PEM

Privileged Endpoint Manager

Enforce "least privilege" policies while enabling productivity

Introduction

Enforcing "least privilege" – removing local administrator accounts from user devices – is a key element in any cybersecurity policy. However, that can mean users don't have access to the applications or resources they need to get their work done without a call to the IT helpdesk. The balance between security and productivity gets tipped towards security at the cost of productivity.

Osirium's Privileged Endpoint Management (PEM) allows organisations to remove local admin rights from users, at the same time enabling the same users to have escalated privileges only for specific processes and executables. The balance tips back towards productivity while increasing the organisation's security posture.

Benefits

Enforce "Least Privilege"

End-users only need user-level accounts.

- No local admin accounts
- Whitelisted applications can be run with elevated privilege

Run Privileged Applications

Approved applications can be run with elevated permissions without contacting IT.

- Permissive mode monitors application usage
- IT defines policies based on actual usage

Show Compliance

Track which privileged applications are used, by who and when

- Audit trail of authorisations and usage to show policy compliance
- Elevated applications are always run in the context of the real user for audit trails

Reduce Help Desk Load

Reduce the need for users to call the IT help desk to run privileged applications.

- Define and deploy policies to allow users to run approved applications as Administrator without contacting the help desk

Manage Permissions

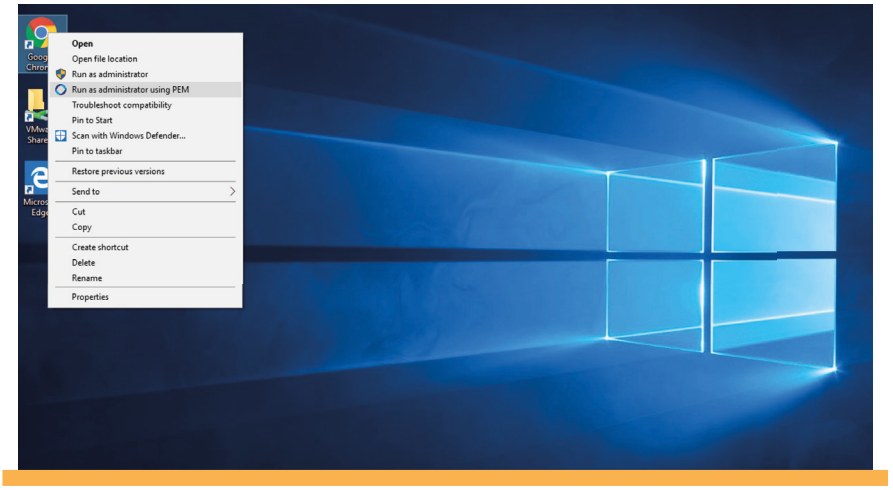
Permissions can be granted at multiple levels to improve control and reduce IT effort.

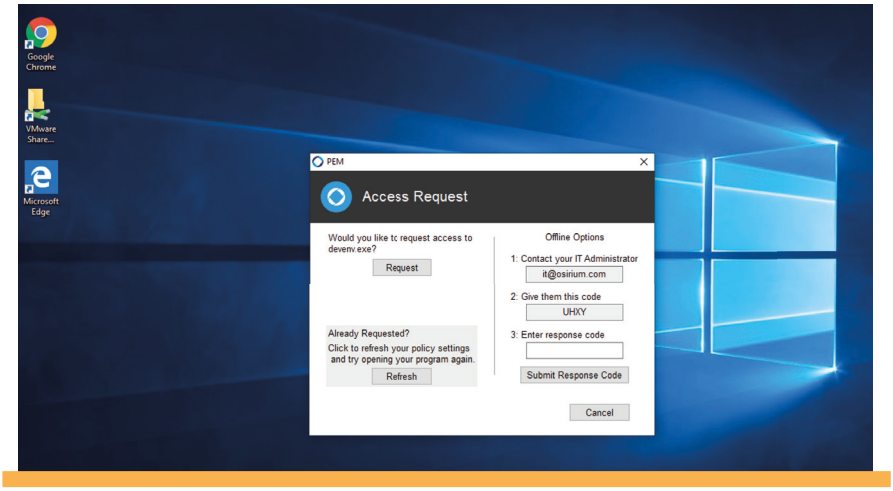
- Define permissions at the user or group level
- Allow access for specific time periods – one-time or forever

Keep Mobile Workers Productive

Mobile workers can request elevated privilege as needed.

- Offline workflow for remote authorisation.
- Ideal for the remote user that needs access to a local device or Wi-Fi





Osirium PEM is a natural extension to the Windows desktop.

Accessed from the application icon context menu, the user requests permission to execute as an Administrator. For whitelisted applications, the application starts with elevated privileges. For new applications, the request is routed to IT, reviewed and, if approved, a policy is deployed to enable access.

Osirium Opus
Privileged Process Automation
Secure and automate key IT processes

Osirium PXM
Privileged Access Management
Protect remote devices and services

Secure
Automate
Audit

Osirium PEM
Privileged Endpoint Management
Manage endpoint privileged applications

The Osirium Privileged Access Management Portfolio

PEM is a part of Osirium's unified Privileged Access Management portfolio protecting valuable corporate devices, services and applications and secure IT Process Automation.

About Osirium

Osirium Technologies plc (AIM: OSI.L) is a leading vendor of Privileged Access Management ("PAM") and Privileged IT Process Automation ("PPA") software. Osirium's cloud-based products protect critical IT assets, infrastructure, and devices through automation and by preventing targeted cyber-attacks from directly accessing Privileged Accounts, removing unnecessary access and powers of Privileged Account users.