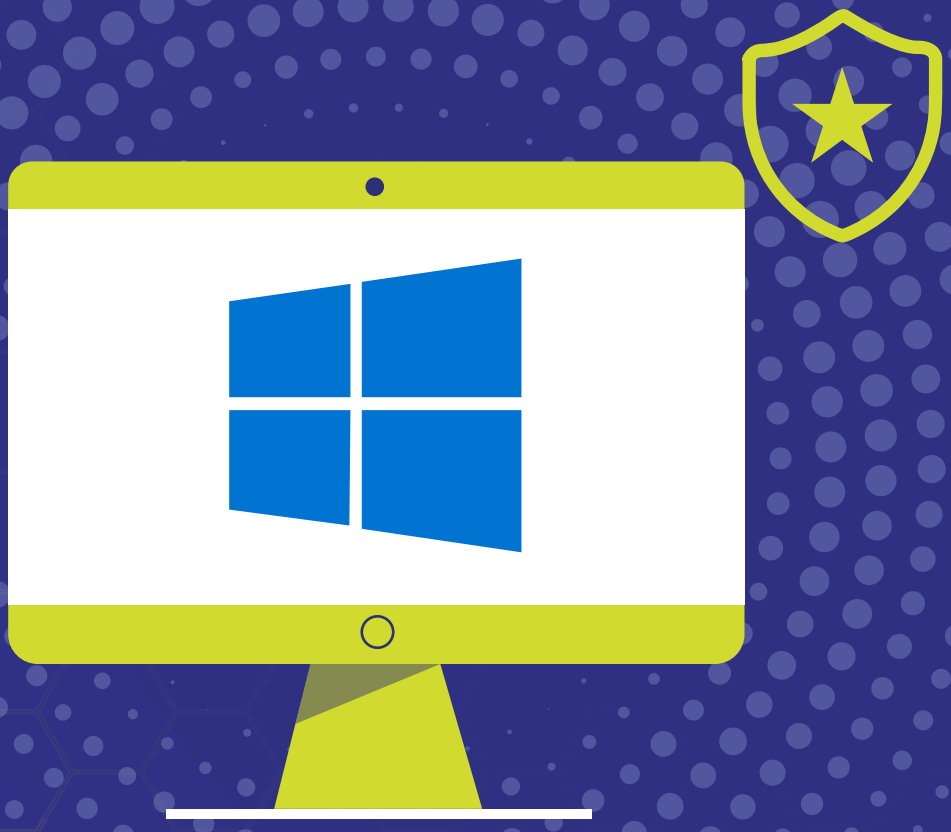
ManageEngine
PAM360

Your ultimate crib sheet to effective Windows privilege management



www.manageengine.com/pam360

Local admin rights: The key to Windows endpoints

An endpoint is essentially any device that serves as an entry point for a user to access the corporate network and its assets. From an IT security standpoint, every endpoint is considered a potential cybersecurity vulnerability. Organizations tend to assign local admin rights to employees company-wide in an attempt to reduce the workload of IT admins and expedite productivity.

Local admin privileges are essentially keys to endpoints. This bestows end users with full privileges to run applications of any kind or install any software on their devices, which, in turn, puts the entire organization's confidential data at risk. On top of this, decentralized admin access also results in poor visibility of the processes and applications running in the background, rendering the IT security team incapable of taking appropriate remedial action when privileges are abused.

On the other hand, removing local admin rights from endpoints increases the workforce's dependency on the IT team as employees go about their day-to-day activities, thereby increasing the workload for IT admins, and negatively impacting productivity overall.

For example, let's say a Windows developer working with Microsoft Visual Studio needs admin privileges to carry out their work efficiently. Removing admin rights from their device means they have to rely on IT to install dev-related extensions, drivers, and other resources that are required to carry out day-to-day tasks. Removing admin privileges also heavily impacts users who need access to various system tasks, processes, and applications—requiring the intervention of IT to successfully complete all such activities.

What is privilege management?

Endpoint privilege management is a cybersecurity approach that focuses on providing an effective immune defense to all user devices across the organization, which typically act as entry points for attackers to access a company's sensitive assets. Restricting and managing user and application privileges at the device level has become all the more

important in the current age of remote work where the traditional network perimeters are shattered, and boundaries are defined by user identities and data flow.

Gartner analyst Lori Robinson clearly defines endpoint privilege management as:

> **Endpoint privilege management (EPM) technologies combine application control and user privilege management to ensure that only trusted applications run, and that they run with the lowest possible privilege. With EPM, organizations can remove local admin access with minimal impact on end users.**

In other words, endpoint privilege management is the process of reducing risks of privilege abuse by removing local admin rights on endpoints and enforcing the principle of least privilege across on user and application permissions. This creates an environment where users are given just the privileges they need to access a particular trusted application and for a specified amount of time required to carry out the task. IT teams exert this control via on-demand privilege elevation and granular application control.

Addressing privileges at the application and process level rather than at the user level offers more tailored control, and with local admin rights revoked, users won't be able to install, access, and run applications unless the applications are used for their roles. By incorporating the right strategies and solutions, companies can ensure productivity is not hampered because of access restrictions without providing local admin rights or excessive privileges to users.

[Privilege management + application control] – local admin rights = Endpoint privilege management

Steps for effective Windows privilege management

Now that we have an understanding of endpoint privilege management and why enterprises need it, let's delve into how organizations can go about deploying endpoint privilege management for their Windows ecosystem.

Listed below are some quick steps organizations can follow to devise and incorporate effective privilege management across their Windows systems:

1. Discover and create an inventory of endpoints

The first step to enforce Windows privilege management is to discover and isolate the endpoints in the network that need least privilege enforcement. Once an inventory of devices is created, it's much easier to create user privilege elevation policies and enforce application control across the necessary endpoints.

2. Remove local admin rights across endpoints

Local admin accounts are non-personal accounts that provide administrative access to the respective local host. Abuse of administrative privileges is a popular technique used by cybercriminals to gain access to mission-critical systems within a network. Removing local admin rights on endpoints and replacing them with standard user accounts deprives users of privileges to install and run applications that affect the security of their local machine, thereby reducing opportunities for attackers to infiltrate the network.

3. Assign granular application control

After creating an endpoint inventory and removing local admin privileges, identify and isolate applications within the ecosystem that require admin privileges. Assign granular privileges to individual applications, including full admin rights. Block access to unauthorized applications, particularly malicious ones, using trust-based application whitelisting. Elevating whitelisted applications on-demand allows standard users to access to the applications when they need to without requiring administrator credentials.

4. Adopt a policy-driven approach to enforce least privilege

Enforce least privilege centrally by defining policies for application control. Create granular policies to define what operations users can perform under what circumstances. Policies help you contextually evaluate access requests to specific applications and elevate applications accordingly. This way, you can assure least privilege access across applications without negatively impacting employee productivity.

5. Grant just-in-time (JIT) administrator access

For applications that absolutely need admin privileges to run, grant time-limited temporary admin access to standard users by elevating their privileges on specific endpoints or across the domain. This can be done by adding the users to the devices' local group and/or to selected AD security groups.

The just-in-time (JIT) privileged access can either be granted on demand or automated via policies. Comprehensively audit the sessions running with elevated access by incorporating appropriate controls for session monitoring and shadowing. This helps standard users seamlessly gain access to applications and processes for only the amount of time required and under complete supervision with no need for administrator credentials.

6. Manage non-domain endpoints

Apart from controlling user access to applications within the corporate network, the principle of least privilege also needs to be applied to third-party user devices such as partner, vendor, and contractor devices facilitating access to sensitive corporate data. This can be done by deploying agents on the devices. Agents help administrators monitor and control privileges with the same dexterity and precision as those mapped within the corporate domain. Effective management of non-domain endpoints is crucial to prevent accumulation of unnecessary privileges and thwart unauthorized access.

7. Privilege monitoring

Continuously monitor and audit executable events on all managed endpoints via a centralized tool so that the logs can be searched, reviewed, and analyzed from a single console for better correlation. A unified reporting dashboard is particularly helpful to get an at-a-glance view of the status of the endpoints, important activity logs, and data, which can be further drilled down to get more information. Furthermore, agent activity from non-domain endpoints needs to be continuously tracked to detect any anomalous user activity.

8. Risk detection and analytics

Incorporate ML- and AI-driven behavioral analytics to detect anomalies in user activity to stay on top of privilege escalation attacks. Calculate and assign a threat score to individual users every time privileges are elevated, so potentially malicious users can be tracked and appropriate remedial actions can be taken quickly.

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360