Partner Brief

# Fully Automating Key and Certificate Lifecycle with Privileged Account Access

## CyberArk Application Identity Manager and Venafi Trust Protection Platform

Automating the lifecycle of keys and certificates to support a machine identity protection strategy has always required tradeoffs. Gaining privileged account access to enable this automation is time consuming. To reduce the chances of cyber attackers gaining unauthorized privilege account access, organizations are gating access to credentials. This avoids the risks inherent in storing privileged account credentials on hard drivers or servers, but it also makes keys and certificates less available for automation.

Many enterprise policies now require a system to authorize privileged account access for the type of credentials needed to perform key and certificate lifecycle operations. Compliance programs have also included similar stringent gating controls. Organizations need a way to open the door to full visibility and automation for keys and certificates by unlocking access to privileged account credentials for applications servers, ADC/load balancers, and other virtual and physical machines.

### Solution: Enable Access to Privileged Accounts to Automate Key and Certificate Lifecycle Operations

Venafi® and CyberArk® have partnered to deliver a seamless integration that expands an organization's ability to fully automate secure key and certificate lifecycle for all systems. The integration gives the Venafi Trust Protection Platform access to privileged system and application accounts held by CyberArk. This allows organizations to perform sensitive renewal, replacement and rekey operations without administrator involvement or storing credentials outside of the enterprise vault.

The combined Venafi and CyberArk solution helps organizations strengthen their machine identity protection by reducing time-consuming administrative tasks that can also increase the risk of exposing private keys to more people. The integration taps the large number of functional integrations, included in the Venafi Technology Network, to automate key and certificate operations. By harnessing the full power of Venafi platform automation, organizations can accelerate the speed of security operations, increase agility to respond to incidents like a CA compromise and reduce overall key and certificate lifetimes.

### How It Works

To gain access to automate the key and certificate lifecycle, Venafi Trust Protection Platform obtains authorization from CyberArk® Application Identity Manager.

1. Administrators authorize the Venafi Trust Protection Platform to gain access to privileged credentials protected by CyberArk Application Identity Manager
2. The Venafi platform requests authorization from CyberArk to access a protected system to perform key and certificate lifecycle operations, such as rotate, request, issue and install new keys and certificates
3. CyberArk issues the Venafi platform an authorization token to access the specific system
4. The Venafi platform performs fully automated key and certificate lifecycle operations without any human involvement

### CyberArk Application Identity Manager

The CyberArk Application Identity Manager includes the CyberArk Enterprise Password Vault, which is designed to secure, rotate and control access to privileged account passwords based on organizational policies. The solution is proven to scale in the largest, most complex enterprise IT environments, and it can protect privileged account passwords used to access the vast majority of systems. CyberArk Enterprise Password Vault proactively protects, isolates, controls and continuously monitors privileged accounts on virtual and physical servers, databases, network devices, hypervisors, security appliances, SaaS and business applications and more.

### Venafi Trust Protection Platform

Venafi Trust Protection Platform protects machine identities by delivering an enterprise-grade platform designed for security, operational efficiency and organizational compliance. The platform provides visibility of all machine identities across the extended enterprise. With full situational awareness of cryptographic security risk posture at all times, organizations are able to automate the identification of weak certificates, such as SHA-1, MD5 or wildcards while enabling quick response with automated remediation.

### Conclusion

Together, Venafi and CyberArk provide an integrated solution that helps organizations improve their protection for machine identities. Using this solution, organizations can achieve fully automated, high-speed key and certificate lifecycle operations without human involvement. And they can realize the efficiencies of automation without sacrificing the security, policy and compliance requirements for privileged accounts.

### ABOUT VENAFI

Venafi is the cybersecurity market leader in protecting cryptographic keys and digital certificates which every business and government depends on to deliver safe encryption, authentication and authorization. Organizations use Venafi key and certificate security to secure machine-to-machine connections and communications—protecting commerce, critical systems and data, and mobile and user access.