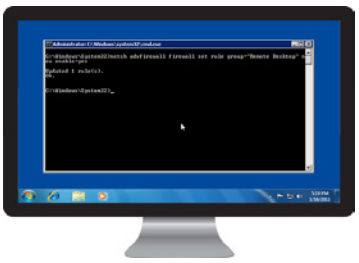
SSH Key Manager

Обнаруживайте, защищайте, управляйте и контролируйте доступ к SSH-ключам в соответствии с корпоративными политиками



SSH Key Manager enables organizations to prevent unauthorized access to privileged accounts in Unix/ Linux environments and reduce the risk of a data breach.

Why CyberArk?

CyberArk is the trusted expert in helping organizations stop the most critical cyber-attacks before they stop the business.

ОПИСАНИЕ ПРОБЛЕМЫ

SSH-ключи обычно используются в качестве средства аутентификации внутри корпоративной ИТ-инфраструктуры, обеспечивая защиту пользователей к привилегированным учётным записям и проверяя разрешения автоматизированных приложений. Если этот процесс не контролируется, то SSH-ключи могут представлять серьезную угрозу безопасности для бизнеса.

Проблема SSH-ключей заключается в том, что у них нет процедуры обязательного контроля и срок действия пары ключей никогда не истекает. Предоставля привилегированный доступ к пользователям и приложениям, эти ключи легко генерируются, распространяются и, как правило быстро забываются. В результате, многие организации при формировании стратегии безопасности с привилегированными учетными записями недооценивают или просто игнорируют эти мощные учётные данные. Не уделяя должного внимания управлению и безопасности SSH-ключей, а также не рассматривая их в качестве привилегированных учётных данных, организации рано или поздно сталкиваются со следующими серьезными проблемами:

- Недооценка рисков.

  Без централизованного подхода к управлению SSH-ключами, трудно определить местонахождение этих данных, а также предвидеть те риски и уязвимости, которые могут быть использованы злоумышленниками.

- Повышенный риск утечки данныхиз-за скомпроментированных ключей

  Без централизованного хранения и контроля доступа SSH-ключи могут быть потеряны, украдены или переданы неавторизованным пользователям. В результате, злоумышленники или любознательные пользователи могут получить неавторизованный доступ к частным SSH-ключам, а затем использовать их для доступа к критическим системам и конфиденциальным данным.

* Непрохождение аудита из-за наличия незащищённых и неуправляемых привилегированных аккаунтов,

Многие ИТ-организации обязаны защищать, контролировать и отслеживать доступ к привилегированным учётным записям. Для обеспечения соответствия внутренним и отраслевым требованиям организации должны обеспечивать, управлять и контролировать использование SSH-ключей , обеспечивающих доступ к привилегированным учетным записям.

- Высокая стоимость операционных расходов при неавтоматизированной замене SSH-ключей

  Смена SSH-ключей в организациях зачастую осуществляется вручную, что требует значительного времени и усилий. Неавтоматизированные процессы всегда приводят к высоким эксплуатационным расходам.

РЕШЕНИЕ

SSH Key Manager позволяет открывать, защищать, менять и контролировать доступ к SSH-ключам в соответствии с политиками организации. Данное решение предлагает надёжные средства контроля доступа, которые гарантируют, что только авторизованные пользователи имеют доступ к закрытым ключам, а также предоставляет возможность формирования отчётности для проверки использования ключей. Благодаря SSH Key Manager можно:

- Обнаруживать откытые и закрытые SSH-ключи

  SSH-ключи могут существовать на машинах всей организации, и один закрытый SSH-ключ может иметь несколько доверительных отношений. SSH Key Manager позволяет централизованно обнаруживать SSH-ключи и доверительные отношения, а также, опционально, загружать встроенные парные пары ключей для управления в Digital Vault.

- Безопасно хранить закрытые SSH-ключи

  Защищённые SSH-ключи можно безопасно хранить в цифровом хранилище CyberArk, которое разработано с использованием многочисленных встроенных средств безопасности, включая иерархическое шифрование, гранулярные средства контроля доступа и автоматическое повышение отказоустойчивости сервера.

- Контролировать доступ к закрытым SSH-ключам

  Гранулярные элементы управления доступом позволяют определять, какие SSH-ключи разрешено просматривать или получать доступ к ним каждому пользователю или группе пользователей, а также ене давать пользователям видеть все другие неавторизованные ключи. Автоматизированные рабочие процессы позволяют пользователям по мере необходимости запрашивать единовременный доступ к SSH-ключам с повышенными привилегиями. Централизованное управление политиками в сочетании с надёжной аутентификацией гарантирует, что только авторизованные пользователи смогут получить доступ к этим привилегированным учетным данным.

- Automate key rotation. By automating SSH key rotation, organizations can reduce the risk of unauthorized privileged access to target systems without burdening the IT team. CyberArk SSH Key Manager enables organizations to automatically rotate and update SSH key pairs either on-demand or based on policy.
- Report on the use of private SSH keys. Built-in audit capabilities enable organizations to view and report on the use of SSH keys, including what systems were accessed, by whom and how long each session lasted. Audit logs are stored in the tamper-resistant Digital Vault. Reports can be generated and handed over to auditors to demonstrate compliance with requirements.

Benefits

CyberArk SSH Key Manager can help organizations incorporate SSH key security and management into a broader privileged account security strategy. CyberArk SSH Key Manager helps organizations:

- Mitigate risks by strengthening privileged account security. By better protecting access to privileged SSH keys, organizations can reduce the risk of unauthorized privileged access to Unix and Linux systems and reduce the risk of a data breach.
- Avoid penalties by meeting and proving compliance. Many standards and regulations require organizations to protect privileged account access. By securely storing, managing and controlling access to SSH keys, organizations can address these requirements, and built-in reporting tools help organizations expedite audit processes.
- Improve operational efficiency by automating security processes. The automated rotation of SSH key pairs, storage of private keys and distribution of public keys to target systems helps organizations strengthen security and meet compliance requirements without burdening the IT team. Integration into the CyberArk Shared Technology Platform enables organizations to manage all privileged credentials from a single platform, behind a single pane of glass.

A Comprehensive Solution

CyberArk SSH Key Manager is a component of the CyberArk Privileged Account Security Solution, a complete solution designed to discover, secure, manage, monitor and control access to privileged account credentials, including both passwords and SSH keys. Products in the solution can be managed independently or combined for a complete privileged account security solution. CyberArk SSH Key Manager is based on the CyberArk Shared Technology Platform which delivers enterprise-class security and allows customers to deploy a single infrastructure and expand the solution to meet changing business requirements.

Specifications

Supported Platforms:

- DNA Discovery: RHEL 4-6; Solaris Intel and Solaris SPARC 9, 10, 11; SUSE 10; Fedora 18; Oracle Linux 5; CentOS 6; AIX 5.3, 6.1, 7.1; ESXi 5.0 and 5.1
- SSH Key Security and Management: RHEL 4-6; Solaris SPARC and Solaris Intel v9, v10, v11; CentOS 6; AIX 5.3, 6.1, 7.1; ESX, ESXi v5.1
- Private Key Security: Windows XP; Windows 7; Windows Vista; Windows 2008R2; Windows 2012R2

Target SSH Servers:

- OpenSSH

Private Key Formats:

- OpenSSH, Putty, Tectia

Encryption Algorithms:

- AES, DSA

SSH Key Lengths:

- 1024, 2048, 4096, 8192

Access and Workflow Management:

- LDAP directories
- Identity and Access Management
- Ticketing and workflow systems

Multi-lingual Portal:

- English, French, German, Spanish, Russian, Japanese, Simplified Chinese, Traditional Chinese, Korean, Brazilian Portuguese

Authentication Methods:

- Username and Password, RSA SecurID, Web SSO, RADIUS , PKI and smartcards, LDAP, SAML

Monitoring:

- ·SIEM integration, SNMP traps, Email notifications