily comply with security policies
- Reduce risk through continuous monitoring of machine identities
- Speed incident response with automated bulk certificate replacement

Machines are driving significant advances in business growth and agility. But before machines can communicate privately and securely, they need machine identities to identify, authenticate and secure machine-to-machine communications. Just as people rely on usernames and passwords to identify and authenticate themselves, machines rely on cryptographic keys and digital certificates to serve as their identities. This includes TLS certificates used for authentication, encryption and decryption.

However, the aggressive enterprise adoption of machines and the expansion of encryption have outpaced the manual, ad hoc tools most organizations rely on to manage their TLS certificates. Due to manual processes or homegrown tools, machine identities go largely untracked, unmanaged and unmonitored. The inability to inventory and enforce policy for certificates can leave organizations vulnerable to certificate-based application outages and security breaches.

Venafi TLS Protect delivers visibility, intelligence and automation to manage TLS certificates and digital keys. Venafi is the only solution that provides complete and continuous visibility and monitoring of machine identities across highly segmented and complex networks, including public and private clouds, combined with automated, intelligence-driven actions that securely scale encryption, remove error-prone manual installation and remediate vulnerabilities and weaknesses.

Challenges

From system outages to network breaches, lack of proper management of TLS results in significant security risks to businesses.

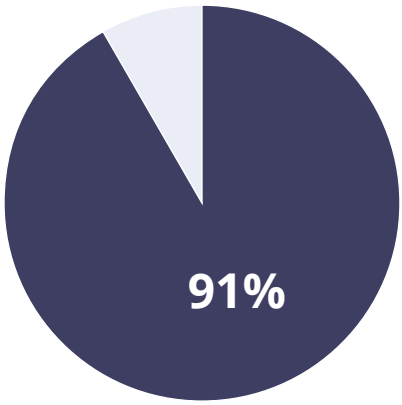
Outages. Without the automation of the entire certificate lifecycle, the risk of certificate-related outages increases. Keys and certificates need to be properly installed and configured, often on multiple systems when clustering or load balancing. Yet, in certificate lifecycles, installation and configuration 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. When the certificates that serve as machine identities are compromised or forged, cybercriminals can use them to appear legitimate, perform Man-in-the-Middle (MiTM) attacks and eavesdrop on communications. And the vast majority of network attacks cloak themselves in HTTPS to evade detection and bypass critical security controls.

No Crypto-Agility. Most organizations lack crypto-agility, the ability to quickly replace certificates in response to security events, such certificate authority (CA) compromises, vulnerabilities or other errors. Without automated installation and validation, crypto-agility is impeded, delaying incident response and increasing the risk of damage.

Compliance Failures. In most organizations, administrators perform key and certificate installation and configuration for the systems that they control.

Outages on Business-Critical Infrastructure



Before Venafi, 91% had at least 1 outage a year that impacted business-critical infrastructure.

Source: TechValidate survey of 34 IT security professionals of Venafi.

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. With the dramatic increase in machines, manual methods of issuing machine identities are slowing down IT services and the rollout of business applications. Plus, each certificate takes an average of four hours per year to maintain. Multiply this by thousands or hundreds of thousands, and overhead can add up quickly. If organizations face outages, breaches or other security incidents, management needs quickly soar.

The Solution: Venafi TLS Protect

By combining visibility, intelligence and automation, TLS Protect delivers comprehensive management and protection of TLS machine identities. The result is improved management and security that stops unplanned outages and breaches, enables fast crypto-agility, validates compliance, supports audits and allows organizations to scale.

Global Visibility. TLS Protect automates enterprisewide discovery of machine identities, providing a complete and accurate inventory. This discovery includes the configuration, location and use of certificates across the extended global enterprise—including those on premises, in virtual or cloud environments and even IoT.

Policy Enforcement. TLS Protect collects detailed machine identity intelligence that enables organizations to apply management and security policies to avoid outages and identify security blind spots. The intelligence is gathered through continuous monitoring and includes use, location, ownership, pending expirations, key lengths, signing algorithms, protocols, ciphers and other attributes.

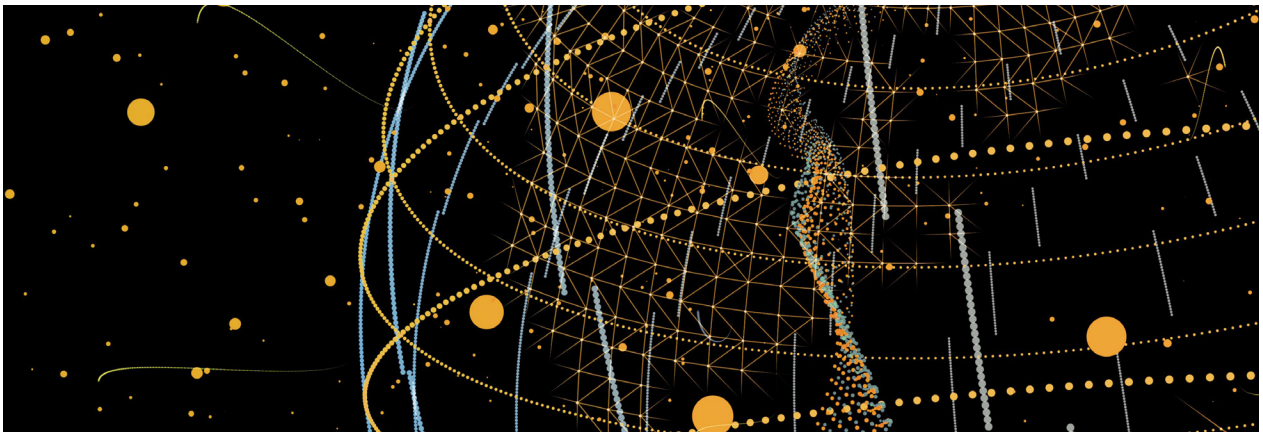
Streamlined Enrollment. TLS Protect supports any CA, including out-of-the-box integrations with leading CAs. It also offers an extensive technology partner ecosystem, with integrations ranging from the world's leading providers of security solutions to the hottest DevOps technologies. Leaders everywhere have joined Venafi to create more than 1,000 technology integrations that automatically coordinate access to machine identities.

> **"Venafi allows DevOps teams to request and manage their own keys and certificates. Plus, an additional layer of security approval makes it easier to bring certificate issuance into governance."**
>
> **Engineer,**
> **Large Enterprise Retail Company**

Automated Installation, Configuration and Validation. TLS Protect provides automated certificate installation with integrations across hundreds of applications, devices, services and CAs. This includes out-of-the-box integrations with load balancers, web applications and network traffic inspection devices. TLS Protect can also integrate automated certificate installation with any system that allows APIs using custom scripts.

Every day, Venafi uses each network device's API to confirm that certificates are still correctly installed, ensuring that out-of-band misconfigurations are detected after installation.

Fast Remediation. TLS Protect 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, vulnerabilities or other errors. With the impacted keys and certificates identified, they can then be automatically replaced, drastically improving crypto-agility and closing the window of exposure.



How It Works

Global Visibility	
Network Discovery	• Discover SSL/TLS certificates via network scanning • Configure one or more discovery jobs • Schedule recurring discoveries • Automatically organize discovered certificates and devices based on configurable rules • Use Scanafi to run complete external scans on Windows, Mac and Linux network devices with a lightweight, standalone executable
Agent-Based Discovery	• Install on local system to discover client and root certificates (certificates not discoverable via network scanning) • Automatically organize agent-discovered certificates and devices • Use minimal agent processing and memory requirements on hosts • Get broad platform support across Red Hat, SUSE, AIX, Solaris, HP-UX, Windows
Onboard Discovery	• Automate the process of importing certificates from network devices and cloud providers • Support Amazon Web Services (AWS), Microsoft Azure, IIS, F5, NetScaler and DataPower out-of-the-box • Can be configured to support other third-party devices
CA Import	• Import certificates from one or more Microsoft CAs automatically • Schedule imports to happen at specified intervals
Action-Based Dashboard	• Identify certificate risks and anomalies via customizable dashboards • Maintain a comprehensive, accurate view of the entire certificate inventory • Leverage trend graphs to detect risks and track remediation progress
Certificate Operation Validation	• Validate that certificates and keys are operating properly on the addresses and ports where they are installed • Configure validation error alert notifications
Comprehensive Reporting	• Deliver reports to certificate owners, executives and others to ensure up-to-date visibility, including pending expirations, key lengths, signing algorithms, protocols, ciphers and more • Apply customizable report filters, column selection, sorting, format (CVS or PDF) and more

Policy Enforcement	
Establishing Policies	• Enforce policies for security and operational parameters, including key length, authorized CAs, key generation location, contacts, approvers, validity period, etc. • Assign policies at any level of folder within a customizable hierarchy for governing subordinate assets, including certificates, applications, devices, etc.

Granular Access Controls	• Apply a least privileged access model for comprehensive asset protection • Set granular permissions for roles and access • Assign group/user permissions at any level of folder hierarchy or on individual assets

Expiration Monitoring	• Monitor certificate expiration dates.
	• Automatically send alerts based on configurable attributes:
	  • Periods before expiration (e.g., 90, 60, 30, 15 days before expiration)
	  • One or more recipients (groups/users)
	  • Customizable messages (HTML or text)
	  • Escalations if action is not taken in timely manner

SIEM/Alerts	• Deliver alerts and notifications via email, syslog, SNMP, Splunk, file, ServiceNow and more
Custom Metadata	• Use custom metadata fields for association of organization-specific data with assets • Set default custom field values on folders for subordinate assets

Streamlined Enrollment	
Certificate Authorities	• Leverage out-of-the-box integrations with popular CAs and centralize certificate enrollment when working with multiple CAs • Address unique organizational needs through an adaptable CA integration framework
Self-Service Portal for Certificate Owners	• Enable independent asset management (request, renew, revoke, manage and report on certificates) based on assigned permissions • Provide rich filtering and sorting for finding assets quickly • Offer customizable dashboard for rapid risk identification • Get a consistent experience across all CAs
Workflow/ Dual Control	• Enforce configurable workflow gates to require reviews and approvals • Assign one or more individuals or groups as approvers to one or more stages in the installation cycle as needed
Revocation Monitoring	• Monitor CRLs to ensure they are updated prior to expiration • Monitor certificate revocation status to identify improperly revoked certificates

Standard Protocol Support	• Get standards-based protocol support for certificate requests
	  • ACME – Automated enrollment for certificates inside and outside the firewall
	  • SCEP – Support multiple SCEP endpoints to enforce different policies and templates

Programmatic Automation	• Leverage RESTful APIs for programmatic automation of all major platform functions, including requesting certificates, searching, importing, reporting, exporting, etc. • Enforce access control permissions for API-based requests • Streamline certificate enrollment in DevOps platforms, including Kubernetes, Docker, Terraform and SaltStack

Automated Certificate Installation and Validation	
Hands-Free Installation of Certificates and Private Keys	• Automate the full certificate lifecycle 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.)
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
Automated Keystore Validation	• 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

The Venafi Trust Protection Platform

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

TLS Protect is part of the Venafi Trust Protection Platform and prevents certificate-based outages and ensures strong management for TLS certificates.

The Venafi Platform is a mature solution:

- Scales up to 1 million certificates with load-balanced architecture
- Is supported by over 30 machine-identity-related patents
- Is Common Criteria Certified
- Integrates with the broadest ecosystem of third-party applications and CAs

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

Next Steps

Are you leaving your machine identities unprotected? Venafi TLS Protect can increase your visibility, stop outages and eliminate security risks with continuous machine identity monitoring and risk intelligence. Contact Venafi to learn how Venafi TLS Protect can manage your machine identities while supporting your broader infrastructure.

To learn more, visit **venafi.com**

References

1. TechValidate. TVID: 6F7-11D-43D
2. TechValidate. TVID: B9B-AB5-655

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
3 OF THE 5 Top Accounting/Consulting Firms
4 OF THE 5 Top Payment Card Issuers
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

Venafi is the cybersecurity market leader in machine identity management, 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 venafi.com**