Seven Steps to Complete Privileged AccessManagement

Step 1: Improve accountability and control over privileged passwords

Step 1 - Improve accountability and control over privileged passwords

- Not effectively managing shared accounts is a problem that has significant scale and risks.
- Certain systems have embedded or hardcoded passwords, opening opportunities for misuse.
- Passwords are generally static so there must be protections against passwords leaving the organization.

Step 2: Implement least privilege, application control for Windows & Mac desktops

Step 2: Implement least privilege, application control for Windows & Mac desktops

- The next step to complete privileged access management is implementing least privilege on end-user machines.
- The process for IT to restrict or enable end user privileges is complex and time-consuming, but it must be done to support audit or compliance mandates.
- And although users should not be granted local administrator or power user privileges in the first place, sometimes certain applications require elevated privileges to run.

Step 3: Leverage application-level risk to make better privilege decisions

Step 3: Leverage application-level risk to make better privilege decisions

- Now that shared credentials are under management and end users have the privileges they need to perform their jobs – and nothing more – you can move to a better understanding of vulnerabilities to help make better-informed privilege elevation decisions.

- The challenge, though, is that most vulnerability management solutions do little to help security leaders put vulnerability and risk information in the context of business.

Step 4: Implement least privilege in Unix and Linux environments

Step 4: Implement least privilege in Unix and Linux environments

- Having root passwords, super-user status, or other elevated privileges is important for users to do their jobs.

- Organizations must be able to efficiently delegate Unix and Linux privileges and authorization without disclosing passwords for root or other accounts. Recording all privileged sessions for audits, including keystroke information, helps to achieve privileged access control requirements without relying on native tools or sudo.

Step 5: Unify management, policy, reporting and threat analytics into under a single pane of glass

Step 5: Unify management, policy, reporting and threat analytics into under a single pane of glass

- How do security and IT operations teams gain an understanding of where threats are coming from, prioritize them, and quickly mitigate the risks?

- Advanced threat analytics enables IT and security professionals to identify the data breach threats typically missed by other security analytics solutions. Solutions pinpoint specific, high-risk users and assets by correlating low-level privilege, vulnerability and threat data from a variety of third-party solutions.

Step 6: Integrate Unix, Linux and Mac into Windows

Step 6: Integrate Unix, Linux and Mac into Windows

- How do IT organizations achieve consistent policy configuration to achieve compliance requirements, a simpler experience for users and administrators, and less risk from an improperly managed system?

- The ideal solution is to centralize authentication for Unix, Linux and Mac environments by extending Microsoft Active Directory's Kerberos authentication and single sign-on capabilities to these platforms. By extending Group Policy to these non-Windows platforms you gain centralized configuration management, reducing the risk and complexity of managing a heterogeneous environment.

-

Step 7: Real-time change auditing and recovery for Windows environments

Step 7: Real-time change auditing and recovery for Windows environments

- How do IT organizations better understand changes, have the capability to roll them back if necessary, and establish the right entitlements in the first place across a complex Windows infrastructure so they can more effectively protect the business?

- Organizations need centralized real-time change auditing for Active Directory, File Servers, Exchange, SQL, and NetApp, the ability to restore Active Directory objects or attributes, and to establish and enforce entitlements across the Windows infrastructure.

Questions?

Thank you