SOLUTION BRIEF

END-TO-END SSH KEY GOVERNANCE AND RISK MITIGATION

AN INTEGRATED SOLUTION: CYBERARK ENTERPRISE PASSWORD VAULT AND VENAFI TRUST PROTECTION PLATFORM

HIGHLIGHTS

- Discover enterprise wide, agent based or agentless SSH keys
- Create central key inventory, map connectivity and analyze for risks
- Remediate risks by prioritizing and rotating out-of-compliance SSH keys
- Automate SSH machine identity lifecycle through self-service on boarding
- Notify InfoSec and risk teams of policy violations

CyberArk and Venafi have teamed up to offer an integrated solution for enterprise-wide governance and risk reduction by enabling easy and robust management of SSH keys. The integration with Venafi's SSH Protect solution is designed to provide higher levels of automation for system administrators, better visibility for InfoSec teams, and results in fast, successful audits for GRC teams.

THE CHALLENGE

Digital transformation results in tremendous growth in the number of machines and pushes IT system administrators to new levels of productivity via automation. Many administrators achieve this productivity by creating and deploying SSH keys, which establish fast, secure, automated connections to critical assets. These SSH keys serve as machine identities, identifying and authenticating administrators and machines for critical business functions.

But history shows how easy it is for organizations to lose track of SSH keys, which can lead to the misuse of privileged access on sensitive internal systems. Poor SSH configuration and management practices have left many organizations vulnerable to cybercriminals, insider threats and failed audits as well as leave IT and security teams without a clear understanding as to what went wrong.

WHY INTEGRATE VENAFI WITH CYBERARK

In this integrated solution, CyberArk provides Privileged Access Management (PAM) for interactive human-user accounts including key management, session isolation and audit, while Venafi provides Machine Identity Protection for automated machine-to-machine connections. Together, encryption key governance is achieved across the entire enterprise, protecting the full lifecycle of keys from creation to termination, including the storage and auditing of those keys.

The tight integration between CyberArk and Venafi ensures that each system is aware of all critical actions, like key Activation, Distribution, Rotation, Expiration, and Termination, as well as any privileged activities or access. This integration allows real-time operations and risk-reduction like CyberArk monitoring SSH sessions and calling Venafi to rotate a keyset only when the session is inactive, while maintaining continuous audit trails across both systems.

In addition, the integration provides CyberArk customers with a level of keyset and host discovery not available to stand-alone users, with integration into enterprise-wide security policies for appropriate key lifecycles. It enables a "true" inventory of all keys within a given environment and allows for trust maps of keysets and governance to be applied.

ABOUT CYBERARK SOLUTION

The CyberArk Privileged Access Security Solution includes an encrypted Digital Vault, which is designed to secure, rotate and control access to privileged account passwords based on organizational policies for both human and non-human users. The solution is proven to scale in the largest, most complex enterprise IT environments, and can protect privileged account passwords used to access the vast majority of systems found in cloud and hybrid environments alike. The CyberArk solution proactively protects, isolates, controls and continuously monitors privileged access on virtual and physical servers, databases, network devices, hypervisors, security appliances, SaaS and business applications and more.

CyberArk Application Access Manager is part of the CyberArk Privileged Access Security Solution and is designed to secure the privileged credentials and provide secret management for widely used application types, scripts and other non-human identities. The solution secures credentials for containerized applications built using DevOps methodologies, as well as for commercial off-the-shelf applications, traditional internally developed applications, and automation scripts. The solution enables organizations to remove hard-coded credentials from code and instead centrally rotate, manage, monitor and secure these credentials which are used by applications and other non-human identities to access databases and other sensitive resources.

ABOUT VENAFI SSH PROTECT

SSH Protect, a part of the Venafi Trust Protection Platform, provides visibility, intelligence and automation for automated SSH keys used in machine-to-machine connections. It safeguards the trusted, automated machine-to-machine connections SSH keys enable. InfoSec teams use SSH Protect to follow best practices defined in standards, such as NIST, with an enterprise-grade SSH management solution that discovers, remediates, governs and audits SSH machine identities, even in environments that scale to millions of SSH keys in daily, active use.

CYBERARK PRODUCTS

- CyberArk Core Privileged Access Security
- CyberArk Application Access Manager (Central Policy Manager)

PARTNER PRODUCTS

- Venafi Trust Protection Platform
- Venafi SSH Protect

JOINT SOLUTION BENEFITS

- Consistent, end-to-end solution safeguards privileged human identities as well as privileged machine identities
- Tight integration enables safe, orchestrated automation for SSH key actions, from activating and rotating of keys to revoking and terminating them, without disabling unseen workflows
- Achieve a Zero Trust network that supports "least privilege" concepts for both human and machine identities, using consistent policies and approaches across both identity types

HOW THE JOINT SOLUTION WORKS: A ZERO TRUST APPROACH TO ACCESS CONTROL

"Zero Trust" is the concept that assumes that rather than a "default approve" response to a previously existing connection, all connections that access an enterprise's resources should be "default deny" and require verification every time a connection is needed. Access is not something to be given once and then forgotten about, but instead should be constantly examined to grant the minimum access and permissions necessary for individuals – or connected and privileged machines – to do their job.

With the integration of Venafi and CyberArk, our joint customers can take a major step towards achieving a Zero Trust Architecture.

Key integration scenarios include:

Consolidated Visibility:

Venafi's SSH Protect discovers and registers SSH Admin Machine identities, along with critical context around identity creation and configuration, and supplies that insight to CyberArk

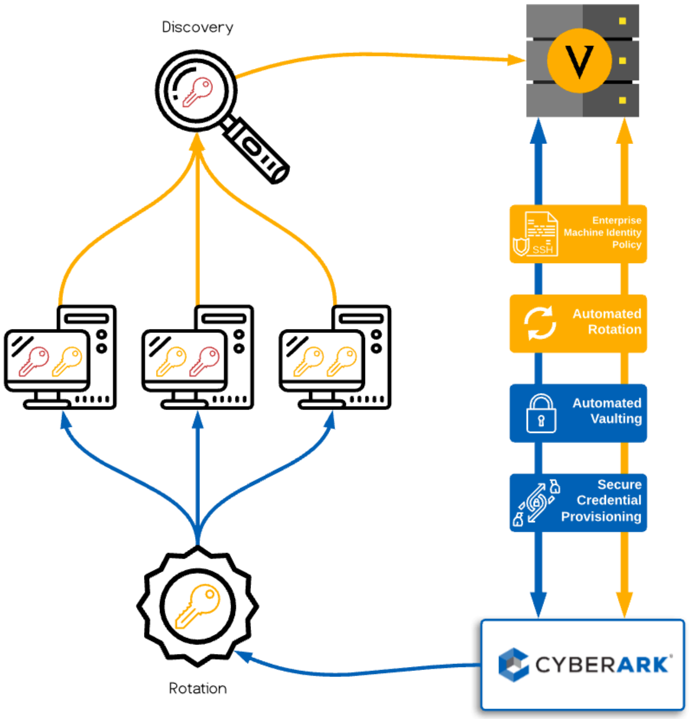
When an employee or contractor is realigned, CyberArk SCIM and vault call a workflow that allows Venafi to delete all Admin Keys associated with the user in question

Enable Event-Based Access:

On certain event triggers, CyberArk's session management capabilities orchestrate Venafi SSH Protect to provision or revoke SSH keys on command

Integrated Risk Reduction:

CyberArk's Application Access Manager (Central Policy Manager) instructs Venafi's SSH Protect to eliminate non-compliant keys, misconfigured keys, or unauthorized keys



Reduced Time-to-Value:

CyberArk Application Access Manager orchestrates Venafi SSH Protect to rapidly provision or revoke all non-human credentials, whether stored in the Venafi Trust Protection Platform or within CyberArk's Enterprise Password Vault

KEY BENEFITS/TAKEAWAYS

Together, Venafi and CyberArk provide an integrated solution that helps organizations protect the end-to-end lifecycles of their critical machine identities. Using this solution, organizations achieve fully automated, high-speed key and certificate lifecycle operations that require limited human interaction or involvement. Together, these solutions realize the efficiencies of automation without sacrificing the security, policy and compliance requirements for privileged accounts, whether human or non-human.

About CyberArk

CyberArk is the global leader in privileged access management, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 500, To learn more, visit www.cyberark.com.

About Venafi

Venafi is the cybersecurity market leader in machine identity protection, 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.

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.