RevBits®

PRODUCT BRIEF

Privileged Access Management

Deploying RevBits PAM in an Operational Technology Environment.

Operational Technology (OT) environments, which encompass industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems, play a significant role in the critical infrastructure of industries such as manufacturing, energy, transportation, and more. Given the increasing digitalization and interconnectedness of OT systems, securing privileged access within these environments has become paramount. This product brief sheds light on the importance of deploying Privileged Access Management (PAM) in OT environments, the challenges, and best practices.

The benefits

PAM is crucial in OT environments for several reasons. First, it helps mitigate security risks by protecting high-value privileged accounts from attackers. If compromised, these accounts can lead to unauthorized system manipulation, data theft, disruptions in operations, and even physical damage. By implementing PAM, organizations can safeguard against malicious activities and the impact of security breaches.

By implementing PAM, organizations can safeguard against malicious activities and the impact of security breaches.

Second, PAM ensures regulatory compliance for industries reliant on OT systems. Many of these industries are subjected to strict regulations and standards. With a PAM solution, organizations can demonstrate compliance by establishing accountability, traceability, and appropriate access controls for privileged users.

Additionally, PAM helps safeguard against internal threats posed by privileged users. Whether intentional or unintentional, these users can pose security risks. PAM addresses this by enforcing granular access controls, monitoring activities, and adhering to the principle of least privilege. Doing so minimizes the potential for abuse or accidental errors by privileged users.

The challenges

While implementing PAM in OT environments, certain challenges need to be overcome. One such challenge is the presence of legacy systems that lack built-in security features. Integrating a PAM solution with these systems requires careful planning and possibly customization.

Another challenge is maintaining operational continuity. Since OT systems are designed for continuous operation, there are limited maintenance windows. Implementing PAM without causing disruptions necessitates thorough planning, testing, and coordination with operational teams.

Furthermore, OT environments often involve intricate networks, multiple vendor systems, and diverse user roles that add complex access requirements. Managing and enforcing access controls for privileged users across these environments without a PAM solution can be difficult and risk-prone.

RevBits PAM overview

As the number of vendors and products increases to support a growing OT environment, access management needs will exponentially increase. RevBits PAM provides comprehensive access management while reducing the number of vendors supporting access controls. With multiple integrated access management modules in one solution, organizations have greater control and, therefore, stronger security.

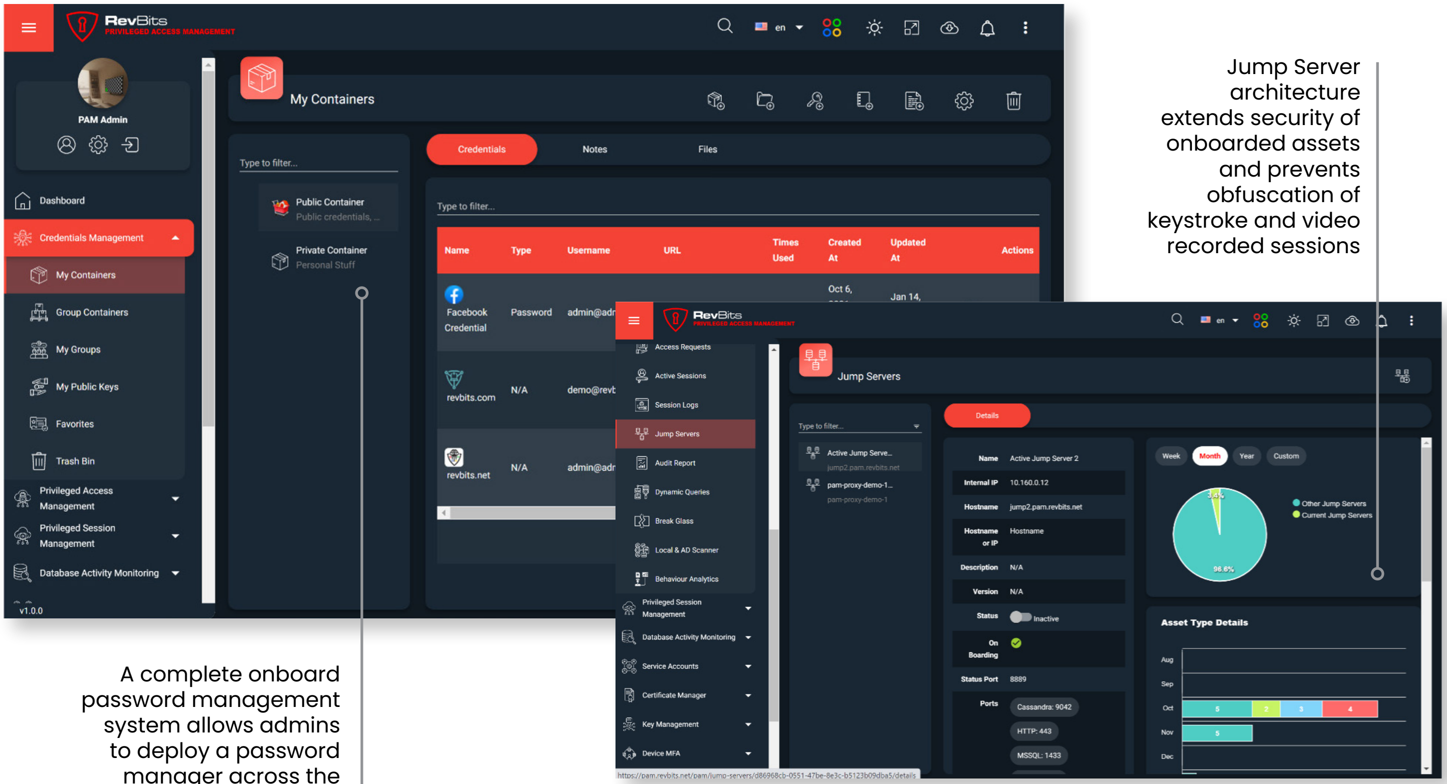
RevBits PAM tightly regulates access to critical resources, captures keystrokes, and video records all privileged sessions. Fine-grained rules include session length, days of the week, time of day, and more. Additionally, single-click server connections eliminate the complexity of managing access to critical infrastructure.

Privileged Access Management is the core capability of RevBits PAM and can be purchased singularly or in combination with seven other natively integrated access management capabilities:

- Privileged Session Management
- Service Account Management
- CI/CD Integration
- Full-featured Password Management
- Certificate Management
- Key Management

RevBits PAM solves five common challenges within OT environments

1. Expands multiple access management capabilities in one solution - without adding vendors
2. Native client capability eases onboarding with single-click connections to servers
3. Jump server architecture optimizes server security
4. Workflow is simplified with a native onboard workflow engine
5. Linux-based PAM servers remove the administrative difficulty and hidden costs of Windows-based servers



Name	Type	Username	URL	Times Used	Created At	Updated At	Actions
Facebook Credential	Password	admin@adr			Oct 6,	Jan 14,	
revbits.com	N/A	demo@revb					
revbits.net	N/A	admin@adr					

Name	Active Jump Server 2
Internal IP	10.160.0.12
Hostname	jump2.pam.revbits.net
Hostname or IP	Hostname
Description	N/A
Version	N/A
Status	Inactive
On Boarding	✓
Status Port	8889
Ports	Cassandra: 9042 HTTP: 443 MSSQL: 1433

Jump Server architecture extends security of onboarded assets and prevents obfuscation of keystroke and video recorded sessions

A complete onboard password management system allows admins to deploy a password manager across the enterprise to all employs and manage policies

RevBits PAM is a multi-module access solution. The password management is deployable to all employees. The Jump Server architecture eliminates direct access to onboarded assets.

For more information, go to www.revbits.com

Best practices for deploying RevBits PAM in OT environments

Organizations should consider the following best practices to effectively implement RevBits PAM in OT environments.

Discover and manage privileged accounts - Identify all privileged accounts in the OT environment, including those associated with devices, applications, and human users. Centralize the management of these accounts, implement strong password policies using password management software, and enable multi-factor authentication (MFA) to enhance security.

Implement least privilege - Privileged users, such as engineers, system administrators, or contractors, may have extensive access rights. These users can intentionally or inadvertently misuse their privileges without proper controls, leading to system disruptions, unauthorized changes, and data breaches. RevBits PAM helps mitigate these risks by enforcing the principle of least privilege, granting access based on specific roles and responsibilities, and monitoring privileged user activities for suspicious behavior. RevBits PAM grants users the minimum privileges required to perform their tasks and enforces just-in-time access, time-bound access, and privilege elevation workflows.

RevBits PAM ensures that privileged accounts are properly managed, authenticated, and authorized, reducing the risk of unauthorized access and preventing malicious actors from manipulating critical systems.

Monitor and audit privileged activities - Deploy robust monitoring solutions to record and analyze privileged user activities in real time. Implementing session recording, anomaly detection, and user behavior analytics helps identify suspicious behavior and facilitates forensic investigations if an incident occurs.

Credential theft and lateral movement - Compromised privileged credentials are a significant security risk in OT environments. If attackers gain access to privileged accounts, they can move laterally within the network, escalating privileges and accessing critical systems. RevBits PAM enhances security by implementing strong authentication mechanisms, such as multi-factor authentication (MFA), and regularly rotating passwords for privileged accounts, reducing the risk of credential theft and unauthorized lateral movement.

Regularly review and update access policies - Conduct periodic access reviews and ensure access privileges are regularly reviewed, updated, and aligned with organizational requirements. Implement a strong joiner, mover, and leaver (JML) process to ensure appropriate access during employee onboarding, role changes, and offboarding.

Accountability and traceability - In OT environments, it is essential to have accountability and traceability of privileged actions to identify potential security incidents, detect anomalies, and conduct effective forensic investigations. RevBits PAM provides detailed audit logs and session recordings, allowing organizations to monitor and review privileged user activities. This ensures accountability and identifies any unauthorized or suspicious actions taken by privileged accounts.

Avoid compliance violations - OT environments are subject to various regulatory frameworks and industry standards, such as NERC CIP, IEC 62443, and ISO 27001. Failure to comply with these requirements can result in penalties, legal liabilities, and reputational damage. RevBits PAM helps organizations meet compliance obligations by implementing controls and access policies, enforcing separation of duties, and ensuring proper documentation and reporting of privileged access.

Managing vendor and third-party risks - OT environments often involve interactions with vendors, contractors, or third-party service providers who require privileged access to systems and networks. Managing these external privileged accounts poses inherent risks. RevBits PAM enables organizations to implement secure vendor access management processes, enforce access controls, and monitor the activities of third-party privileged users, reducing the potential for external threats.

Continuous education and awareness – Educate and train employees about the significance of privileged access in OT environments and the potential risks of mishandling privileged accounts. Foster a culture of cybersecurity awareness and provide regular training sessions to ensure employees understand their responsibilities and adhere to security best practices.

PAM is a critical component of securing operational technology environments. Unauthorized access to OT systems can lead to system manipulation, unauthorized configuration changes, and the introduction of malicious code. RevBits PAM ensures that privileged accounts are properly managed, authenticated, and authorized, reducing the risk of unauthorized access and preventing malicious actors from manipulating critical systems.

By implementing RevBits PAM and following best practices, organizations can mitigate external security risks, ensure compliance with regulations, safeguard against internal threats, and enhance the overall security posture of their OT environments.

Keep Your Enterprise Protected. Get a Demo or Free Evaluation.
To learn more, visit www.revbits.com