RevBits
PRIVILEGED ACCOUNT SCANNER

RevBits PAS is the First Step in Assessing On-Premises and Cloud Security Risks

Secure IT resources and digital assets

Most organizations have diverse and growing attack surfaces from a multitude of endpoints, like workstations, laptops, and mobile devices, to network file servers, passwords and privileged accounts, just to name a few.

Securing access into the accounts that utilize enterprise assets and resources is critical. These include privileged and non-privileged accounts. Privileged account users are administrators responsible for managing IT software and hardware. They have elevated privileges that allow them to install, update and configure systems. If these accounts aren't protected, managed and monitored, they can present significant security risks.

Privileged account discovery

Privileged account discovery allows security managers to identify potential security risks related to privileged access, by automatically mapping network, devices, accounts and systems, looking for privileged access points.

Privileged accounts can include:

- Local Administrative Accounts
- Privileged User Accounts
- Domain Administrative Accounts
- Emergency Accounts
- Service Accounts
  - Active Directory or Domain Service Accounts
  - Application Accounts

Measuring and assessing risk across your organization's IT estate provides the security necessary to defend against growing cyber threats. The ability to discover and inventory all digital assets and accounts by scanning an enterprise-wide network is needed to ensure a robust security posture with complete visibility. Discovering and inventorying all your digital assets and accounts will enable you to secure them against growing and ever-changing cyber threats from external bad actors and malicious insiders.

RevBits Privileged Account Scanner

RevBits Privileged Account Scanner (PAS) allows organizations to get their arms around the distributed accounts they have across on-premises and multi-cloud environments. RevBits PAS scans multi-cloud environments to discover and inventory digital assets and privileged accounts to identify vulnerable access points, while providing critical data needed to protect your organization.

Through scanning your enterprise-wide network with RevBits PAS, accounts and users with the most sensitive and risky permissions can be discovered, including potentially damaging shadow admins, or users that have sensitive permissions with escalation privileges within the cloud. Attackers and malicious insiders can exploit these permissions to gain access to critical cloud infrastructure.

RevBits PAS detects signs of account misconfigurations that can increase the chance for intrusion, such as default settings or expired accounts. Reviewing information discovered by RevBits PAS allows security teams to ensure these accounts are carefully managed and monitored.

www.revbits.com
844-4REVBITS (844-473-8248

RevBits Cyber Security Solutions

Securing privileged accounts at scale requires the ability to know where privileged accounts are, if they are active, and to maintain a comprehensive inventory of these accounts. RevBits PAS auto-discovers privileged and non-privileged accounts and identifies their locations, reducing time-consuming manual tasks for your IT staff.

You'll locate privileged accounts you didn't even know you had, and be able to immediately bring them under management. Most organizations have hundreds, if not thousands of privileged accounts, including domain accounts, service accounts and local administrator accounts. The more accounts you have, the larger your account attack surface and the greater your risk.

RevBits PAS eliminates potential vulnerabilities, such as:

- Service accounts, especially those that require elevated privileges.
- Non-expiring service accounts that increase the potential risk of attacks.
- Non-expiring normal AD accounts that if compromised, can increase security risk.
- Non-expiring passwords on local accounts that can provide threat actors with the means to enter the network and introduce malware.

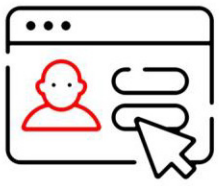
RevBits PAS Benefits

- Strengthens security controls by revealing vulnerabilities.
- Bolsters the organization's security posture by revealing the status of all privileged and non-privileged account details across your entire IT infrastructure.
- Eliminates security vulnerabilities before they become problems by scanning accounts and adding privileged access controls.
- Discovers hidden account privileged access from former employees, ex-contractors and other third-party service providers, to reduce attack surfaces and risk exposure.
- Keeps PAM up to date with a best practices approach of consistent automated discovery of privileged accounts.

Software Requirements

RevBits PAS supports cross-platform environments, including Windows, Linux and Mac. Account types supported include:

- Internal on-premises networks
- Active Directory (AD) and LDAP servers
- Service accounts
- Google Cloud Platform (GCP) assets
- Amazon Web Services (AWS) assets
- Microsoft® Azure assets



RevBits PAS is the First Step in Assessing On-Premises and Cloud Security Risks

www.revbits.com
844-4REVBITS (844-473-8248)