Minimize the risk from privileged access

Users with privileged access to an organization's systems and networks pose a special threat. Since privileged accounts are so powerful, a single misuse or compromise can lead to a data breach or costly business disruption. With Netwrix, you can dramatically reduce this risk while ensuring individual accountability and hard evidence for auditors.

MINIMIZE SECURITY RISKS

Reduce attack surface by removing standing privileged accounts that can be compromized by attackers.

BALANCE CONVENIENCE AND SECURITY

Enable admins to efficiently accomplish their tasks while enforcing accountability.

PASS AUDITS WITH LESS EFFORT

Avoid audit findings and provide solid proof that privileged activity is not creating security risks.

CUSTOMER FEEDBACK

"We can truly manage the access to our systems to the level of least privilege. The concept of temporary elevation, or just-in-time access, makes so much sense: The admin is granted access on the fly and access is removed when no longer needed."

Craig Larsen, Information Systems Administrator
Eastern Carver County Schools

Gold Winner
Privileged Access Management

netwrix.com/pam
Powerful Data Security Made Easy

Key features

ELIMINATE STANDING PRIVILEGES

Minimize security risk by removing standing privileged accounts. Instead, create on-demand accounts that have just enough access to do the job at hand and are deleted automatically afterward.

ENHANCE ADMIN ACCOUNTABILITY

See exactly what privileged activity is happening across your systems, live or retrospectively, to spot policy violations, or collect evidence during investigations.

MINIMIZE ATTACK SURFACE WITH AUTOMATIC CLEANUP

Mitigate the risk of pass-the-hash, Golden Ticket and related attacks with automatic purging of Kerberos tickets after each privileged session. Avoid unsanctioned remote connections by automatically disabling RDP on the server once an administrative task is completed.

CONTROL PRIVILEGED ACCESS

Know exactly who has access to critical resources, track membership in the powerful Domain Admins group, get a list of service accounts, and more, so you can maintain a least-privilege state to keep risks low.

PROTECT YOUR SERVICE ACCOUNTS

Safeguard service accounts by rotating their passwords from one place; receive an alert if the process is disrupted so you can pause it and roll back any unwanted changes.

ANSWER AUDITORS' QUESTIONS WITH LESS EFFORT

Be prepared for tricky questions from auditors with an easy-to-pull audit trail of all admin activity, from the initial request for privileged access and who approved it, through all actions taken (including changes to files or local groups), to account deletion afterward

WHY NETWRIX

ZERO STANDING PRIVILEGE

Other privileged account management solutions attempt to slap band-aids on the inherently risky approach of using standing admin accounts. With Netwrix you can minimize your attack surface by replacing standing privileges with on-demand accounts.

LOW TOTAL COST OF OWNERSHIP

Save time and money with a solution that installs in minutes and typically runs on existing infrastructure. Everything you need is included in one reasonable license — you won't face extra fees for add-ons for databases, appliances, proxies, high availability or other common needs.

LEVERAGE THE INVESTMENT YOU'VE ALREADY MADE

Keep using the tools you know, such as Remote Desktop Connection Manager, Local Administrator Password Solution (LAPS) or your current password vault, but make them more secure by integrating them with the Netwrix PAM solution.

Download your free 30-day trial

netwrix.com/pam

Corporate Headquarters: 300 Spectrum Center Drive, Suite 200, Irvine, CA 92618

Phone: 1-949-407-5125 **Int'l:** 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023

netwrix.com/social