Venafi

DATA SHEET

Venafi TLS Protect

Protect TLS Machine Identities and Prevent Certificate-Based Outages

Key Features

Discover all certificates

Continuously discover and validate all TLS certificates across your extended network

Issue certificates

Issue TLS certificates through integration with multiple Certificate Authorities (CAs) or using the built-in CA in TLS Protect Cloud.

Empower owners

Give application owners and developers safe, self-service ability to request and manage TLS certificates when and where they're needed

Verify security compliance

Ensure all certificates have proper ownership, attributes and configuration from the CAs you have chosen and vetted.

Eliminate errors

Eliminate outages caused by human errors by automatically generating public and private keys, installing them, and performing renewals before certificates expire. 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.

The unprecedented expansion in the number of machines requiring TLS identities, the increasing speed at which these identities are being created and changed, and the growing variety of machine types that need identities to communicate securely make it increasingly difficult to manage and protect machine-tomachine communication.

Venafi TLS Protect

Venafi TLS Protect, part of the Venafi Control Plane for machine identities, allows security teams, application owners and developers to effectively keep up with the rapid growth of TLS machine identities to prevent outages, while at the same time improve security by minimizing risks introduced by humans and manual processes. TLS Protect identifies all TLS keys and certificates, continually validates that they are installed and operating properly and automates the entire TLS machine identity lifecycle.



Venafi Dashboard Inventor	гу∨ Арр	lications Machines !	Settings ~ s 55284 ⑦	Managed certificates 60560 ⑦ Old ce	rtificates 34738 @	 Retired certificates 4042 		
 Expired certificates His His Certificates assigned to 22 	-		m risk: 8 - 30 day:	s expiration 🥚 Low risk: 31 - 60 days ex 4195 Certificates not assigned				
Expired 55152 High Risk 23 Mec	dium Risk 41	. 📕 Low Risk 62 📕 Hea	Ithy 1090	Expired 132 High Risk 94	Medium Risk 269	Low Risk 310 Healthy 3390		
5 Certificates expired, or about Expired	t to expire	0 - 7 days	8 - 30 days	31 - 6	0 dava			
					o daya			④ III
		Certificates Name	Installations	Certificate Authority	Validity	Validation	Applications	. ∃II Archived on
			Installations	Certificate Authority DigiCert TLS RSA SHA2		Validation Failed	Applications ADCS Private CA	
		Certificates Name			Validity			
		Certificates Name	25	DigiCert TLS RSA SHA2	Validity 4 months	Failed		
		Certificates Name	25 18	DigiCert TLS RSA SHA2 VenafiLab-CA	Validity 4 months Expired	Failed Failed		
		Certificates Name	25 18 5	DigiCert TLS RSA SHA2 VenofiLob-CA HydrontID SSL CA G3	Validity 4 months Expired 8 months	Failed Failed Success		
		Certificates Name *sevenafi.com apachelabvenafilab. secret.engvenafi.com coolsolutions.venafi.com	25 18 5 2	DigiCert TLS RSA SHA2 VenofiLab-CA HydrantID SSL CA G3 HydrantID SSL CA G3	Validity 4 months Expired 8 months 5 months	Failed Failed Success Success		
		Certificates Name	25 18 5 2 1	DigiCert TLS RSA SHA2_ VenofiLab-CA HydrantID SSL CA G3 R3	Validity 4 months Expired 8 months 5 months Expired	Failed Failed Success Success Success		

Why use Venafi TLS Protect?

Stop Outages: TLS Protect discovers all TLS machine identities, provides knowledge on which are about to expire and can fully automate the TLS machine identity lifecycle process to eliminate outages to applications, services and security infrastructure.

Automate for Efficiency: TLS Protect offers endto-end automation across the TLS machine identity lifecycle (acquire, renew, approve, install, validate) integrated into a broad and deep ecosystem of technology partners and innovative developers to ensure organizations have the speed and efficiency they require for digital transformation.

Modernize with Speed and Agility: TLS Protect offers deep integrations with modern DevOps tooling and cloud platforms so that organizations can deliver faster, more secure cloud and DevOps and so that development teams can be #fastsecure.

Prevent Misuse and Compromise: TLS Protect provides intelligence on the security risks from

discovered TLS machine identities (e.g., key length, key strength, cipher strength) and alerts on deviations from security policy to prevent malicious or unintended use.

Ready to get started?

TLS Protect is available as-a-service or to run in your data center. Go to vaas.venafi.com/signup to start a free 30-day trial.

The Venafi Control Plane

The Venafi Control Plane for machine identities accelerates digital transformation and eliminates security incidents and revenue stream disruptions caused by machine identity management failures. With comprehensive support for all machine identities in data centers, clouds, hybrid environments and at the edge, Control Plane gives enterprises the observability, consistency, reliability and freedom of choice needed to stop outages, automate for efficiency, prevent misuse and compromise and modernize with speed and agility.

Venafi is the cybersecurity market leader in identity management for machines. From the ground to the cloud, Venafi solutions automate the lifecycle of identities for all types of machines—from physical devices to software applications, APIs and containers. With more than 30 patents, Venafi delivers innovative solutions for the most demanding, security-conscious organizations in the world. **To learn more, visit venafi.com**