Securden

Best Practices for Enforcing Least Privilege

Expert Recommendations for Enterprises

Best Practices in Enforcing Least Privilege: Expert Recommendations for Enterprises

This guide is designed to break implementing the principle of least privilege into simpler, achievable, and less intimidating steps. By setting stepwise goals and providing guidance to achieve these goals, this guide will help you achieve the principle of least privilege in your own organization.

Summary of Steps:

Least Privilege Strategy

Before even touching the Securden Endpoint Privilege Manager, you need to define what you are looking to achieve by enforcing least privilege to determine where to focus first, and how to adopt the principle for implementing the principle of least privilege successfully.

Identifying Current Risk Profile

Goal: Estimating how exposed the organization is to privilege misuse and cyberattacks.

Run an audit to find out how many administrator accounts are in current use and their purpose. Most times, accounts accrue privileges and permissions due to obsolete requirements from the past. All permissions being delegated to accounts must be purposeful.

Ensure you include all non-human identities and service accounts in this audit. For service accounts, list the dependencies of each service account like services, processes, and app pools.

> **Pro Tip:**
> Discovering service accounts along with their dependencies can be painstaking without a dedicated solution. You may look at **Securden Unified PAM** for this.

Prioritizing High Risk Accounts

Goal: Ensuring a smooth large-scale adoption of least privilege by taking the 'Crawl-Walk-Run' framework.

Instead of going all in and removing admin rights across all endpoints, we must prioritize high impact accounts and target them first.

To begin with, identify the most sensitive accounts, like root users and domain admins. They have high privileges on multiple critical devices across the network and are highly sought after by threat actors. Secure them by rotating the password and storing them in a safe, encrypted location.

Once root users and domain admin accounts are secure, you must aim to secure sensitive non-human identities like service accounts. These accounts often carry very high privileges and are criminally overlooked. You must secure them by locking them inside a secure, encrypted vault and enforce periodic password rotation.

> **Pro Tip:**
> Periodic password rotation is prone to mistakes when done manually. Automating them with a dedicated solution is often more rewarding for organizations. You may explore **Securden Unified PAM** for combining credential management along with least privilege.

Defining 'Just Enough' Privilege

Goal: Identifying how much privilege/permission each team needs?

Privileges and permissions allow users to access data, run applications, make changes, and get their work done. While most users can make do with a standard user account, users often find themselves unable to do their task without the permissions and privileges associated with a local admin account.

Does this mean they should be working with an administrator account? The short answer is **No**. They should be given the minimum permission required to go about their jobs while keeping security at the back of the mind.

"Just Enough Privilege" is the minimum level of permission required by a user to the get a job done.

You must explore and find out what is just enough privilege for each functional unit in your organization.

> **Pro Tip:**
> Monitoring the activities performed by existing admin users will give you insights into use of admin rights in your organization. Running the Securden agent on learning mode will help in this regard.

Implementing Least Privilege Using Securden Endpoint Privilege Manager

Integrating With Directories

For efficient management of devices and users, it is highly recommended to integrate Securden with Microsoft Entra ID or Active Directory or both for hybrid deployments. Navigate to **Admin -> Integrations** for adding your domain to Securden.

Onboarding Endpoints

Goal: To efficiently identify and onboard endpoints that must be managed using Securden.

To manage privileges on endpoints, you must deploy the Securden agent. You can install the agent on endpoints using any of the following methods.

1. Direct installation on device
2. Bulk deployment through GPO or SCCM
3. Use MDM tools like Intune and PDQ
4. Create custom scripts

Once the agents are deployed, the computer will automatically be onboarded into Securden. Domain devices will be mapped automatically if the Active Directory or Entra ID domain is integrated.

> **Pro Tip:**
> It is recommended to import devices from Active Directory domains and Entra ID domains. While importing, you can import domain computer groups into Securden. Computer groups resemble the organizational structure and can be used for streamlining policy creation.

Onboarding and Managing Users

Once the agent is deployed on devices, the agent fetches the computers; the user accounts registered on each device. Apart from this list of user accounts, you must import the domain users from Active Directory and Entra ID. Domain user accounts are used in policy creation and onboarding them beforehand streamlines the process.

> **Pro Tip:**
> Import User Groups from domains to retain organizational structure. You can make use of this structure to create better policies; assign managers to approve/reject requests raised by their team members and reduce IT helpdesk burden.

After onboarding users, assign roles to the users based on their function inside Securden Endpoint Privilege Manager.

1. **Admin**: Users who are going to configure the Endpoint Privilege Manager, onboard users and computers, maintain the application repository, and create policies must be assigned this role.

> **Pro Tip:**
> Once you assign the **Admin** role to a user, you may go ahead and delete the built-in admin account that came pre-loaded into the product.

2. **Approver:** Users who are going to manage requests must be assigned this role. This helps delegate the burden of managing requests to designated approvers without granting them too many permissions within the EPM solution.

3. **Auditor:** This role must be assigned to users from the compliance team and people responsible for providing policy creation insights.

4. **User:** All users apart from the ones listed above must be assigned this user role. These users will predominantly interact using the Agent from their own endpoints.

> **Pro Tip:**
> You can also create custom roles with specific permissions. You can achieve separation of duties and separation of privileges using this method.

Managing the Application Repository

Once the agents are deployed on the computers, they start tracking which applications are run with admin rights on the endpoints. These apps are automatically added to the application repository in the Endpoint Privilege Manager. You can manually add applications that are used by teams in your organization too.

Securden supports different application types for Windows and macOS. You can add individual applications by providing attributes like file location, publisher name, etc.

> **Pro Tip:**
> Some users might need to modify the contents of a specific folder and edit configuration files. While these are not contemporary applications, these actions are allowed by adding the actions as applications to the repository. Open the **Application** page in the web interface, navigate to **Add -> Add Application** and click on the info icon next to the application type to explore these options.

Identifying Application Usage Trends

The Securden Agent can run in pure observation mode. Before creating policies or removing admin rights, it is recommended to run the agent in **Learning Mode**. The agent quietly collects data from the endpoints and provides you with insights on which users are running which application with admin rights.

Once sufficient data is gathered, you can plan how you want to create policies. Then move the Agent to **Operational Mode**. This will ensure the policies take effect soon after they are enforced.

> **Pro Tip:**
> Identify applications that are commonly used by specific teams instead of users. Use group-wise insights to map applications to the functional requirements of a specific team.

Automating Just-in-Time Privileges

With the application usage data, you now have clear insight on which applications are being run with admin rights by specific teams. You can create policies that are mapped to individual user groups that represent a functional team within the organization.

For example, you can create a policy that allows all designers to run Adobe applications with admin rights by mapping the policy with the user group that represents the designers.

> **Pro Tip:**
> When creating a policy, try to associate the policy with user groups rather than specific users. This way, if a new member joins a team, the permissions can be quickly provisioned by adding them to the respective domain group in Active Directory/Entra ID.

These policies ensure that the users have the permission to run specific apps with admin privileges even after their local admin rights are removed, thereby ensuring productivity.

Users can exercise policy-granted permissions by right-clicking on the applications and selecting **Run with Securden Privilege.**

Pro Tip:
Ask users to start using the **Run with Securden Privilege** option as soon as you create and enforce policies. This helps them get used to this procedure and allows you enough time to address requirements that are not covered by the policies.

Implementing and Optimizing Request-Release Workflow

Because you followed the Pro Tip to retain the organizational structure, the requests raised by team members will be managed by their managers. You can also manually assign designated approvers for each user/user group.

Pro Tip:

1. Allowing temporary full-admin access

You can grant temporary full admin access through the request-release workflow. Reserve this option only for rarest of the rare cases. For example, if a developer needs to install multiple applications, go ahead and grant them approval. However, for installing just one or two applications, you can ask the developer to raise a request for the installer file alone.

2. Automatic approvals for device owners.

You can enable automatic device owner discovery and assignment. Once owners are assigned to devices, you can choose to automatically grant approval to requests raised by the device owners. Navigate to **Admin -> Configurations** to do this.

3. Designated Approvers for Users

You can delegate the responsibility of managing requests raised by certain users/groups to specific approvers. This helps streamline the request-release workflow.

4. Leveraging ITSM Integration to Streamline Approval Workflow

You can integrate Securden EPM with your ticketing system. Once integrated, approvers can receive the requests directly in their ticketing system from where they can approve and reject the request.

Removing Standing Admin Rights

Once you have automated privilege elevation using policies and configured approval workflow for dynamically handling the requirements from standard users, you can safely remove admin rights from endpoints. It is recommended to perform this in a phased manner. Identify teams that rarely use admin rights and demote them first. Then move to the other teams.

> **Pro Tip:**
> Once you remove admin rights, monitor whether any repetitive request for elevating the same individual applications arise. Use the **Create Policy** button in the request approval page to add the application to an existing policy or create a new policy for this application.

Enforcing Application Control

While outside the scope of privilege management, Securden's allowlisting and blocklisting capabilities give you control over what applications each user or a user group can run on their endpoint. Permissions granted through allowlisting or blocklisting will not grant admin rights to users. The application will run with the permissions of the user account that is logged in.

> **Pro Tip:**
> Make use of the built-in application groups for creating allowlists. The groups have applications that are mapped to the common functional groups in an organization.

Least Privilege for Technicians

Helpdesk technicians and IT admins are often overlooked when organizations try to eliminate overprivileged local admin accounts. IT helpdesk admins and technicians use admin accounts on multiple endpoints for troubleshooting, installing and updating applications/software. This practice is not recommended as it increases the risk of credential theft leading to privilege misuse.

You can make use of the Technician access provisions in Securden to allow helpdesk users and administrators to login on employee machines using a standard user account to troubleshoot, install, and upgrade applications. The agent will recognize technicians and grant them elevated access when needed.

Navigate to **Admin -> Technician Access Policies** to explore this option.

> **Pro Tip:**
> You can granularly control which applications a specific technician can access/elevate on an employee's endpoint through technician access policies. This further reduces the threat surface.

Privilege Elevation for Offline Users

The agent will pull live data from the Securden server periodically when offline. However, when the device is no longer connected to the Server, the agent enforces the latest data it pulled from the Server. Users will not be able to raise requests with their approvers. To facilitate least privilege access in such scenarios, Securden provides offline access codes that allow users to elevate their privilege when offline.

> **Pro Tip:**
> You can control how users use the offline codes to elevate privileges. You can restrict users from using offline codes to gain temporary full-admin access. Navigate to **Admin -> Configurations** and search for offline access to find this option.

Continuous Operational Oversight

Securden provides ultimate visibility into how users are using their permissions and privileges. The various reports provided by Securden offer insights into what applications are being elevated by which users. You can make use of these insights to improve policies and demonstrate compliance with regulations.

Scheduling Periodic Reports

Set up scheduled tasks for automatically exporting reports every week/month. You have various reporting options to choose from. We recommend you review the **Applications vs. Number of Elevations in the last 30 days** report under **Concise Reports** without fail. The insights provided by this report help fine tune policies for least privilege.

Setting Up Alerts for Suspicious Activities

You can configure notifications whenever certain activities are detected. You must set up alerts for events that can have serious ramifications. For example, if a user tries to uninstall

the Securden agent or a command is executed with SUDO privileges, alerts must be triggered. Navigate to Admin -> Notifications to set this up.

> **Pro Tip:**
> You can choose who receives these alerts. You can designate specific users/auditors/administrators/managers to receive alerts based on the seriousness of the event.

Setting Up Centralized Privilege Management for Distributed Deployments

In very large enterprises, endpoints are often distributed across different locations. Securden supports distributed deployments through application servers. You can install the Securden server on the primary network and deploy application servers for all other locations. Ensure connectivity between the application server and the Securden server in the primary network, and you have centralized control over privileges on all endpoints in the organization.

> **Pro Tip:**
> You can maintain central oversight and delegate responsibility to administrators/approvers in the secondary network by using designated approvers in the approval workflow.

Setting Up Redundancy Measures

Redundancy measures help keep the operations running in case of unforeseen adversities. Securden supports high availability configurations and database backups for on-premises installations. For cloud edition, the redundancy measures are enforced from Securden's end.

High Availability

To ensure users can avail privilege management facilities at all times, you must make use of the high availability setup in Securden. You can configure secondary servers that automatically activate and become the primary server during a failover. Once the primary is back online, you can revert to the initial configuration.

Navigate to **Admin -> High Availability** to configure this redundancy measure.

Pro Tip:
You can make use of the high availability setup to configure load balancers as well. The secondary application servers will help handle large volumes of requests and database queries by distributing the load amongst themselves.

Backups

You can take backups of your database to safeguard configurations, policies, and application repositories among other data in rare scenarios where the server fails to work as intended. Once you take the backup, ensure you keep the copy at a secure location away from the server.

Pro Tip
When taking a backup, you must ensure that you take a backup of the encryption key. Without the encryption key, the backups cannot be decrypted.