Securden

CLOUD EDITION

Endpoint Privilege Manager

Security Design and Specifications

Index

Securden EPM eliminates administrator privileges on endpoints and helps prevent privilege escalation attacks. The security design of such a solution is of paramount importance. The product has been forged using the latest security standards.

Security Framework in the Software Development Life Cycle

Software development life cycle

Security framework

Ideation and design	Development of software	Quality assurance	Release
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 team works tightly with Agile Infosec for security and penetration testing to identify, address, and prevent vulnerabilities in the product before and after release.

Apart from partnering with third parties, the engineering team and quality assurance team work tirelessly to make the application as secure as possible. The sections below explain the different measures undertaken to ensure the security and sanity of Securden Endpoint Privilege Manager (Cloud Edition).

Securing Data When Stationary

Securden is hosted as a bundle of two servers. An application layer working in tandem with a backend database. While the application layer handles the business logic, the database hosts all the information in an encrypted.

Data encryption

All sensitive data stored in Securden is encrypted at the application level using AES 256 algorithm. This encrypted data cannot be used by anyone without the appropriate encryption key. Your data stays safe even in case of data spills.

Data segmentation for multi-tenancy

Since multiple clients connect to the central server for endpoint privilege management in the SaaS model, Securden works by allocating individual segments in the database for each customer and employs unique encryption key for each segment.

It can be considered as a model that uses a separate database for storing each customer's data.

Amazon key management system

The unique keys used for encrypting the data are generated automatically and stored in Amazon KMS. The keys cannot be accessed by anyone outside the organization as AWS's cloud HSM is used to secure these unique encryption keys at the time of encryption and decryption. The key is used to create a slot for the cryptographic operation and is completely stored and used in an unextractable form.

Design Highlights

- AES-256 data encryption
- Data segregated at the database level
- Data integrity ensured through the use of CloudHSM

Controlling Access to the Interface

Securden EPM (Cloud Edition) is designed so that end users don't have the need to access the main application interface at all. Administrators, auditors, and approvers who are tasked with managing privilege requests can access the web interface using a web browser. End users use the Securden Agent on their endpoints to fulfill their requirements.

Access to the web interface is controlled in two levels. The first one is either through the native authentication method or authentication through an identity provider. Securden integrates with AD, Azure, G Suite for user onboarding and users can authenticate themselves using their directory identities. Additionally, Securden can integrate with all LDAP compliant directories and all SAML based SSO solutions for seamless authentication.

How does Securden authenticate using directory services?

Securden doesn't store the directory credentials anywhere. The authentication is carried over secure channels over SSL and authenticates against AD. To connect with the Active Directory service running on your server, Securden uses a remote connector to connect the AD from cloud.

To connect with Azure (Entra ID), a client secret and secret key pair is used to establish the secure connection.

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.

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

Securing Data During Communication

For managing privileges on endpoints, a lightweight Securden agent has to be deployed on endpoints. The agents help enforce privilege management and application control policies on endpoints. These agents communicate with the central server periodically to pull the latest information. They also help discover applications on endpoints that run with admin privileges and help create control policies.

Communication between server and web-interface, and the database

All data transmission to and from the Securden server is encrypted. Communication between the Securden web-interface and the server happens through HTTPS. Data transmission between the Securden server and database happens through SSL. Securden helps enforce a third-party signed or a wildcard SSL certificate. certificate can be enforced through Securden.

Communication between agent and server

All communication between the agent and server occurs over the internet. The agent authenticates itself with an auth token generated at the time of agent deployment. All communication is handled via HTTPS and is therefore encrypted and verified using TLS (SSL).

Data storage by the agents

Typically, the agent pulls the latest change from the server whenever access to a new application is requested. If the agent is unable to communicate with the server, the policy pulled last will be enforced. The policies stored by the agent cannot be tampered since they are encrypted using the local user credentials along with a unique key. This ensures that the agent cannot be tampered with even if anyone manages to gain access to the encryption key.

Accessing the server from mobile application

Administrators in Securden and users tasked with managing privilege requests can access the server from their mobile through the Securden EPM mobile application. The communication between the app and server is just as secure and no credentials are cached locally.

Communication between AD, remote connector, and the server

If the EPM (Cloud Edition) solution is working with a on premise Active Directory instance, a remote connector should be deployed in a device that can reach the server on which AD is hosted.

The communication from the remote connector and the AD instance is one way only and an inbound port needs to be opened in the firewall of the device running the directory. This communication between AD and remote connector is encrypted and handled via SSL. The remote connector communicates with the Securden server via HTTPS and encrypted and verified through TLS (SSL). The remote connector authenticates itself with the server through a unique auth token.

Design Highlights

- Encrypted communication between server and interface
- HTTPS based communication between server and agent
- Policies are encrypted and locally stored
- Encrypted communication with remote connector

Accountability for Actions

A fool-proof mechanism that tracks, monitors, and records all activities performed by users helps establish a culture of accountability for actions. The basic design of Securden works in accordance with this principle and ensures users are held accountable for their actions.

Comprehensive audit trails

Securden tracks and maintains a record of all activities made by users in the interface. Along with these activities any privilege related activity such as application elevation, commencing an administrator session or a triggering a technician access session will be recorded in the text-based audit trails. These text-based trails serve two purposes. They can be used to generate reports for external audits and in forensic analysis of events.

Tamper-proof

Audit trails pertaining to user activity and privilege management are securely stored. Access to the data follows granular controls. Trails cannot be tampered with. Any attempt to delete data triggers alerts.

Design Highlights

- External audit ready with activity trails
- Tamper proof audit trails

Data Availability

Securden is tasked for managing access to applications and privileges on endpoints. The very use case of the endpoint privilege management solution is business critical. If the privilege management service is not available for a short time, any or all privilege requests will go unattended and result in downtime. To prevent such an event, Securden EPM (Cloud Edition) is hosted with high availability setups so that the agents can continue enforcing policies to the full effect.

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 for PostgreSQL database which is redundant and highly available.

Miscellaneous

Input validation

Securden validates all inputs in the web-interface, and the application is guarded against attacks like SQL injections, cross-site scripting, buffer overflow, and other attacks.

Incident and Vulnerability Response

Securden EPM (Cloud Edition) 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.