

CyberArk Certificate Manager, SaaS

Secure TLS machine identities and prevent certificate-based outages

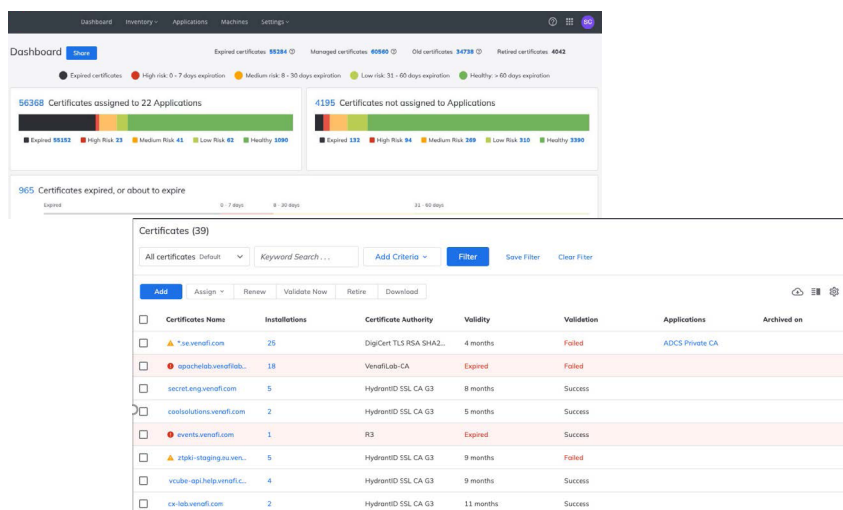
DATA SHEET

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-to-machine communication.

Certificate Manager, SaaS

CyberArk Certificate Manager, SaaS (formerly Venafi TLS Protect Cloud), 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. Certificate Manager, SaaS identifies all TLS keys and certificates, continually validates that they are installed and operating properly and automates the entire TLS machine identity lifecycle.



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 Certificate Manager, SaaS

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.

Why use Certificate Manager, SaaS?

Deliver Cyber Risk Reduction: Automate and simplify the certificate management process to help avoid business disruption and costly outages. CyberArk uses policy-driven automation to minimize human error, enable compliance with regulations and address the Google 90-day and Apple 45-day certificate lifetime requirement.

Increase Efficiency and Automation: Automate the entire certificate lifecycle management process from request to installation, including alerting on failures and validating successful updates. Streamline operations with self-service capabilities and leverage our expansive integrated ecosystem.

Enable Business Resilience: Replace legacy PKI with a modern PKIaaS solution designed to scale and meet the demands of modern cloud environments and mobile devices, while reducing enterprise PKI costs and simplifying complexity. Leverage CyberArk's expertise, global scale, services and partner capabilities to help futureproof enterprise PKI.

Satisfy Audit & Compliance: Mitigate the risk of human error that leads to certificates and keys being misused or compromised. Visualize potential risks and attacks, and centrally secure automation processes with CyberArk Privileged Access Manager integrations to protect against emerging threats from insecure machine identities.

Ready to get started?

[Visit our site to learn more about Certificate Manager, SaaS](#)

