Elevating Cybersecurity with Privileged Access Management (PAM)

info@kriptone.com | www.kriptone.com

In a landscape plagued by data breaches and relentless cyberattacks, Privileged Access Management (PAM) has emerged as the linchpin of an organization's cybersecurity strategy. PAM is not just a technology; it represents a holistic approach, encompassing a suite of practices metic lously designed to oversee, control, and monitor account and data access rights within an organization.

01 The Core Purpose of PAM:

At its core, PAM is driven by a singular mission - to ensure that both individuals and systems possess precisely the level of access needed to critical resources, nothing more and nothing less. PAM casts its protective net over the often-underestimated concept of privileged access, be it human access (employees, vendors, or contractors) or non-human entities (applications, systems, or connected devices).

info@kriptone.com | www.kriptone.com

02 The Significance of PAM:

The evolving sophistication of modern cyber threats demands a solution that transcends traditional perimeter-based security models. PAM delivers a granular level of control, safeguarding sensitive information and critical systems by meticulously restricting access based on necessity and relevance. Furthermore, PAM acts as an unwavering bulwark against external threats and profoundly curtails insider risks. By assiduously managing privileged access, PAM helps curtail the risk of data leaks, misuse of privileges, and unauthorized access, fostering a resilient security environment within the organization.

03 PAM in the Digital Age:

As we delve deeper into the digital age, where cloud-based solutions, remote work arrangements, and digital transformations proliferate, the role of PAM in fortifying an organization's security posture becomes indisputably paramount. It is high time for organizations to embrace PAM as an indispensable element of their cybersecurity strategy.

kntrol™

Best Practices in Privileged Access Management (PAM):

info@kriptone.com | www.kriptone.com

kntrol™

01 Employ Temporary Privilege Escalation:

Reduce vulnerabilities stemming from excessive user access rights. Grant admin privileges solely when essential. This strategy effectively curtails unnecessary exposure, managing insider threats and lowering the risk of both internal and external attacks.

02 Keep Track of Assets and Privileges:

The visibility of your digital assets and their corresponding privileges is central to effective management. Maintaining a precise inventory of digital assets helps discern redundant, obsolete, or potentially risky privileges. This proactive approach ensures that your organization remains ahead in asset management, averting unforeseen security challenges.

info@kriptone.com | www.kriptone.com

kntrol™

03 Deploy Attribute-Based Access Control (ABAC):

Attribute-Based Access Control (ABAC) adds an extra layer of security to your organization. It leverages a blend of user, device, and environmental attributes to dictate access decisions. This comprehensive approach bolsters your security posture, offering more control and flexibility in determining who can access what, when, and under what conditions.

04 Monitor Assignment of Privileges Versus Usage:

Assigned privileges may not always align with actual usage. Regularly reviewing assigned privileges versus actual usage unveils unused privileges that could potentially pose security risks. Active monitoring ensures that organizations maintain a lean, efficient, and secure access management strategy.

info@kriptone.com | www.kriptone.com

kntrol™

05 Deploy Zero Trust, Everywhere:

Embrace the Zero Trust model, which operates under the assumption of a breach. It scrutinizes every access request as if it originates from an open network. This rigorous approach enhances security by mandating comprehensive authentication, authorization, and encryption for every request, regardless of its origin.

06 Record and Audit:

Robust record-keeping and regular audits are pivotal to maintaining a healthy PAM strategy. An audit trail of all privileged activities aids in identifying irregular patterns, supporting forensic investigations. Regular audits ensure that your organization remains compliant with regulatory requirements, making this practice vital for effective PAM.

info@kriptone.com | www.kriptone.com

kntrol™

07

Monitor and Alert:

Implement real-time monitoring and alerting systems to significantly boost your organization's ability to detect unusual or potentially harmful activities. Swift detection can either preempt potential breaches or minimize their impact, preserving your organization's cybersecurity integrity.

info@kriptone.com | www.kriptone.com

kntrol™

Kntrol Privileged Access Manager (KPAM):

Kntrol Privileged Access Manager is a formidable safeguard for your organization's privileged accounts. It features an encrypted password vault, comprehensive session recording, 2FA authentication, and more. Beyond security, it enhances operational efficiency by automating tasks and enforcing policies. KPAM not only safeguards assets but also fosters compliance, operational excellence, and business growth.

info@kriptone.com | www.kriptone.com

Discover how Kntrol can bolster your cybersecurity efforts and operational efficiency. Reach out to us today!

info@kriptone.com | www.kriptone.com