Securden

Endpoint Privilege Manager

Remove local admin rights on Windows servers and endpoints, elevate applications for standard users, whitelist trusted applications, enforce least privilege across the enterprise, and prevent malware propagation.

- Enforce Least Privilege
- Control Applications
- Prevent Malware Propagation

Inventory of Devices

Discover and create an inventory of endpoints and servers in your organization. Decide which devices require least privilege enforcement.

Local Admin Analysis

Identify and track the list of users and groups that are part of the local admin group on computers in the domain.

Applications Discovery

Automatically discover the applications that require administrator privileges across the enterprise. Consolidate and centrally track them.

Granular Application Control

Define and control which applications can be run by standard users. Whitelist trusted applications and prevent unapproved and malicious applications.

Policy-based Management

Centrally manage least privileges through control policies. Allow processes to be elevated on specific endpoints by specific users or groups.

Offline Scenarios

Ensure least privilege and application controls even when the endpoint is offline or away from the network or when users are working from home.

Remove Admin Privilege

Remove local administrator rights from users on Windows endpoints. Enforce least privilege without impacting operational efficiency.

Elevate Applications On-Demand

Empower standard users to seamlessly run approved applications (that would normally require admin rights) whenever needed. Elevate applications, not users.

Temporary Administrator Access

Grant time-limited, fully controlled, and comprehensively audited temporary administrator access to standard users on a need basis. Automatically revoke access.

Workflow Controls

Well-defined workflows with automation options to handle the lifecycle of all requests for approvals from end-users.

Application Elevation Trends

Track the trend of applications that are elevated by standard users over a period of time and detect unusual or suspicious activities.

Continuous Monitoring

Continuously monitor who all have administrator privileges. Detect if new local administrator accounts are added.

Technical Specifications

Product Installation	Windows Server 2019 (OR) Windows Server 2008 R2 and later
Deployment Model	On-prem, VMs (or) private cloud (AWS/Azure)
Web-interface	IE, Chrome, Safari, Edge, Firefox
Backend Database	PostgreSQL (bundled) or MS SQL server
Primary Authentication	Active Directory
MFA	Any TOTP authenticator (Google authenticator or Microsoft authenticator), any RADIUS-based authentication mechanism (RSA SecurID, Digipass, and others), Duo Security, Yubikey, Email to SMS gateway, and OTP through email
Data Encryption	AES-256
Data Transmission	SSL over HTTPS
Devices Discovery	Agentless

Admin Rights Removal	Agentless
Privilege Management, Application Control, and Temporary Admin Rights	Through a light-weight agent
Integrations	Active Directory, SIEM solutions
High Availability	Redundant servers pointing to the same database, MS SQL clusters
Disaster Recovery	Periodic database backup and recovery

Securden | support@securden.com | www.securden.com

Trusted by hundreds of SMBs and Enterprises across the globe

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