Securden

Endpoint Privilege Manager

Security Design and Specifications

Securden deals with the all-important privileged access, and hence the product's security design assumes significance. The solution has been architected by adopting the latest security principles and standards to ensure data security and integrity. This document outlines some of the security considerations and design aspects at various levels.

Contents

Section 1

Central Server

Securden runs on a dedicated central server connected to a backend database. It is implemented as a fully access controlled and highly available cluster of application servers. While the server handles all the business logic, users connect to it using any standard web-browser.

Every installation is secured with an automatically generated, unique random key. The key serves as the master key for various encryption operations in the product.

Data Storage

All sensitive data gets stored in an encrypted form inside the digital vault. Securden uses the *AES-256 algorithm* to do the encryption.

- The sensitive data provided as input to the Securden server is encrypted using the unique installation key. This happens at the application level.
- The encrypted data is securely stored in the database.

Data Integrity

- The encryption key cannot be held together with the encrypted data.
- The encryption key is needed only for starting Securden. It has to be kept somewhere outside and made available to the Securden server during startup.

Even if the database gets into a malicious user's hands, sensitive data cannot be deciphered in plain-text without the installation key.

Database connections

The database accepts only secure connections. Clients can connect only from the same localhost. In high availability configuration, where the server and the database run on different servers, the database accepts connections only from specific IP addresses.

Design Highlights

Data Encryption and Storage	• AES-256 encryption • Encryption key separated from encrypted data.

Section 2

Controlling Access: Strong Authentication Mechanism

Access to Securden is primarily controlled through authentication mechanism. Securden can communicate with LDAP-compliant directory servers (Active Directory/Azure AD) for user onboarding, management, and authentication.

How does AD authentication / Azure AD authentication work?

In this case, Securden doesn't store the passwords. Instead, it connects with the AD through SSL and authenticates against AD or Azure AD.

Security Reinforcement

An additional layer of security with MFA

As an additional layer of security, Securden helps enforce a second authentication factor to grant access to application. It integrates with a variety of MFA solutions to achieve this.

Design Highlights

Primary Authentication	• Active Directory / Azure AD authentication
MFA Enforcement for Additional Security	• Any TOTP Authentication • Any RADIUS-based Authentication • Duo Security • Yubikey • OTP through email • Email-to-SMS gateway

Section 3

Securden Agent

On the end-user machines, a light-weight agent has to be installed. The agent communicates with the server periodically and gets the policies. The agent takes care of enforcing the policies. The agent can also discover the applications from end-user machines and list them on Securden applications inventory. This would come in handy to create policies.

One way communication

The Securden Agent makes use of the HTTPS protocol to establish connection with the Securden server through the server port (5151, by default).

The communication between the agent and the server is always one-way. So, only the inbound connection is required to be open in the firewall.

Typically, the agent tries to get the latest policy from the server when a standard user attempts to run an application. If the agent is not able to communicate with the server, it enforces the policy that was last pulled by it from the server. The product can be deployed in high availability mode with redundant servers. Agents can be pushed to the endpoints in two ways: Either directly from the GUI or through Group Policy Objects.

Data storage by agents

The policies fetched by the Securden agent from the server are kept in fully encrypted form. The policies are encrypted with AES-256. The policies cannot be tampered with at the agent level.

Design Highlights

Agent Communication	• One-way with the server, HTTPS
Data Transmission	• SSL
Data Storage by Securden Agent	• Encrypted (AES-256)

Section 4

Data Transmission Between Various Components

Administrators and end users connect to the Securden server through the web-interface. Securden ensures that the data transmission happens through secure channels in encrypted form. (Endusers generally need not have to connect to the web-interface).

Data Transmission: Server - Web-interface, Server - Database

All data transmission to and from the Securden server is encrypted. The communication between the Securden web-interface and the server is encrypted and happens through HTTPS. Data transmission between the Securden server and database happens through SSL. Securden enforces deploying a third-party signed or a wildcard SSL certificate.

Design Highlights

Communication (Server and Web-interface)	• Encrypted over HTTPS
Data Transmission (Server and Database)	• SSL

Section 5

Accountability for Actions

A robust mechanism to record and trace activities helps establish a culture of accountability for actions (unintentional or otherwise). The basic design of Securden precisely ensures that.

Comprehensive audit trails

Securden maintains a complete trail of all user activities across the organization. The comprehensive trails help in forensic audits when something goes wrong.

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

Accountability for Actions	• Comprehensive audit trails • Tamper-proof • Controlled access to trails

Section 6

Availability

Reliable, uninterrupted access to Securden is critical for business continuity. There should be provisions for data backup to handle unexpected situations like a server crash or other physical damages to machines in addition to continuous availability. While the backup and high availability provisions are offered to handle these scenarios, it is important ensure security around these measures.

The high availability architecture ensures security in all aspects. As the configuration involves running the Securden server and the database on different servers, the database has been configured to accept connections only from specific IP addresses - typically, the servers configured as 'high availability servers' alone. Besides, the database is enforced to accept only SSL connections. The database is guarded not to accept other connections.

To ensure security, the backup copy remains fully encrypted. The encryption key is separated from the backup copy. Typically, the live version and the backup share the same encryption key. While trying to restore data from the backup, the encryption key is needed. Without that, the restoration will not happen.

Section 7

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.

Server hardening

Securden is recommended to be run on a dedicated, hardened server. Except for the web-server port, no other port needs to be opened on the firewall. No other communication happens with outside entities.

Securden, Inc.
2035 Sunset Lake Road,
Suite B-2, Newark,
Delaware, 19702