RevBits®

DATA SHEET

Privileged Accessed Management

RevBits PAM – Fully Covered and Simply Delivered at Enterprise Scale.

Discover an access management solution that delivers multiple access control modules in a single solution to manage privileged accounts of users across the entire organization.

Privileged Access Management

Native clients
As a result of an extensive reverse engineering effort RevBits Privileged Accessed Management (PAM) uniquely supplies native clients on all operating systems for all supported protocols. This means privileged users are free to use any tool or application of their preference to connect to their assets while being fully protected by RevBits PAM while maintaining the full functionality of the original protocol. Native clients are available for SSH, RDP, VNC, Telnet, Oracle, MS SQL, PostgreSQL, MySQL, Cassandra...

Web app monitoring
As companies are relying more and more on web-based applications (SaaS), RevBits PAM supports onboarding and monitoring any HTTP application and session.

Extensive monitoring and logging
All privileged sessions can be both video and keystroke recorded. All recording is strictly done on a central server to prevent tampering with evidence. Unique to RevBits PAM and powered by our native clients, all database activity can be logged at the individual SQL statement level. Command watchlists and filtering are readily available while clickable keylogs make navigating to relevant video segments extremely easy.

Protects and monitors privileged accounts through a wide variety of modules, including privileged access, privileged session, password, CI/CD integration, service account management, key management and certificate management.

Extensive reporting and analysis
A large set of audit reports and metrics are available as standard features. Custom detailed reporting and analysis is provided through an easy-to-use, dynamic query language which allows even non-technical users to generate sophisticated reports.

Behavioral analytics
RevBits PAM will gradually learn the usage pattern of Privileged Accounts and proactively alert in case anomalies are detected.

Integrated workflow management
An integrated workflow engine and visual designer allow for easy creation of even the most complex multilevel approval workflows for granting access to assets. For audit purposes all workflow execution steps are recorded and stored.

Automated onboarding of cloud assets
Automated discovery and onboarding of assets for all major cloud infrastructure providers.

Automated data migration and asset onboarding from existing PAM solutions
To meet customer requirements for automated data migration and asset onboarding from popular incumbent PAM solutions, RevBits PAM developed technology to enable admins to accomplish system migration efforts both swiftly and cost-effectively.

Privileged Session Management

Monitoring and recording

Using native clients, Privileged Session Management provides monitoring and recording for assets that are not onboarded to PAM. Sessions can be keystroke and video recorded.

Password Management

Customizable password management

Password management module supports authentication in common protocols such as web applications, SSH/RDP/VNC servers and more.

Hardware tokens

Extend authentication security with hardware security modules (HSMs), smart cards, USB tokens, Near-Field Communications (NFC), and RFID technologies.

Comprehensive platform coverage

Native applications and browser plugins are available for all major platforms and operating systems. Operating systems include Windows, Linux, Mac OS, iOS, Android (OS) and browsers include Chrome, Firefox, Opera, Safari, IE and Edge.

Stop acquisition of data in memory

Password manager will block unauthorized access to process memory.

Service Account Management

Service account management

The module can scan and onboard service accounts, scheduled tasks and IIS web applications running under the context of hard-coded credentials.

Run services under managed control

Run selected services, applications, and scheduled tasks under the context of a managed service account.

Proper security for services

Through the module, secure service account passwords with automatic rotation and proper maintenance.
CI/CD Integration

CI/CD Integration

Common pipeline toolset integration

RevBits CI/CD module allows seamless integration with the most popular CI/CD pipeline toolsets. The module supports Jenkins, Puppet, Terraform, OpenShift, Ansible, Docker, Cloud Foundry, and Kubernetes with future tools under development.

Secure secret management

Installing the RevBits CI/CD pipeline plug-in to your current secure secrets management solution across the CI/CD lifecycle, allows for easy management of CI/CD users, credentials, and assets.

Certificate Management

Multifactor authentication

Configurable to require the use of multifactor authentication for users to access network assets.

Protective SSL scanner

The SSL Scanner provides periodic updates on expiring certificates, identifies weak hashing algorithms (in certificates) and other weaknesses in SSL implementations.

Key Management

Complete key management

Generate symmetric and asymmetric keys and encrypt, decrypt, sign and verify data, all in one module with comprehensive source code samples.

Ensured data security

All data is encrypted and decrypted in the browser, never at the server - ensures that if server is breached only encrypted data is accessible. Keys never leave the device. (U.S. Patent)

Comprehensive dashboard

RevBits Privileged Access Management dashboard provides administrators with a complete overview of the status of passwords, privileged sessions, keys and certificates.

Software Requirements

Operating systems: Available on Windows, Linux, and MacOS (all versions)

Mobile apps: Available for Android and iOS

Browser environment: Accessible in any web browser

Available web Browser extentions: Chrome, Safari, Firefox, and Internet Explorer

Privileged Access Management Benefits

High-end privilege access management – Provides the ultimate security abstraction by leveraging ephemeral access control and detailed records to that users aren't able to circumvent password management systems.

User selectable algorithms – Based on the information being protected, choose which algorithm meets the level of security needed.

Custom softwared and app integrations – Choose where to integrate in any application, database, or microservice architecture though our API.

Automated password rotation – User definable password rotation and frequency so that selected passwords will automatically be changed.

Fully customizable – Create as many password storage-vaults as needed and specify options, access controls, encryption, two-factor authentication, sharing options, and more.

Additional Solution Features

Fully featured in an Air-Gap environment – RevBits Privileged Access Management is fully deployable in an air-gap environment. All modules are also deployable in an air-gap environment, except for the CI/CD Integration module. All product features are functional and actionable without an internet connection.

Zero-knowledge encryption – RevBits Privileged Access Management utilizes a zero-knowledge encryption model for maximum data security, where data encryption takes place on the device. The encrypted data is stored on the server and the encryption key never leaves the device. Encryption keys can be derived from user provided passwords (PBKDF) or from smart cards, HSM devices, USB keys, keyfiles and RFID/NFC tags.

Full integration – RevBits Privileged Access Management can be integrated into different directory services including Microsoft AD, LDAP and event managements system i.e. SIEM. Additionally, for ease of integration, RevBits Privileged Access Management provides full API functionality with documentation and sample source code in all common programming languages.

Complete password management solution – RevBits Privileged Access Management Password Module includes native clients for all common operating systems and browsers, saves and files all web application passwords. The Password Module also automatically provides strong password suggestions based on minimum password policies. Additionally, zero-knowledge encryption is used to ensure safety and security of user passwords.

Modern, easy-to-use and comprehensive – RevBits Privileged Access Management regulates access to critical resources, captures keystrokes and video records all privileged sessions. Fine-grained rules such as session length, days of the week, time of day and more control user access. Additionally, single-click server connections eliminate the common, complex process of accessing critical infrastructure.

Simplify and streamline key management – Through the RevBits Privileged Access Management Key Management Module, users can easily generate and store encryption keys. The key management library, which includes sample source code in all common programming languages, simplifies the processes of encrypting, decrypting, signing and verifying data. This eliminates the need to store and safeguard the keys separately and write, test and implement cryptographic libraries.

Real-time certificate monitoring – Scheduled or on-demand scanning detects and identifies all SSL servers in the network. The RevBits Privileged Access Management Certificate Management Module reports all expired or soon-to-expire certificates and vulnerable implementations of SSL. The historical and current status of all SSL servers and certificates are displayed in an easy to navigate dashboard with a single-click export feature.

DBA monitoring – RevBits Privileged Access Management is uniquely designed to augment asset access management with DBA monitoring capability. Through unique architectural design, critical database servers such as Oracle SQL, MSSQL, PostgreSQL, MySQL and Cassandra can be onboarded and access to these servers by database administrators, can be monitored.

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