Local admin rights: removing the threat

THE CHALLENGE

Security threats

- Proliferation of administrator accounts on end-users' workstations and laptops poses a significant security risk at many organisations
- These accounts can be used by attackers to install malware or open back doors for uncontrolled access at a future time
- Removing these accounts is a common goal, but usually means an increased load on the IT help desk dealing with requests to install software or make configuration changes
- With PEM, IT can remove local administrator accounts without increasing requests to the help desk

THE SOLUTION

Privileged Endpoint Management (PEM)

It enables organisations to:

- remove local administrator rights from users
- provide users with escalated privileges only for specific processes and executables or for a specific time frame
- increase its security posture, while tipping the balance towards productivity

Key features

Simple to deploy

Reassuringly easy, lightweight and quick to deploy, it won't sap your time. Will run in the background with minimal effort required and complementary to other tools. For organisations using Azure, PEM can be deployed directly from the Azure Marketplace.

100% native Azure AD support

Supports workstations managed by Azure Active Directory (AD), ensuring the solution and the business is future-proofed.

On-premise AD or hybrid

Also supports on-premise, or hybrid Azure AD for those businesses making the transition to the 'modern desktop'.

Temporary admin rights

Boost productivity by providing users with an elevated session on their endpoint for a set period of time, via a request response system or by granting users ability for self-approval. Can also be carried out offline if internet access is unavailable.

Role-based access control

Assign policies on premise to Active Directory groups or Azure AD groups to avoid defining policies for individual users.

Centralised policy management

Manage applications by policy to avoid repeating configurations for each user.

Intuitive end-user experience

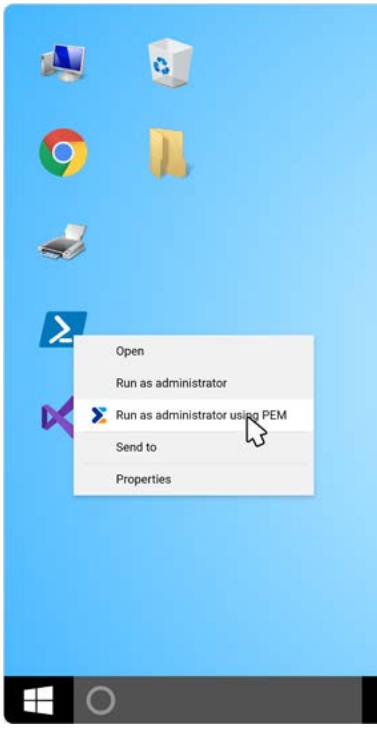
Users run permitted applications using the "run as Administrator using PEM" - just as they would with any privileged application.

User and admin audit trail

A full audit trail of admin operations and user activity is maintained for compliance.

Monitor elevated processes

Record all applications and processes running with elevated privileges.



Benefits

Enhance security

Remove local admin rights and enforce least privilege. Elevate only approved applications, not users.

Reduce workload

Cut down on the burden on your help desk staff by reducing messages with admin-related requests.

Reduce risk

Remove risky local admin rights from users to reduce the attack surface of your IT estate.

Boost productivity

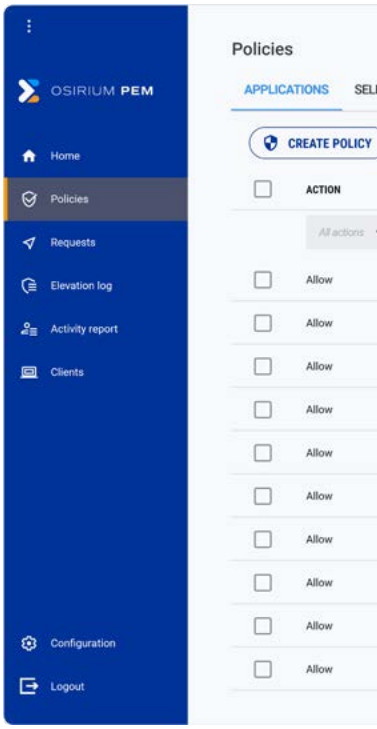
Become more productive, not less, despite the elevated level of security.

Simplify IT operations

Give end users a fast and easy way to get elevated privileges only when they need them.

Enforce governance

Review policies and monitor user activity regularly to prove compliance with the least privilege model.



Osirium Privileged Access Security

Osirium PEM is a part of Osirium Privileged Access Security – the comprehensive solution for secure privilege management and process automation.

Privileged Access Management (PAM)

Isolate users from privileged account credentials and securely manage privileged sessions.

Privileged Endpoint Management (PEM)

Remove administrator rights from endpoints for least privilege compliance without impacting productivity.

Privileged Process Automation (PPA)

Automate cross-system processes to delegate administrator tasks to help desks and users.