



# Endpoint Privilege Manager

Remove local administrator rights without impacting productivity.

A single plane of control to remove local admin rights and elevate individual applications across Windows, macOS, and Linux endpoints for standard users.



## Windows, Mac, & Linux

One console to manage devices across all three operating systems.



## Zero Standing Privilege

No employee holds administrator rights permanently.



## Just in Time Elevation

Elevate applications for standard users temporarily, only when needed.



## Works Offline

Cached policies and code-based elevation to ensure least privilege for remote workforce.



**Product Datasheet**

SaaS, On-Premises, and  
Private Cloud Deployment Options

For enterprise security, IT operations, compliance, and infrastructure leadership teams.

# Product Overview

| Platform Goal                                                                                                              | Deployment Model                              | Primary Security Outcome                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Discover and eliminate local administrator accounts from endpoints and elevate individual applications for standard users. | SaaS, On-premises, and private cloud options. | Ensuring zero standing privileges, granting just enough privileges on a just-in-time basis, and audit privileged access across hybrid IT environments. |

Securden Endpoint Privilege Manager (EPM) helps organizations enforce least privilege by removing unnecessary local admin rights across Windows, macOS, and Linux endpoints. It enables secure, just-in-time privilege elevation and application control through granular, policy-based controls and robust approval workflows. EPM also provides centralized visibility into endpoint privileges, applications, and admin accounts to reduce security risks and strengthen endpoint protection – without compromising on productivity.

## Core Technical Capabilities

| Function                | Capability                   | Description                                                                                                                                                                                                     |
|-------------------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Discovery and Inventory | <b>Computer Onboarding</b>   | Import computers from Active Directory or Entra ID by group or individual machine, and onboard non-domain devices using the Securden Agent.                                                                     |
|                         | <b>Local Admin Analysis</b>  | Identify users and groups with local administrator rights and view local accounts across managed endpoints.                                                                                                     |
|                         | <b>Application Discovery</b> | Discover applications requiring elevated privileges and maintain them in a centralized repository. Add applications using attributes such as digital signature, file path, original file name, or SHA-256 hash. |

| Function             | Capability                              | Description                                                                                                                                                                    |
|----------------------|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Admin Rights Removal | <b>Remove Admin Privilege</b>           | Remove administrator rights from selected users, groups, or account types across multiple computers in a single operation.                                                     |
|                      | <b>Local Group Management</b>           | Manage local group memberships and move users between local groups.                                                                                                            |
|                      | <b>Exclusion Lists</b>                  | Exclude specific users and groups from local administrator rights removal policies.                                                                                            |
|                      | <b>Continuous Monitoring</b>            | Detect new local administrator accounts and receive alerts when privileged group memberships change.                                                                           |
| Privilege Elevation  | <b>Policy-Based Privilege Elevation</b> | Define who can elevate which applications, and on which computers. Grant approved applications elevated privileges without requiring users to enter administrator credentials. |
|                      | <b>Elevation Request Workflows</b>      | Let users request elevation for applications outside existing policies, with designated or automated approval workflows.                                                       |
|                      | <b>Manage Request from Anywhere</b>     | Approve or reject requests using mobile app, web interface, or directly from your ticketing system.                                                                            |
|                      | <b>Temporary Administrator Access</b>   | Grant time-bound local administrator access and automatically revoke it when the approved period expires.                                                                      |
|                      | <b>Offline Access Codes</b>             | Enable single-use application elevation codes when endpoints are offline, with activity recorded for audit when connectivity is restored.                                      |
|                      | <b>Technician Access</b>                | Give technicians temporary administrator access to assigned endpoints using their own accounts, eliminating the need to expose domain administrator credentials.               |

| Function              | Capability                            | Description                                                                                                                               |
|-----------------------|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Privilege Elevation   | <b>Sudo Command Control</b>           | Control which SUDO commands standard users can execute on Linux and macOS based on command paths and parameters.                          |
|                       | <b>Script Execution Policies</b>      | Control which users can execute PowerShell, VBScript, and batch scripts with elevated privileges.                                         |
| Secure Remote Assist* | <b>Attended and Unattended Access</b> | Launch attended and unattended remote sessions to employee machines for troubleshooting, routine maintenance, and support tickets         |
|                       | <b>On-demand Support</b>              | Launch browser-based remote connections to any device instantly.                                                                          |
|                       | <b>Least Privilege Sessions</b>       | Administrators log in as standard users on remote endpoint by default with the option to elevate privileges only when required.           |
| Application Control   | <b>Application Control Policies</b>   | Allow approved applications and block all others, or block selected applications while permitting the rest.                               |
|                       | <b>Application Repository</b>         | Centrally manage approved executables, installers, management consoles, Control Panel items, and trusted folders for use across policies. |
|                       | <b>Application Access Workflows</b>   | Enable users to submit self-service requests for temporary access to restricted applications.                                             |
| Endpoint Controls     | <b>URL Blocklisting</b>               | Block access to specified websites using regex-based policies targeting URLs or addresses containing defined terms.                       |
|                       | <b>Browser Extension Control</b>      | Allow or block browser extensions by extension ID for selected users and groups.                                                          |
|                       | <b>USB Port Blocking</b>              | Disable or re-enable USB ports on managed endpoints to prevent unauthorized removable storage devices.                                    |

| Function             | Capability                         | Description                                                                                                                                                              |
|----------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Audit and Governance | <b>Activity and Access Reports</b> | Track logins, access requests, application elevations, policy changes, revoked privileges, and privileged group membership. Export reports in PDF, CSV, or XLSX formats. |
|                      | <b>Dual Approval Controls</b>      | Require secondary administrator approval for sensitive policy changes, technician access, application changes, and custom roles before they take effect.                 |

\*Secure Remote Assist is available as an add-on with separate license based on number of concurrent sessions.

## Architecture and Deployment

| Area                                         | Details                                                                                                                                                           |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Deployment Models</b>                     | SaaS, On-premises, private cloud                                                                                                                                  |
| <b>Server Operating System (for on-prem)</b> | Windows Server 2019 or later.                                                                                                                                     |
| <b>Installation Package (for on-prem)</b>    | Single binary installer with bundled components and database.                                                                                                     |
| <b>Backend Database (for on-prem)</b>        | PostgreSQL bundled by default; Microsoft SQL Server supported as an optional backend.                                                                             |
| <b>Database Selection (for on-prem)</b>      | Database choice is selected during installation; migration between databases can be handled with Securden support.                                                |
| <b>System Sizing</b>                         | Up to 1,000 endpoints: 4 cores, 16 GB RAM, 50 GB disk. 1,000–10,000 endpoints: 8 cores, 32 GB RAM, 100 GB disk. Above 10,000 endpoints: contact Securden support. |
| <b>Agent Deployment</b>                      | Supports individual and bulk installation methods through GPOs, Patch Management software like Intune, PDQ, etc.                                                  |

# Security Architecture: On-Premises vs SaaS

| Security Area                    | On-Premises Edition                                                                                                                                                                               | SaaS Edition                                                                                                                                                                    |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Operation Model</b>           | Dedicated central server connected to a backend database; server handles business logic, admins connect through a standard web browser, and users interact with the agent installed on endpoints. | Access-controlled, highly available Endpoint Privilege Manager instance hosted on AWS cloud with browser-based admin access. Users interact with agents installed on endpoints. |
| <b>Data Encryption</b>           | Sensitive data is encrypted at the application level using AES-256 before being stored in the database.                                                                                           | Customer data is encrypted using AES-256 and stored in segmented encrypted database storage.                                                                                    |
| <b>Encryption Key Management</b> | Each installation uses an automatically generated unique random installation key that must be kept separate from encrypted data and made available only during startup.                           | Each customer segment uses a unique encryption key stored through Amazon KMS with cryptographic operations handled in an AWS CloudHSM cluster.                                  |
| <b>Database Protection</b>       | Database accepts secure connections; localhost-only access by default and specific IP allow-listing for high-availability configurations.                                                         | Each customer's data is segregated and encrypted with a unique key so unauthorized access exposes only encrypted data.                                                          |
| <b>Data Integrity</b>            | Encrypted data cannot be deciphered without the installation key even if the database is compromised.                                                                                             | Encrypted customer data cannot be deciphered without the corresponding organization-specific key.                                                                               |

## Security Controls

| Security Control                 | Details                                                                                           |
|----------------------------------|---------------------------------------------------------------------------------------------------|
| <b>Credential Encryption</b>     | AES-256 encryption.                                                                               |
| <b>Encryption Key Management</b> | Per-installation encryption key stored separately from encrypted database; HSM support available. |
| <b>FIPS Mode</b>                 | FIPS-compliant mode available.                                                                    |

| Security Control                 | Details                                                                                                               |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Certificate Handling             | Self-signed certificate by default; CA-signed certificate installable.                                                |
| Certifications and Testing       | ISO/IEC 27001, SOC 2 Type II, GDPR alignment, and periodic third-party penetration testing.                           |
| Access Governance                | Granular RBAC, request-release workflows, emergency access controls, and just-in-time access.                         |
| Passwordless Privilege Elevation | Application elevation for users without requiring admin account passwords                                             |
| Auditability                     | Audit trails for privilege elevation, application execution, technician access sessions, and administrative activity. |

## Endpoint Privilege Manager Control Design

| Control Layer                  | Technical Detail                                                                                                                                                                                                                   |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Primary Authentication         | Admin console access can be controlled through LDAP-compliant directory services such as Active Directory and Microsoft Entra ID, SAML-based SSO, RADIUS authentication, smartcard authentication, or native local authentication. |
| Directory-Based Authentication | When directory authentication is used, EPM reconciles and authenticates through the configured directory and does not need to store directory user passwords.                                                                      |
| User Lifecycle                 | Directory integrations support user onboarding, offboarding, authentication, and access provisioning workflows.                                                                                                                    |
| Second Factor                  | Cloud and on-premises designs support MFA through any TOTP authenticator, Securden Authenticator, OTP through email, any RADIUS-based MFA, Duo, Yubikey, and others.                                                               |
| Access Policies                | Granular role-based access controls, request-release workflows, just-in-time access, and passwordless privilege elevation reduce admin credential exposure.                                                                        |

# Identity, MFA, and Integration Support

| Integration Area          | Supported Options                                                                                                                                                |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Primary Authentication    | Local accounts, Active Directory, Microsoft Entra ID, LDAP, and RADIUS.                                                                                          |
| SSO                       | SAML 2.0 support for Okta, Microsoft Entra ID, ADFS, OneLogin, PingIdentity, Google Workspace, and other SAML identity providers.                                |
| MFA                       | TOTP apps such as Google Authenticator and Microsoft Authenticator, Securden Authenticator, Duo Security, RSA SecurID, YubiKey, email OTP, and RADIUS-based MFA. |
| Smart Card Authentication | Supported for on-premises deployments.                                                                                                                           |
| RBAC                      | Predefined and custom roles for granular access control.                                                                                                         |
| Supported Browsers        | Chrome, Edge, Firefox, and Safari.                                                                                                                               |
| Client Applications       | Browser, Desktop application (Windows, Mac, Linux), and Mobile Application for iOS and Android devices                                                           |
| API Access                | REST API access with token-based authentication for computer management, policy governance, and general administration.                                          |

## Product Specifications Snapshot

| Specification             | Details                                                                                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supported Access Controls | Removal of local administrator rights, application control, on-demand elevation for standard users, temporary administrator rights, and least-privilege enforcement. |
| Enterprise Integrations   | Active Directory, Microsoft Entra ID, LDAP, Google Workspace, SAML SSO, SIEM, ticketing systems, MFA providers, SDKs, CLI access, and APIs.                          |

| Specification              | Details                                                                                                                                    |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MSP Support</b>         | Multi-tenant architecture for managed service providers, with data segregation and client-specific administration.                         |
| <b>Audit and Reporting</b> | Visibility into who has access to what, privileged activity tracking, password hygiene monitoring, access reports, and compliance support. |

## Scale and Resilience

| Resilience Area                 | Details                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>High Availability</b>        | Secondary application server with automatic failover; read-only replica on a separate subnet.                           |
| <b>Database Clustering</b>      | SQL clusters supported with Microsoft SQL Server backend.                                                               |
| <b>Disaster Recovery</b>        | Scheduled full database backup to remote destination; minimum hourly interval.                                          |
| <b>Offline Access</b>           | Cached policies govern privileged access on offline endpoints; Exception handling managed through offline access codes. |
| <b>Distributed Architecture</b> | Application servers and remote gateways deployable per network.                                                         |

## Commercial Notes

| Commercial Area                    | Details                                                           |
|------------------------------------|-------------------------------------------------------------------|
| <b>Licensing Model</b>             | Per endpoint managed through Securden Endpoint Privilege Manager. |
| <b>Secure Remote Assist</b>        | Included; Concurrent session licenses purchased separately.       |
| <b>Non-Production Environments</b> | No separate license required for test, staging, or DR instances.  |

| Commercial Area | Details                                           |
|-----------------|---------------------------------------------------|
| Support         | 24x5 standard support; 24x7 premium support.      |
| Upgrade Cadence | Minor monthly releases; major quarterly releases. |
| Free Trial      | 30 days; no credit card required.                 |

Compliance ISO/IEC 27001 · SOC 2 Type 2 · GDPR. Supports least privilege, application control, and audit requirements under PCI DSS, HIPAA, NIST, ISO 27001, GDPR, SOX, and NERC-CIP.

See how Securden can help your organization

Book a Demo