

# Securing Certificates and PKI

SOLUTION BRIEF

## HIGHLIGHTS

### Stop outages and disruptions:

Automate and simplify the certificate management process to help avoid business disruptions and costly outages.

**Modernize PKI:** Scale and meet the demands of cloud environments and mobile devices, while reducing enterprise PKI costs with modern PKIaaS.

**Automate to maximize efficiency and resiliency:** Automate the entire certificate lifecycle management (CLM) process from request to installation.

**Prevent misuse and compromise:** Mitigate the risk of human error and help prevent certificates and keys from being misused or compromised.



## Challenge

Protecting transport layer security (TLS) certificates and public key infrastructure (PKI) is critical for any digital business, especially as cloud operations scale. No organization wants to face the consequences of outages and security failures, but as environments grow more complex, these key security challenges become increasingly difficult:

**Outages, downtime and business disruptions.** To ensure business continuity, security and operations teams must prevent application and infrastructure outages caused by certificate expirations. These outages can lead to significant business losses including revenue, customers, reputational damage and increased operational and compliance costs. Additionally, the frequency of such incidents is rising, disrupting regular business operations.

**Manual certificate management.** Manual processes lead to human errors and higher costs. Automated certificate management is essential to handle the increasing complexity of multi-cloud environments, the surge in machine identities and the accelerated pace of certificate renewals, without introducing human error, risk or burdensome costs.

**Legacy PKI costs and risks.** Security teams are burdened with outdated PKI like Active Directory Certificate Services (ADCS) and Enterprise JavaBeans Certificate Authority (EJBCA) due to their limitations in addressing the security requirements of modern applications and cloud environments. They need a modern, flexible architecture to support the high performance and availability needs of global organizations.



**Machine identities are the very basis of security. Venafi is the expert. They invented the space of machine identity management.**

–Scott Barronton, CISO, DN



**Without the automation capabilities Venafi brought to us, we couldn't manage our identities at all.**

–Alan Morton, Technical Lead for Certificate Services, BP



**Security, compliance and audit failures.** When certificates lapse, organizations risk compliance violations, costly downtime, security breaches and potential fines. Security teams are responsible for managing certificate renewals and revocations, including monitoring expirations, initiating renewals and handling cryptographic keys. Robust certificate management processes are essential to prevent these serious consequences, regardless of varying compliance requirements.

## Solution

CyberArk's solution is designed to secure and automate your CLM and modernize your PKI with a solution that scales to meet business requirements across any environment and helps maximize uptime, reduce security incidents and prevent costly disruptions. The solution is designed to improve security across cloud environments and provide:

**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 and 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.

For additional information and resources, contact [sales@cyberark.com](mailto:sales@cyberark.com) and learn how to secure certificates and modernize your PKI.

