Slash the risk from privileged activity

A single compromise or misuse of privileged account can lead to a data breach or costly business disruption, since these powerful accounts provide malicious actors with access to critical data and systems as well as the ability to effectively cover their tracks. With Netwrix solutions, you can dramatically reduce these risks by discovering and removing standing privileges and monitoring privileged activity to catch threats before major damage is done.

MINIMIZE PRIVILEGED ACCESS RISKS

Reduce your attack surface area by discovering and removing standing privileged accounts that can be compromised by attackers.

CONTROL PRIVILEGED ACTIVITY

Reduce the damage from a security incident by detecting suspicious privileged activity and responding to it faster.

PASS AUDITS WITH LESS EFFORT

Avoid audit findings and provide solid proof that privileged activity is not creating security risks with prebuilt reports and easy search.

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
Slash the risk from privileged activity

Key features

PRIVILEGED ACCOUNT DISCOVERY

Get a firm handle on the risk that admin accounts pose to your organization by discovering all human and non-human privileged accounts across your IT environment.

ON-DEMAND PRIVILEGES

Minimize security risk by removing standing privileges. Instead, create on-demand accounts that have just enough access to do the job at hand, and delete them automatically afterward, along with any artifacts that attackers could exploit.

PRIVILEGED ACTIVITY MONITORING

Spot suspicious behavior faster and enforce individual accountability by monitoring, logging and video-recording all privileged activity. Minimize damage by promptly blocking threats and policy violations.

ZERO TRUST PRIVILEGED ACCESS

Validate identities in accordance with Zero Trust principles by enforcing contextual multifactor authentication (MFA) for each privileged session using granular policies tailored to specific actions and resources.

LOCAL ADMINISTRATOR SECURITY

Shut down a common attack vector while still enabling users to perform specific tasks that require elevated privileges on their machines by replacing all-or-nothing local Administrator rights with granular privilege elevation.

COMPLIANCE REPORTING

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

Minimize your attack surface by removing standing privileges in favor of on-demand accounts.

COMPLETE SOLUTION

Improve the security of privileged access with full coverage of critical PAM capabilities.

FASTER TIME TO VALUE

Realize value faster with easy deployment and implementation that is much faster than traditional solutions.

ECOSYSTEM INTEGRATIONS

Leverage previous investments by integrating Netwrix solutions with your existing tools, such as LAPS, your vault or your SIEM.

Next Steps

REQUEST ONE-TO-ONE DEMO
netwrix.com/pam

REQUEST PRICING
netwrix.com/buy

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