

CyberArk Expands Privileged Account Security Solution to Include SSH Key Management

October 21, 2014 8:30 AM ET

Single, Integrated Platform Protects Customers from Cyber Attackers and Malicious Insiders

NEWTON, Mass.--(BUSINESS WIRE)--Oct. 21, 2014-- [CyberArk](#) (NASDAQ: CYBR), the company that protects organizations from cyber attacks that have made their way inside the network perimeter, today introduced comprehensive [Secure Shell \(SSH\) key management](#) with the release of version nine of [CyberArk Privileged Account Security Solution](#). Customers can now secure and manage SSH keys as well as other privileged credentials in a single, integrated platform to identify, manage and protect against advanced external attackers and malicious insiders.

Widely used by IT teams to get direct, root access to critical systems, SSH keys are often created without any oversight or management, essentially providing ongoing, uncontrolled privileged access to the target system. Research by Ponemon Institute showed that three out of four enterprises have no security controls in place for SSH keys and that 51 percent of enterprises have already experienced an SSH key-related compromise.¹ Further, because SSH keys are commonly used in automated application-to-application authentication, keys can be created, distributed and never thought of again, leaving systems riddled with unknown and undocumented vulnerabilities ready to be exploited.

“Cyber attackers know that hundreds of thousands of SSH keys exist in large enterprises and they exploit this situation to gain privileged access to critical systems. In an attempt to simplify trust and connectivity, organizations unwittingly leave giant holes in their defences,” said Roy Adar, vice president of product management, CyberArk. “Our focus is on preventing exploited privileged accounts through any attack vector, and therefore the protection of SSH keys is a natural expansion for our Privileged Account Security solution – one that will immediately improve our customers’ security.”

Key benefits include:

- Securely manage privileged accounts accessed through passwords or SSH keys from a single platform to protect, detect, monitor and respond to potential threats.
- Discover how many SSH keys exist, where they are located, how they’re being used and the potential risks they pose.
- Prevent SSH keys from being stolen by securely storing them in a hardened, central storage location.
- Eliminate ‘timeless’ keys that create a permanent backdoor into critical systems by automatically rotating all SSH keys at regular intervals.
- Extend controls to secure SSH keys used in Amazon Web Services UNIX images.
- Support audit and compliance teams with full SSH key session recording.

“Attackers are looking for ways to blend in with normal IT operations as long as they can and by hijacking an SSH key, they gain direct, seemingly legitimate access to critical systems that are very difficult to detect,” said Adar. “Customers are asking for solutions that prevent legitimate IT operations from being exploited by criminals, without compromising the company’s ability to stay competitive.”

In addition to SSH key management, CyberArk Privileged Account Security Solution v9 enables customers to:

- Reduce the cost of managing UNIX user provisioning through agentless Active Directory bridging capabilities, while increasing security with complete session monitoring.
- Eliminate hardcoded passwords from applications and scripts using an agentless web services-based approach.

[CyberArk SSH Key Manager](#) and CyberArk Privileged Account Security Solution v9 will be generally available worldwide in November, 2014. CyberArk SSH Key Manager is licensed on a per target server basis. Additional resources can be found here:

- [SSH Key Security Infographic](#)
- [Discover the Keys to SSH Security Whitepaper](#)
- [SSH Key Security Solution Overview](#)
- [SSH Key Manager Data Sheet](#)

About CyberArk

CyberArk (NASDAQ: CYBR) is the only security company focused on eliminating the most advanced cyber threats; those that use insider privileges to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk proactively secures against cyber threats before attacks can escalate and do irreparable damage. The company is trusted by the world's leading companies – including more than 35 percent of the Fortune 100 and 17 of the world's top 20 banks – to protect their highest value information assets, infrastructure and applications. A global company, CyberArk is headquartered in Petach Tikvah, Israel, with U.S. headquarters located in Newton, MA. The company also has offices throughout EMEA and Asia-Pacific. To learn more about CyberArk, visit www.cyberark.com, read the company blog, <http://www.cyberark.com/blog> follow on Twitter @CyberArk or Facebook at <https://www.facebook.com/CyberArk>.

Copyright © 2014 CyberArk Software. All Rights Reserved. All other brand names, product names, or trademarks belong to their respective holders.

¹ “The Ponemon 2014 SSH Security Vulnerability Report,” Feb. 2014

Source: CyberArk

Media Relations Contacts:

fama PR

Brian Merrill, +1-617-986-5005

cyberark@famapr.com

or

CyberArk

Eric Seymour, +1-617-796-3240

eric.seymour@cyberark.com

or

Investor Relations Contact:

ICR

Staci Mortenson, +1-617-558-2132

IR@cyberark.com