Safeguard Critical Systems from Malicious Users and Compromised Devices

Isolate privileged sessions to protect critical systems from potentially malicious users and devices.

The Challenge

Privileged internal and third-party users require administrative access to critical systems to maintain infrastructure, apply updates and administer applications. The trouble is, by enabling this privileged access, organizations inevitably expose their critical systems to untrusted third-party users, potentially malicious insiders and vulnerable user devices.

Third-party users, such as vendors or consultants, do not have direct relationships with the organization, and they typically access critical systems from untrusted endpoints. Similarly, though trusted by the organization, internal users can cause intentional or accidental damage to critical systems, and they often access privileged accounts from managed devices vulnerable to malware and compromise. In this environment, organizations must find a way to enable the necessary privileged access while simultaneously safeguarding critical systems from potentially malicious users and devices. Without the proper controls in place, organizations will face a variety of challenges:

- **Spread of Malware to Critical Systems.** Users and their endpoints are vulnerable to socially engineered phishing attacks, and research suggests that if attackers send 20 to 30 phishing emails, they will likely succeed at least once.[1] If a privileged user fell victim to such an attack and then accessed critical systems from an infected endpoint, the malware could easily spread to those systems, giving the attacker direct access to critical systems and sensitive data.
- **Compromised Privileged Credentials.** To access privileged accounts, users typically enter the account credentials from their endpoints, and a cache of those credentials – including password hashes – remain on the local system. As a result, if a privileged user's endpoint were compromised, an attacker could harvest the credentials, use them to laterally move through the network and escalate privileges, which are necessary steps in any successful attack.
- **Ineffective Security Controls.** Organizations often put security measures in place to track privileged user access to critical systems. But, if users are able to gain knowledge of the privileged account credentials, those controls can be easily circumvented to directly access privileged accounts. In such a state, security and audit teams lose the ability to track and monitor activity, leaving them vulnerable to inside attacks.
- **Failed Audits.** Best practices dictate that privileged account access should be controlled and monitored, and several regulatory bodies have adopted these standards as requirements. Without the proper controls in place – and the ability to prove that those controls are effective – organizations can potentially face failed audits and regulatory fines.

The Solution

To protect critical systems from potentially malicious users and devices, organizations should consider leveraging a secure jump server. By forcing all privileged sessions through a secure jump server, organizations can isolate privileged sessions to separate users and devices from critical systems, as well as establish an isolated network segment without the use of a VPN. With the secure jump server in the middle, organizations are able to prevent the spread of malware from infected user devices to critical systems. Further, when coupled with a credential vault, the jump server can manage the privileged account authentication to ensure that neither users nor their devices are ever exposed to the underlying credentials, thus minimizing the risk of credential theft.

Figure 1 shows how a secure jump server, coupled with a credential vault, can isolate privileged, remote sessions. First, a user accesses a secure jump server and selects the privileged account needed. Next, the jump server calls the credential vault to

1 CyberArk Threat Report: Privileged Account Exploits Shift the Front Lines of Security. November 2014.

Why CyberArk?

CyberArk is the trusted expert in stopping cyber attacks before they stop business.

retrieve the appropriate password or SSH key. The credential is then sent to the target system, and upon authentication, a new remote session is established on the hardened jump server. With this architecture, malware is unable to jump from user devices to critical systems, and neither users nor their devices are exposed to the underlying privileged account credentials.

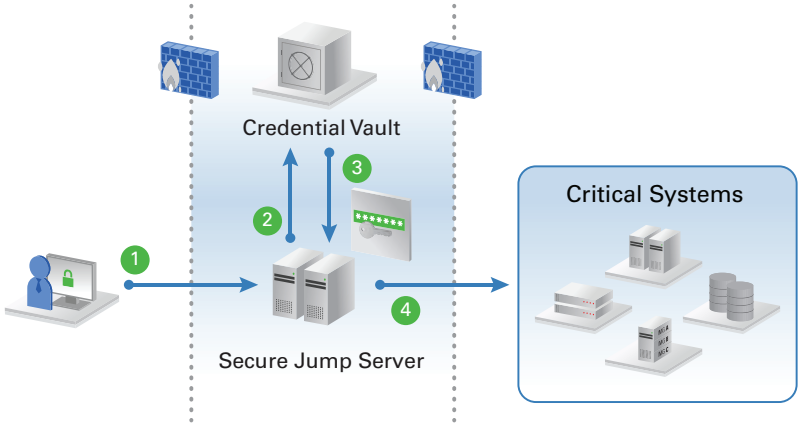

Figure 1: Secure jump server architecture, integrated with a credential vault

Benefits

- **Prevent the spread of malware to critical systems.** By isolating privileged sessions on a secure, hardened jump server, organizations can prevent malware from a user's device from reaching protected critical systems. As the malware attempts to spread, a hardened jump server can prevent the file from executing, thus protecting connected systems from infection.
- **Mitigate the risk of stolen credentials and hashes.** When integrated with a credential vault, a secure jump server can be used to facilitate privileged account access and initiate remote sessions, all without ever exposing users or their endpoints to the underlying passwords or SSH keys. Because there is no trace of the credential – in plaintext or hash form – on the user's machine, it cannot be stolen from a compromised endpoint. Further, an integrated credential vault can automatically rotate privileged passwords and SSH keys after each use, thus limiting the useful life of credentials in the event of a compromise.
- **Prevent users from circumventing controls.** By pairing a secure jump server with a credential vault, organizations can prevent privileged users from knowing or learning privileged account credentials. By masking these credentials, users can only gain privileged access via the jump server, thus ensuring that privileged account security controls are always enforced.
- **Demonstrate compliance with audit requirements.** To meet internal and regulatory audit requirements, organizations must not only prove that the proper controls are in place, but also that the controls are effective. By preventing users from knowing any privileged account credentials, they are unable to bypass the secure jump server. As a result, security and audit teams can leverage the jump server for complementary controls, such as session recording and user activity monitoring, while assuring that those controls are effective and compliant.

CyberArk's Solution

CyberArk Privileged Session Manager acts as a secure jump server, isolating privileged sessions to protect critical systems from untrusted users and devices. With CyberArk Privileged Session Manager, organizations can protect critical systems from malware on endpoints, mitigate the risk of privileged credential theft and misuse, and comply with audit requirements. As an added benefit, the secure jump server can be leveraged as a single point of control from which organizations can monitor and record privileged session activity, as well as remotely terminate suspicious sessions.

An enterprise-scalable solution, CyberArk Privileged Session Manager isolates and controls access to systems in even the most diverse, complex and distributed network environments, ensuring the greatest amount of protection of critical systems. CyberArk Privileged Session Manager seamlessly integrates into the CyberArk Privileged Account Security Solution, enabling organizations to secure, protect, and detect suspicious usage of all privileged account credentials from one common infrastructure managed behind a single pane of glass.