PATECCO
dynamic identity systems.

Top Privileged Access Risks and How to Eliminate Them with PAM?

	RISK	SOLUTION
Credential theft	Stolen privileged credentials allow attackers to impersonate admins and bypass security barriers. Credential theft remains one of the most common entry points in cyberattacks.	✓ Enforce strong authentication ✓ Restrict access rights: Grant employees only the data and tools essential for their role. ✓ Adopt strong password policies: Critical accounts should be protected with unique, 16+ character passwords.
Insider threats	Employees, contractors, or administrators with elevated rights may misuse their privileges - either maliciously or by accident. This can lead to data leaks or system outages.	✓ Apply the least privilege principle. ✓ Monitor privileged sessions in real time. ✓ Apply approval workflows for sensitive actions.
Generic and unmanaged accounts	Shared “admin” accounts or forgotten system accounts create blind spots where accountability is lost. Attackers can exploit these unmanaged accounts unnoticed.	✓ Discover all privileged accounts. ✓ Eliminate generic logins. ✓ Assign unique credentials tied to individual users.
Connection with a compromised device	If a privileged user connects from an infected endpoint, attackers can hijack sessions and infiltrate malware into critical systems.	✓ Enforce secure access gateways. ✓ Verify device health before granting access. ✓ Isolate risky connections.
Transfer of infected files	Privileged users often share sensitive files across systems. If a file is compromised, malware can spread rapidly with elevated permissions.	✓ Restrict file transfer options. ✓ Scan files for threats before uploading. ✓ Log all privileged data movements.
Operational inefficiency	Without automation, managing privileged accounts manually slows down IT teams, increases errors, and disrupts workflows.	✓ Automate provisioning. ✓ Streamline approvals. ✓ Standardize access processes to boost efficiency and reduce costs.
Compliance violations	Regulations such as GDPR, NIS2, and ISO 27001 Standard require strict privileged access controls. Weak monitoring or lack of audit trials can result in costly fines.	✓ Automate provisioning and streamline approvals. ✓ Standardize access processes to boost efficiency and reduce costs.

www.patecco.com

Tel.: +49 (0) 23 23 - 9 87 97 96

Ringstrasse 72 - 44627 Herne

E-Mail: info@patecco.com