ManageEngine
PAM360

7 ways to reinforce privileged access security in your enterprise

In any enterprise, privileged users have unfettered administrative access to an extensive range of mission-critical systems and data across the IT infrastructure. Although many cyberattacks today are linked to the misuse of such unrestrained elevated access—either by malicious privileged insiders or by external threat actors—most organizations' security programs often incorporate only fragile, superficial controls over privileged operations.

This is where privileged access management (PAM) comes into play. PAM refers to a set of policies that secure, control, and monitor privileged activities and sessions on critical enterprise systems without compromising business productivity.

Here are some sure shot techniques that will help you design, build, and develop a powerful defence mechanism against privilege abuse.

1 Create visibility into all the privileged access in your network:

Discover and identify all privileged accounts, keys, certificates, and sensitive documents strewn across the IT infrastructure, and consolidate them in a central location. Set permissions and policies around who can access them and for how long. This way, you can establish visibility and control of all privileged access to critical data—especially long-forgotten and abandoned privileged accounts—that present high-risk backdoors for malicious actors.

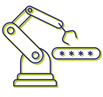
2 Build multiple layers of security for privileged access:

Implement multi-factor authentication to confirm the identities of those performing privileged activities. To further fortify security, restrict access to critical systems by requiring approvals from superiors, and automatically check in and reset the access credentials after a set period. With such strong access controls in place, it's much harder for attackers to gain entry via obscure pathways, escalate their privileges and move laterally within the network, and impede business operations.

3 Adopt easier and quicker workflows to improve business productivity:

Enable privileged users to remotely access crucial systems via secure pathways without modifying firewall policies, connecting to a VPN, or remembering numerous complex passwords. Automate remote login capabilities for them to access systems and applications across hybrid environments using single sign-on. Such practices will prevent rogue access from unknown sources while simultaneously speeding up operations and boosting productivity with faster time to value.

4 Condense the attack surface by eliminating credential hard-coding:



Uncover default, hard-coded credentials in your DevOps automation files, and consolidate them in a central location. Enforce APIs and automation scripts to fetch the required credentials from the central password vault to prevent the exposure of high-risk passwords. Implement password security best practices, like password rotation and complexity, to drastically reduce credential-theft attacks and openings for exploits.

5 Improve oversight and accountability of privileged sessions:

Record every privileged user session and store them as video files in a secure, encrypted database for future review. Shadow privileged sessions, and monitor them in real-time to promptly detect and terminate suspicious activities, and efficiently investigate risky sessions. Having foolproof and fine-grained recordings of privileged sessions launched by trusted privileged insiders and third-party vendors alike facilitates easier governance and better accountability of privileged sessions.

6 Readily demonstrate compliance with regulations and security policies:

Capture all events involving privileged credentials and access in clear, downloadable audit trails and reports. Many compliance standards and industry regulations, like SOX, HIPAA, and PCI DSS, specify the need to track and monitor all access to your critical systems. With a central point of management for audit and compliance, you can conveniently prove to auditors and forensic investigators that the required security controls are in place.

7 Integrate with advanced technologies to make better business decisions:

Adopt AI and ML-driven monitoring capabilities to continuously detect unusual and potentially harmful privileged activities, and automatically set off mitigating controls to prevent damage. Integrate with SIEM and scanning tools to discover vulnerabilities and promptly issue remediation measures.

Add ITSM into the mix to streamline privileged access requests, and improve the efficiency of change and asset management. Correlate and synchronize privileged access data with all the capabilities above, and orchestrate their workflows from a central console. This way, you can gain increased situational awareness by implementing privileged access security across the entire infrastructure, mitigating organizational silos.

ManageEngine PAM360 is a comprehensive privileged access management solution that enables enterprises to implement strict control and governance over administrative access and permissions for users, systems, and applications across their IT infrastructure.

ManageEngine PAM360 was positioned in the Gartner 2020 Magic Quadrant for Privileged Access Management for the second consecutive time for advancing with the evolving PAM needs of modern businesses.

Register for a personalized demo now!