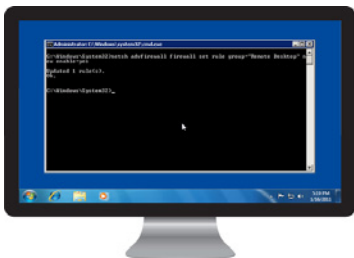




SSH 金鑰管理器 (SSH Key Manager)

依照企業的政策探索、保護、管理、
監控和控管對 SSH 金鑰的存取。



SSH 金鑰管理器可讓企業防範 Unix / Linux 環境內對未授權的特權帳號的存取，並且降低資料洩漏的風險。

為何選擇 CyberArk？

CyberArk 是值得信賴的專家，能夠協助企業防堵最緊要的網路攻擊，使營運不致受到影響。

挑戰

SSH 金鑰通常被當成企業 IT 環境內部的驗證方法，可保護使用者存取特權帳號，以及驗證應用程式對應用程式間自動通訊的信任。若管理不當，SSH 金鑰可能會對企業造成重大安全風險。

使用 SSH 金鑰的挑戰是金鑰本身沒有監控機制，只要一經建立，金鑰組就可無限期使用。這些金鑰為使用者和應用程式提供特權存取，很容易產生、散發，而且很容易被忘記。因此，許多企業在建立特權帳號安全策略時，都忽略了這些強大的憑證。將 SSH 金鑰棄置不管或未加保護，而且未能將之以特權憑證來看待，企業將面臨嚴峻的挑戰，包括：

- **缺乏對風險的預見性。**無法掌握何處存在哪些 SSH 金鑰，企業很容易落入無法察覺可遭惡意使用者利用的風險的境地。
- **因遭入侵的金鑰而提高資料外洩的風險。**若沒有集中化的儲存和存取控管機制，私密 SSH 金鑰可能會遺失、遭竊或與未經授權的使用者共享。惡意或好奇的使用者因而能夠非法存取私密 SSH 金鑰，然後利用這些金鑰來存取關鍵系統和機密資料。
- **未受保護和管理的特權帳號導致稽核不合格。**許多 IT 企業都必須保護、控管和追蹤對特權帳號的存取。為了持續符合內部和業界規定，企業必須保護、管理和監控提供特權帳號存取權的 SSH 金鑰。
- **手動輪換 SSH 金鑰導致高營運成本。**當企業必須輪換 SSH 金鑰時，通常都是需要耗費大量時間和人力的人工方式來進行。這種人工方式往往導致高營運成本。

解決方案

CyberArk SSH 金鑰管理器 (CyberArk SSH Key Manager) 讓企業可以依照組織政策來探索、保護、輪換和控管對 SSH 金鑰的存取。本解決方案提供嚴格存取控管，可確保只有已授權的使用者才能存取私密金鑰和報告功能，並藉此稽核金鑰的使用狀況。使用 CyberArk SSH 金鑰管理器，企業可以：

- **探索公開和私密 SSH 金鑰。**SSH 金鑰可存在整個企業內的機器上，並且單一私密 SSH 金鑰可擁有多重信任。CyberArk SSH 金鑰管理器可以讓企業集中探索 SSH 金鑰和信任關係，並選擇將已授權的金鑰組列入數位金庫以進行管理。
- **安全地儲存私密 SSH 金鑰。**私密 SSH 金鑰可以安全地儲存在 CyberArk 數位金庫 (CyberArk Digital Vault) 內，此數位金庫具有多重內建安全機制，包括分層加密、嚴格存取控管和自動伺服器強固。
- **控管對私密 SSH 金鑰的存取。**嚴格的存取控管方式，讓企業可定義允許每個使用者或使用者群組檢視或存取的 SSH 金鑰、保護對這些金鑰的存取，並隱藏所有其他未經授權的金鑰讓使用者無法檢視。自動化作業流程讓使用者在有業務需求時，申請一次性存取較高層級特權的 SSH 金鑰。集中化政策管理，搭配對強式驗證的支援，協助確保只有已授權的使用者才能存取特權憑證。

- **自動輪換金鑰**。藉由自動輪換 SSH 金鑰，企業就可以在不增加 IT 人員的負擔下，降低未授權的特權存取目標系統的風險。CyberArk SSH 金鑰管理器讓企業可以視需要或根據既定政策，自動輪換和更新 SSH 金鑰組。
- **報告私密 SSH 金鑰的使用**。內建的稽核功能可讓企業查看和報告 SSH 金鑰的使用狀況，包括哪些人存取了哪些系統，以及每次連線維持多久時間。稽核記錄檔會儲存在抗竄改的。

數位金庫內。此外可產生報告並且交給稽核人員，以確認符合法規需求。

優勢

CyberArk SSH 金鑰管理器可以幫助企業將 SSH 金鑰安全和管理整合至規模更大的特權帳號安全性策略。CyberArk SSH 金鑰管理器可以協助企業：

- **透過強化特權帳號安全來減緩風險**。藉由對 SSH 金鑰的存取提供更好的防護，企業可以降低對 Unix 和 Linux 系統的未授權的特權存取並且降低資料洩漏的風險。
- **符合並證實合規以防受到處罰**。許多標準和法規都規定企業必須防護特權帳號的存取。

透過安全地儲存、管理和控管對 SSH 金鑰的存取，企業就可以滿足法規規範，而內建的報告工具更可協助企業加速稽核程序。

- **透過自動化安全流程提升營運效率**。自動輪換 SSH 金鑰組、儲存私密金鑰以即將公開金鑰散發到目標系統，有助企業強化安全並且滿足法規規範，又不會增加 IT 人員的負擔。整合至 CyberArk 共享技術平台 (CyberArk Shared Technology Platform) 可讓企業從單一平台，在單一窗口後管理所有的特權憑證。

全方位的解決方案

CyberArk SSH 金鑰管理器是 CyberArk 特權帳號安全解決方案 (CyberArk Privileged Account Security Solution) 的一個元件。這是一套專為探索、防護、管理、監控和控制對特權帳號憑證 (包括密碼和 SSH 金鑰) 的存取所設計的完整解決方案。本解決方案內的產品可單獨進行管理，或是結合成一套整合性和全面性的特權帳號安全解決方案。CyberArk SSH 金鑰管理器是以 CyberArk 共享技術平台為基礎，提供企業級的安全性，並且可讓客戶部署單一基礎結構並擴充解決方案以符合業務變化的需求。

規格

支援的平台：

- DNA Discovery：RHEL 4-6；Solaris Intel 和 Solaris SPARC 9、10、11；SUSE 10；Fedora 18；Oracle Linux 5；CentOS 6；AIX 5.3、6.1、7.1；ESXi 5.0 和 5.1
- SSH 金鑰安全和管理：RHEL 4-6；Solaris SPARC 和 Solaris Intel v9、v10、v11；CentOS 6；AIX 5.3、6.1、7.1；ESX、ESXi v5.1
- 私密金鑰安全性：Windows XP；Windows 7；Windows Vista；Windows 2008R2；Windows 2012R2

目標 SSH 伺服器：

- OpenSSH

私密金鑰格式：

- OpenSSH、Putty、Tectia

加密演算法：

- AES、DSA

SSH 金鑰長度：

- 1024, 2048, 4096, 8192

存取和作業流程管理：

- LDAP 目錄
- 身分和存取管理
- 票證核發和作業流程系統

多語言入口網站：

- 英文、法文、德文、西班牙文、俄文、日文、簡體中文、繁體中文、韓文、巴西葡萄牙文

驗證方法：

- 使用者名稱和密碼、RSA SecurID、Web SSO、RADIUS、PKI 和智慧卡、LDAP、SAML

監控：

- SIEM 整合、SNMP 陷阱、電子郵件通知

保留所有權利。未經 CyberArk Software 事前書面同意，本文件之任一部分皆不可以任何形式或方式重製。CyberArk®、CyberArk 標誌和其他上列之貿易或服務名稱皆屬 CyberArk Software 在美國和其他司法管轄區的註冊商標 (或商標)。其他貿易和服務名稱之所有權屬於各自所有權人。U.S., 10.16。Doc # 125

CyberArk 確認本文件內之資訊於出版日期之時正確無誤。所提供之資訊不提供任何明示、法定或是默示之保證，如有變更，恕不另行通知。