

## Privileged Access Management

# PAM Administration Expands with Secure Workflow, Password, and Native Client Access Management.



Digitally-enabled companies rely upon critical resources, including servers, databases and applications that are on premise and/or in the cloud, to run day-to-day business operations. Privileged accounts, when unmanaged, can allow unlimited access to these critical IT resources.

Due to their exceptional nature, privileged accounts should be highly protected, and usage should be secured, limited, monitored and recorded. Privileged Access Management, or PAM, has become a key enterprise security stack requirement for managing and controlling access to these resources as part of an overall cybersecurity strategy.

### Privileged Access Management

RevBits PAM is a next generation solution with comprehensive drag-and-drop functionality based on a modern architecture. Several unique features and capabilities make it stand out from the competition.

Instead of buying multiple solutions from different vendors for all of these capabilities, RevBits PAM leverages these extensive capabilities within a single solution. Further still, RevBits PAM can be brought into the full capabilities of RevBits Cyber Intelligence Platform (CIP) with native integration of Email Security, Zero Trust Networking (ZTN), XDR/Endpoint Security and Deception Technology.

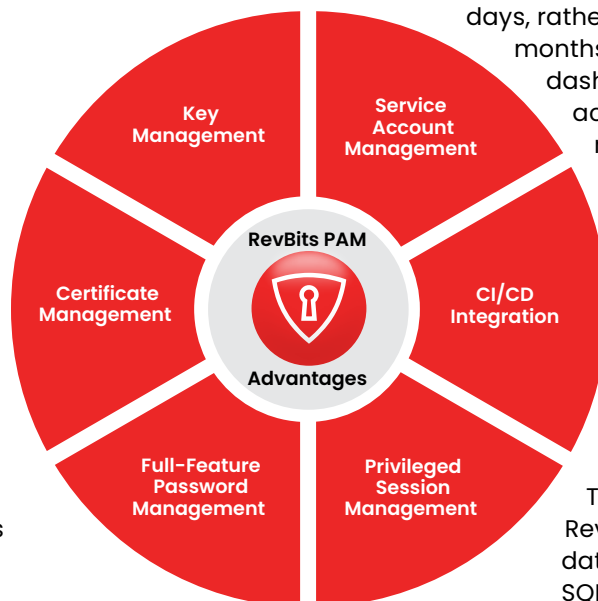
RevBits PAM has a modern and scalable architecture using a combination of PAM servers, jump servers and support for native clients for each protocol. There is no

need to install agent software on endpoints or the IT resources that users and devices access. As demand grows, more jump servers may be added as needed, making RevBits PAM infinitely scalable.

RevBits patented zero-knowledge encryption technology ensures all critical data exchanged is safe, whether at rest or in transit. Using Active Directory, LDAP and Kerberos SSO, for resources on-premises and on popular cloud platforms, resources and users are automatically discovered and onboarded to RevBits PAM.

RevBits PAM implementation can be completed within days, rather than the usual multiple weeks or months for other solutions. The modern dashboard allows for single-click access to the most frequently used resources. RevBits includes communication protocols for all major databases and operating systems, such as RDP, Oracle, Cassandra DB, MySQL, SSH, Telnet, MS Sequel, and others. This allows admins to use their tools and applications of choice to manage and control server and database access.

Through enabling native clients, RevBits can monitor and record all database activity at the individual SQL statement level. All privileged sessions can be monitored and recorded live, including video and keystroke recording. Recorded sessions are easily searchable for specific actions and relevant video segments, and video recordings can be exported, along with key logs and metadata.



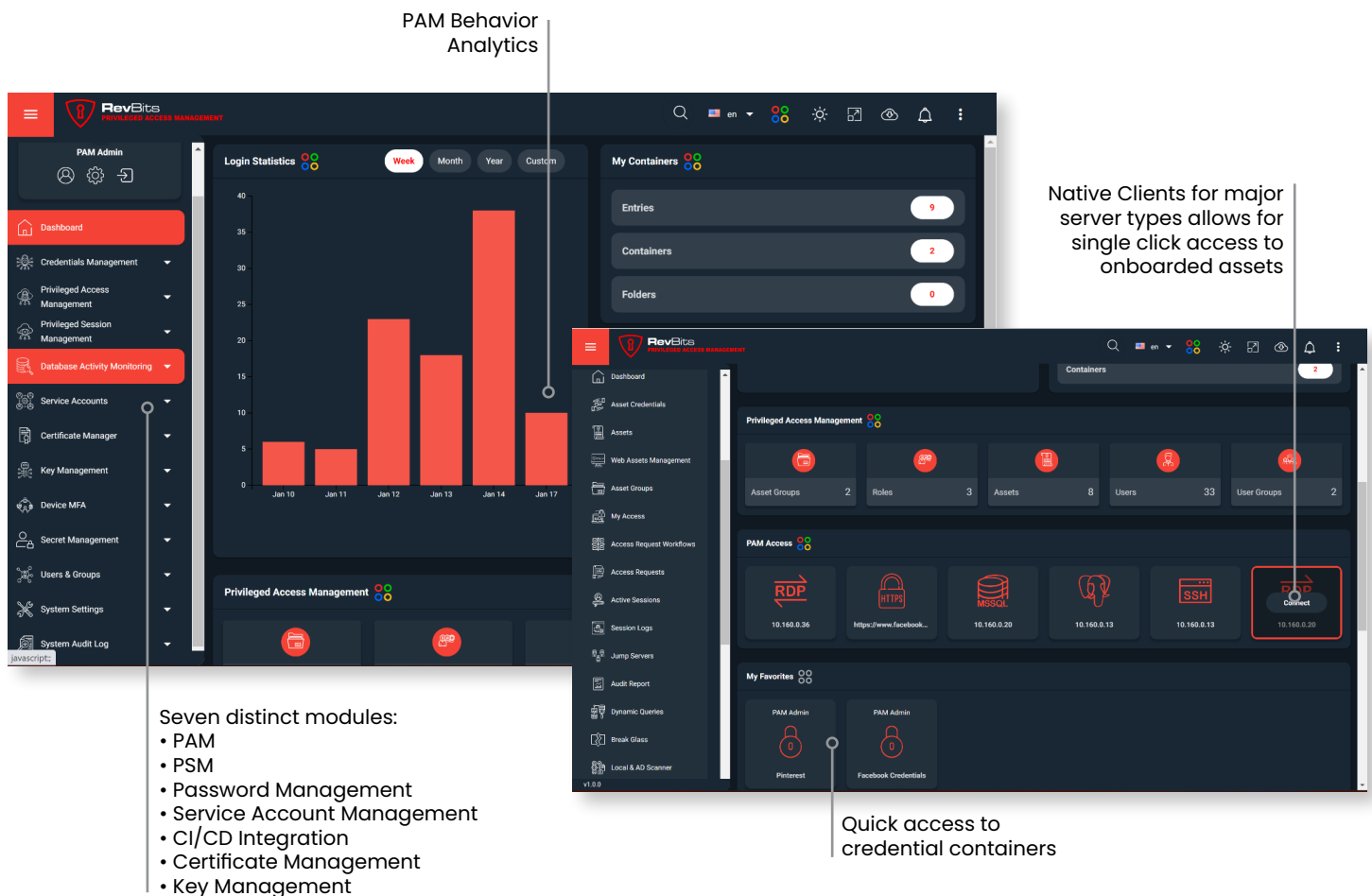
Revbits PAM extends core privileged access management with natively integrated security modules.

In today's complex business environments, granting external or remote third-parties access to internal servers, databases, services and applications is a common need. RevBits PAM's remote access management module is based on Zero Trust Networking (ZTN), to provide a safer, faster and more reliable alternative to VPN. ZTN within RevBits PAM can grant highly granular access to specific servers, databases, services and applications, while recording all remote user activity.

Organizations often use SaaS and web-based applications for their critical business functions. RevBits PAM web application management secures and monitors access to these applications. Popular SaaS applications come predefined "out-of-the-box", but with just a few clicks, any custom web app can be added to RevBits PAM.

Behavioral analytics across all modules further enhances the protection of critical accounts. Early detection of anomalies in the usage pattern of privileged accounts triggers alerts to take quick action and secure critical resources.

RevBits PAM conducts privileged management, session management and elevation management via device multi-factor authentication (MFA). Service accounts for Windows tasks scheduler, Windows services, and IAS web applications are agentless, and integrated with AD, LDAP and Kerberos. Rules can be easily and quickly enabled, and hard-coded credentials can be automatically on-boarded to RevBits PAM with updated and rotated credentials. Human and machine discovery is accomplished by scanning privileged accounts wherever they are located.



RevBits PAM offers seven management modules in one solution. Native-client architectures for common server types are quickly onboarded and accessed with one click.

## Expand PAM administration with onboard workflow manager

Onboard Workflow Manager (OWM) is a fully integrated GUI-based design and workflow engine natively integrated within RevBits PAM. Admins can simply drag-and-drop and easily design an access request workflow for a single asset or group of assets. Automating access requests from users to admins to approve workflows saves time, resources and money, enabling the process to be ten times faster, smoother and more efficient.

The comprehensive workflow management engine supports multilevel approvals for granting access to resources. All approved workflows are stored for audit and analysis, and can be attributed to users, credentials, resources, and groups.

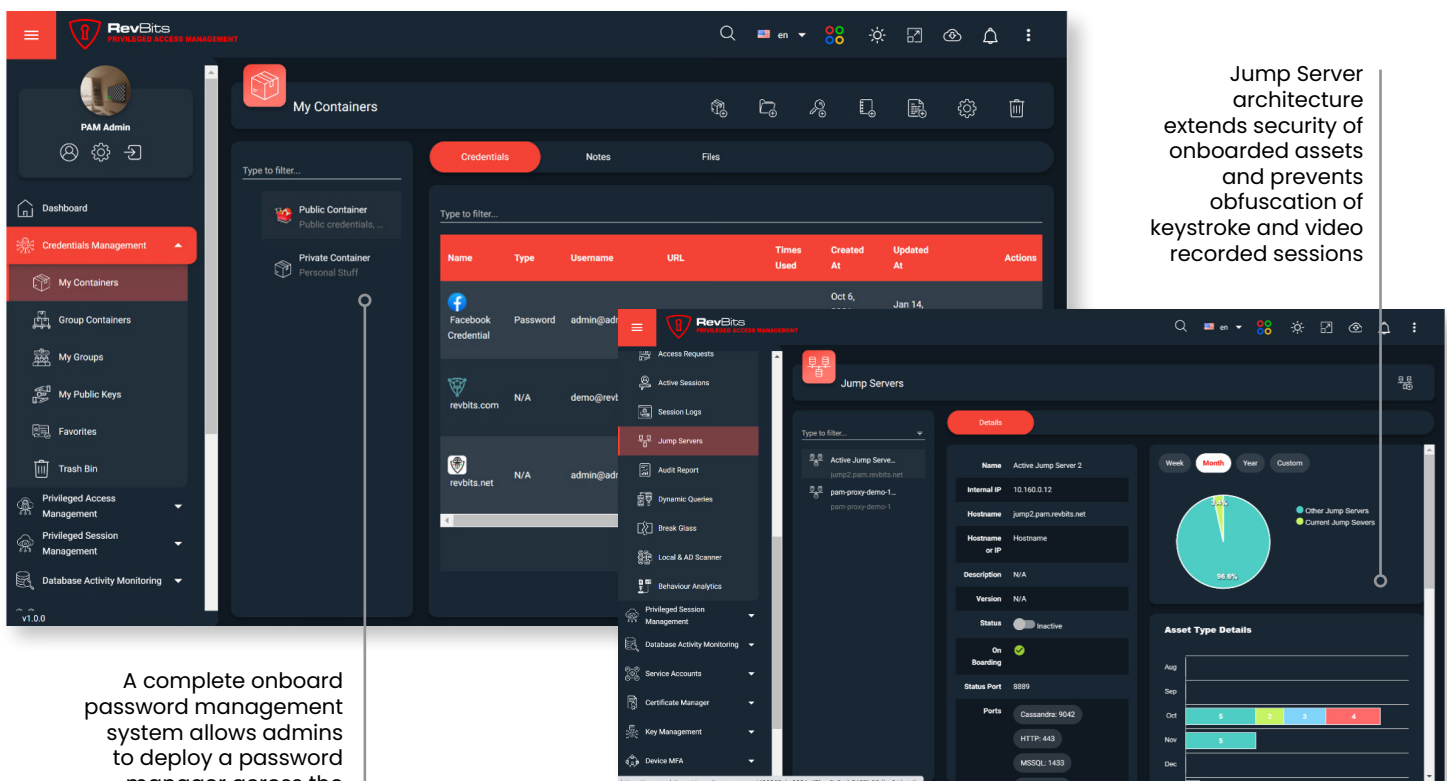
Orchestration of workflow management within the intuitive dashboard makes it easy to define workflow steps needed for user role approvals. With a single click,

approvals can be easily and quickly recalled. Workflow processes and user activity is integrated with behavior analytics, and can be integrated with any SIEM.

## Password management with browser-based zero-knowledge encryption

Password Manager is built into RevBits PAM as an optional module. It can also be purchased as a standalone product. With Password Manager natively integrated into RevBits PAM, organizations can automatically expand their identity access management (IAM) architecture to include automated password management for all employees, without onboarding a separate product into their security stack.

Transmitting and receiving encrypted data through a client browser without agent software installed can be difficult. Similarly, maintaining encrypted data at rest and in transit for web applications is not a simple process. However, RevBits overcomes this problem through patented browser-based zero-knowledge encryption.



The screenshot displays the RevBits PAM Admin interface. The left sidebar contains navigation links: Dashboard, Credentials Management, My Containers, Group Containers, My Groups, My Public Keys, Favorites, Trash Bin, Privileged Access Management, Privileged Session Management, and Database Activity Monitoring. The main content area is divided into two sections. The top section, 'My Containers', shows a table of credentials with columns: Name, Type, Username, URL, Times Used, Created At, Updated At, and Actions. The bottom section, 'Jump Servers', shows details for 'Active Jump Server 2' with fields for Internal IP, Hostname, Description, Version, Status, On Boarding, Status Port, and Ports. A pie chart and a bar chart are also visible in the Jump Servers section.

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 employees 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.



When employees use a password manager, businesses increase the security of their business-critical login environments, portals and applications. With RevBits browser-based zero-knowledge encryption, encryption keys remain on the endpoints, no aspect of the password is revealed in communication, and encryption keys are never transmitted to the servers. This protects the businesses' servers against malicious hackers trying to harvest credentials.

With data encryption taking place on the endpoint device, RevBits PAM browser-based zero-knowledge encryption model enables maximum data security. Encryption keys can be derived from user-provided passwords (PBKDF), smart cards, HSM devices, USB keys, key files and RFID/NFC tags.

RevBits Password Manager provides complete password management for all employees to control access for corporate logins, and optionally for employee's personal accounts, while being centrally contained and administered within a single dashboard.

RevBits Password Manager supports Windows, Mac, Android, iOS and browser extensions, and allows admins to create user and group containers for various purposes. Within user and group containers, admins can choose among different encryption algorithms, as well as cascading encryption.

## Jump server architecture enhances asset protection and secures forensic review of sessions

There are two main principal security enhancements a jump server provides for PAM. First, the user and the resource are not directly connected to each other. In other words, the user does not have a direct connection to a resource, and therefore, cannot leave "backdoor" access credentials on a resource. Secondly, all session recording is conducted at the jump server, not on user devices. This protects the organization from malicious activity by not allowing a bad actor to obfuscate logs and recordings, as session recordings and logs on a jump server are not accessible by the user.

The RevBits jump server isolates user sessions by passing a randomly generated credential that is valid for two minutes, for a one-time use. The jump server makes the connection, and then passes the real credentials directly to the real server or database. The user never sees the real credentials or real server IP addresses.

RevBits jump servers run on-premises, in the cloud, and within hybrid environments. RevBits PAM is integrated with Active Directory and LDAP, as well as clouds, including AWS, Azure, Google Cloud, and others using API keys. Admins can define filters for servers within specific zones, data centers, IP ranges and tags, and automatically pull the servers into RevBits PAM. Jump servers can also be located within a VLAN for highly restricted access control. RevBits PAM is network segmentation aware, and handles connections to segmented assets through appropriate jump servers automatically.

## Native client capability is integral to next-gen PAM

As discussed above, jump server architecture offers enhanced server security and session auditing integrity. But, to also offer a true next-gen PAM, the solution needs to provide native client capabilities.

Native client capabilities enable enhanced resource security and simplifies onboarding and access to resources. Additionally, management is greatly enhanced with single click access and easy communication with onboarded servers, regardless of OS or browser environment.

RevBits PAM native clients include Windows, Lynx, Mac, Android, iOS, and browser extensions. These are located within the dashboard's system tray menu. Other PAM products require admins to login, locate the account and



server, and download an RDP file to gain asset access. RevBits PAM jump server architecture allows for its native clients to be maintained as protocols on the jump server, and thereby user interaction and connection with those clients are seamless, without requiring additional user effort.

The automated native client technology in RevBits PAM enables fast and safe connections to various server types running in a particular environment. Leveraging the original protocols through native clients, RevBits PAM allows admins to use their tools of choice to access assets, while not being forced to use a specific tool or workaround. For accessing databases, using a native protocol allows admins to log all activity at the individual statement level. This helps increase forensics and oversight to quickly remediate any potential resource abuse.

For native clients, RevBits supports communication protocols, including RDP, Oracle DB, Cassandra DB, MySQL, SSH, Telnet, MSSQL, and others, through RevBits protocol handler.

### **Do other PAM solutions “offer” native client capabilities?**

In most cases the native capabilities are usually a patchwork of connections and manual workarounds. Typically, the PAM solution architecture will log users into an RDP session, load their client of choice on the server, and then log the user in. The user may be required to install Oracle client tools on the jump server, or on the admin's workstation, to login to an Oracle DB. While this may seem a minor issue, it creates additional admin work, and requires the installation of tool sets onto the jump server or admin workstation.

Additionally, the admin will still need to establish an additional session to interact with the desired server and the desired server tool set. While the Oracle client might be the user or developer's preferred choice for the application, connecting via SSH to an SQL database first requires admins to log into an RDP session by opening an RDP window, before they can enter commands.

For ease-of-use, and more granular control, admins generally prefer to use native protocols that apply to the technology that is best suited for their application. Additionally, for video and keystroke recording of user sessions, RevBits PAM enables the use of native clients, including SSH, RDP, VNC, SQL, Telnet and others.

When native clients are supported, all protocol capabilities are supported as well. For instance, in other PAM products, you cannot use SSH port forwarding or SCP. With RevBits PAM, if admins enable and grant these permissions, users can use SCP or SSH port forwarding with any native SSH client, and RevBits PAM videos will capture keys pressed for all these sessions.

### **RevBits PAM is a next generation solution built on a modern architecture**

RevBits PAM management capabilities bring extraordinarily intuitive and easy-to-use drag-and-drop functionality. Diverse security modules extend privileged access management to include privileged session management, service account management, web application access management, third-party access management, full-featured password management, certificate management, key management, and more. Its modern architecture combines PAM servers, jump servers and native clients for a more secure and easily managed solution that flexibly scales to meet growing security requirements wherever the corporate perimeter happens to be.

[Learn](#) about RevBits PAM managing and protecting CI/CD secrets.

[Download](#) RevBits' Cyberbrief “Zero Trust Networking is Digital Transformation's Response to Enterprise Security”.

**[Keep Your Enterprise Protected. Get a Demo or Free Evaluation.](#)**  
**To learn more, visit [www.revbits.com](http://www.revbits.com)**