Netwrix SbPAM

Leave no chance for compromise or misuse of privileged accounts

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 SbPAM, 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/sbpam
Secure Privileged Activity With Just-in-Time Access

Key features of Netwrix SbPAM

EPHEMERAL PRIVILEGED ACCOUNTS

Shrink your attack surface by eliminating standing privilege. Instead, create on-demand accounts that have just enough access to do the job at hand and are deleted automatically afterward.

ACCESS APPROVAL AND CERTIFICATION

Ensure all privileged activity is legitimate and performed by a trusted user with workflows for approving or denying requests for privileged access and regularly certifying privileged users' rights.

SESSION MONITORING AND RECORDING

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

CLEANUP OF PRIVILEGED ACCESS ARTIFACTS

Mitigate the risk of 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.

SERVICE ACCOUNT MANAGEMENT

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.

ZERO TRUST PRIVILEGED ACCESS

Validate identities by enforcing contextual multifactor authentication (MFA) each time an admin requests a privileged session, using granular policies for specific activities and resources.

HOW IS NETWRIX SBPAM DIFFERENT?

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 SbPAM 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 RDP/SHH clients, Local Administrator Password Solution (LAPS) or your current password vault, but make your processes more secure by integrating these products with Netwrix SbPAM.

Next Steps

GET A FREE TRIAL
netwrix.com/sbpam

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

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