Securden

Unified PAM | Cloud Edition

Security Design and Specifications

Index

Introduction

Securden restricts and controls access to the most sensitive assets in your organization and its security design takes paramount importance. The product has been forged using the latest and robust security standards.

Securing Stored Data - Encrypted Central Vault

The encrypted credential vault forms the core of Securden Password Vault, Unified PAM, and Enterprise PAM solutions. The vault is a completely access controlled, highly available server instance hosted on AWS cloud. While the business logic is handled by the server, end users can access it using a web browser.

Design of the vault

Each customer's data is completely segregated and stored in the database. Each customer's segment can be considered a separate database since each customer's data in the database will be encrypted using a unique encryption key.

Encryption key management

The unique encryption key is generated automatically and stored in Amazon's Key Management Solution and cannot be accessed by anyone outside your organization. This is ensured by enforcing the use of AWS CloudHSM keystores for encrypting and decrypting the database using the key. Whenever a customer's data is in the queue for decryption or encryption, a separate slot is created with the corresponding key. The key is stored in an unextractable form by the key management system within the CloudHSM cluster.

Data storage

All sensitive data is stored in the digital vault in the encrypted form using AES-256 algorithm. The sensitive data is encrypted by using the encryption key at the application level. The encrypted data is securely stored inside the segmented database.

Data integrity

Each organization's data in the database is encrypted using a unique encryption key. It cannot be accessed by anyone outside the organization. Even if unauthorized intruders manage to infiltrate, they get access only to the encrypted data. It cannot be deciphered in plain text without the encryption key.

Design Highlights

- AES-256 data encryption
- Each organization/client data is encrypted using unique encryption key to ensure data integrity
- Encryption key is stored in Amazon KMS and all cryptographic operations are handled within a CloudHSM cluster

Controlling Access to Unified PAM Cloud Edition - Authentication Methods

Access to the vault is controlled at two levels. The vault can communicate with all LDAP compliant directory services including Azure, AD, and G Suite for user onboarding, offboarding, authentication and access provisioning. In addition to this,

the solution also supports all SAML-based SSO options for a single sign on experience. For the second factor of authentication, Securden integrates with all RADIUS-based MFA solutions. Use of smartcard-based primary authentication is also supported.

Alternatively, the Securden's native authentication methods can be used by locally created users to log in to the vault.

How does Securden authenticate using directory services?

Securden doesn't store credentials when authenticating through a directory service. It connects with the directory service through SSL and authenticates against AD. Securden Unified PAM communicates with Azure through secure channels by using Azure client IDs and secrets.

How secure is Securden's native authentication?

To withstand brute force attacks, a one-way hash of the password is created through *brcypt* hash function, one of the advanced algorithms available. Once the hash is created, the hash is then combined with salts to protect against attacks. Even in the rare case of the database getting breached, the encrypted data cannot be deciphered without the encryption key.

Additional layer of protection using MFA

Securden helps add an additional layer of security by requiring a second factor of authentication before allowing users to access the vault. Securden integrates with an array of solutions from which you can use any to enforce MFA.

Programmatic access using authentication tokens

The vault can be accessed programmatically for fetching credentials using APIs. For authenticating the API requests, Securden follows a token-based authentication mechanism. Human and non-human entities need a URL and Auth token to access the vault's content.

Design Highlights

- AD authentication over SSL
- Azure authentication through secret generated in Azure
- Credentials are hashed using brcypt function and then salted
- Integration with MFA solutions for added security
- Secure token-based authentication for APIs

Securing Data in Transit - Communication between Components

Users from different devices access the vault through the web UI, browser extension, and the desktop client to gain access to the credentials and their corresponding IT assets. In all the methods mentioned above, Securden secures the transfer of data through secure channels in the encrypted form.

Data transmission between Securden and the web interface

All data transmitted between the vault and the interface is encrypted and communication is handled through HTTPS. Access to the database is authenticated through SSL certificates. A third-party signed SSL certificate or a wild card SSL certificate can be enforced through Securden.

Accessing credentials through APIs, browser extensions, desktop clients, and mobile applications

Accessing your credentials using Securden is secure across all platforms. The mobile app, desktop application, browser extension, and programmatic access through API is just as secure as accessing the web UI. No data from Securden will be cached locally. The data is always fetched only from Securden server. Also, you can grant and revoke access to extensions, APIs, mobile applications, and desktop clients for specific users from the interface.

Establishing Remote Access and Recording Sessions

Securden helps launch secure connections to servers, databases, network devices, and other assets. By default, all remote connections and remote operations are routed through Securden to prevent direct access from end user machines to target devices.

This method helps launch remote connections without adopting perimeter-based security systems such as VPN or perforating the corporate firewall. The remote connection can either be web-based or through native RDP and SSH clients.

Web-based connections

Web-based connections are supported out of the box and no ports are required to be opened. All connections are routed through a remote gateway and web-based connections are recorded as a series of screenshots that can be played back as a video later.

Native clients for RDP and SSH

To launch remote connections to IT assets through native RDP and SSH clients, you need to install a lightweight session management agent on the remote gateway in your network. The remote gateway is an API-based application server which communicates with the Securden server in the cloud. Session recording and routing happens through the Securden session manager. Recorded sessions are securely stored in the database.

Grant access without revealing passwords

The remote access mechanism allows you to grant access to IT assets without revealing the underlying passwords, SSH keys, and certificates. This helps avert risks associated with privilege misuse.

Data Access Controls

The access control methods in Securden ensure even after successfully passing through multiple levels of authentication, users will only have access to the data allotted to them. With a combination of granular access permissions and role-based access controls, Securden ensures that users don't get access to passwords that are not required for their job profile. Granular access sharing ensures users get only the level of control over a credential that they require.

Clear ownership of accounts

The person who adds an account to the vault is designated as the default owner. If an owner leaves the organization, all passwords owned by the user can be transferred to a different user. This way none of the accounts stored in Securden is orphaned. Risks associated with orphaned accounts such as stale passwords and privilege creeps can be averted.

Streamlined access provisioning

Securden allows users and administrators to group similar accounts into folders. These entities can be shared with other users and user groups with granular access privileges. For example, if there is a group of Windows administrators in your organization, you can create a user group in Securden for them and share the folder containing all the corresponding accounts in it. When a new Windows administrator is onboarded into the organization, they will automatically gain access to the accounts. This way a folder works as a micro vault for a group of users requiring access to the same resources.

Just-in-Time access with release controls

Users can raise access requests to their administrators and gain access to sensitive

assets for a limited period. Once this temporary access ends, the password of the account concerned can be randomized. This way, just-in-time access is enforced, and risks associated with standing access to sensitive assets are averted.

Design Highlights

- Just-in-time access
- Folders functioning as micro vaults
- Zero orphaned accounts

Accountability for Actions

An ever-present activity tracking mechanism ensures any privileged activity performed intentionally or otherwise, is always tracked and recorded. The basic design of Securden ensures all activities performed are tracked and establishes a culture of accountability for actions.

Comprehensive text-based audit trails

Securden captures and records activities performed by users such as retrieval, rotation, sharing among others, and more. The details pertaining to each activity are comprehensive and include the user's name who performed it, the device on which it was performed, the exact time of the activity, and others. These details help provide complete visibility into privilege usage within the organization.

Session recordings

All privileged sessions launched can be monitored live, recorded, and stored for future analysis. The video can be used for tracing specific activities and as a solid piece of forensic evidence.

Tamper-proof trails

Access to audits and recorded sessions is granularly controlled. Any attempt made to tamper with the trails and the video recordings will trigger alerts.

Real-time monitoring

Live remote sessions can be monitored. If any malicious activity is suspected, the session can be terminated immediately. This provision also paves the way for users to collaborate and get assistance from the administrator in the middle of a remote session.

Alerts and notifications

Securden sends out timely email alerts as and when specific events transpire. These alerts can prove vital during emergencies where timely action could mean all the difference. Timely alerts help prevent security breaches, issues, and threats.

Design Highlights

- Tamper proof audit trails and video recordings
- Timely alerts on events
- Privileged session monitoring

Data Availability

Reliable and uninterrupted access to critical credentials is crucial for businesses to operate seamlessly. When a solution that regulates access to sensitive credentials is down, the critical business operations suffer and at times fail. Scenarios such as

server crashes or physical damage to machines are very real and to prevent unnecessary downtime, Securden has deployed redundancies and secondary application servers that provide continuous availability of credentials.

Scalable design to handle huge quantities of requests

The solution is hosted in various data centers around the world. Organizations from different locations will use the data center that is geographically closest. Databases specific to the data center will only accept connections from the application server(s). Within a data center, multiple application servers will be used along with a load balancer for optimum scalability.

All application servers are deployed in AWS and have the same security measures. AWS provides an RDS PostgreSQL database which is redundant and highly available.

Miscellaneous

Security aspects of the Securden browser extension

Content security policy is enforced. Inline Java script execution and AJAX requests to other sites are prohibited.

Incident and vulnerability response

Securden Unified PAM is developed by employing the highest standards of security. In the event of an incident, we will provide our customers with all the required information such as what happened, who is affected, why the incident occurred, and when it did occur along with all relevant information available.

Securden products are subjected to multiple levels of rigorous testing to weed out bugs and vulnerabilities. Additionally, Securden partners with Agile Infosec, London

to periodically subject the solution to penetration tests. In case a vulnerability is detected, the hotfix will be released within 24-72 hours depending on the severity of the vulnerability.

Security Framework in the Software Development Life Cycle

Software development life cycle

	Ideation and design	Development of software	Quality assurance	Release
Security framework	Collaborate and brainstorm to identify the possible security flaws and loopholes.	Develop business logic for the new features and security improvements and test the logic for sanity.	Integrate the newly developed modules into the code and perform penetration testing to identify and rectify vulnerabilities.	Run security assessment to identify further areas of improvement for future releases.
	Prepare an action plan taking into account the different flaws and loopholes identified in the brainstorm session along with difficulties faced by users in previous releases, and security recommendations by penetration testing partners.	Continuously test the newly added features and modules to check whether the intended purpose of each feature and module is satisfied.	Continuous sanity testing to ensure the core funtionalities of the product are working as intended after integration of newly developed features and modules.	Run continuous penetration testing activities through partners for identification and timely response to identified vulnerabilities in the product after release.
	Fabricate a design framework and a prototype including all the changes, updates, and security fixes and submit it to the change management team for approval.	Check and verify whether all the third-party libraries used in the product are free from known vulnerabilities before incorporation.		

Our development repositories are secured through https protocol and are subjected to strict authentication and access controls. The Securden engineering team works tightly with the security and quality assurance team to identify, address, and prevent vulnerabilities in the product before and after release.

The team partners and collaborates with third party penetration testing teams to identify areas of improvement and obtains suggestions to improve our security posture.

Apart from the security measures mentioned above, the engineering team and quality assurance team work tirelessly to make the application as secure as possible.