PEM PLATFORM

Overview of Privileged Endpoint Management

OSIRIUM

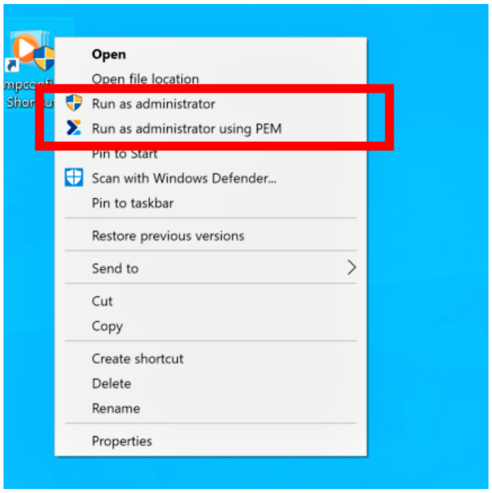
Privileged Endpoint Management

An Overview

A significant security risk at many organisations is the proliferation of administrator accounts on end-user's workstations and laptops. These accounts can be used by attackers to install malware or open backdoors 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 Privileged Endpoint Management (PEM), IT can remove local administrator accounts without increasing requests to the help desk.

Elevate Applications Not Users



PEM allows IT administrators to create policies (stored in Microsoft Active Directory as Group Policy Objects (GPOs)) determining which applications can be run with elevated privileges. For the end-user, they run the approved applications using the "Run as Administrator using PEM" option from the application's context menu, just as they would previously.

The user is then presented the Windows User Account Control (UAC) prompt where they enter their own credentials to confirm they want to run a process as an administrator, assuming the policy you've established allows them to do so.

User context is maintained while privilege is elevated. As a result, any files created will be owned by the user's account and any 'save' or 'open' dialog will default to the user's standard locations. This produces a seamless experience for users to elevate privileges on demand.

Building Approved Application Policies

GPOs enabling elevation of privilege are built automatically or manually.

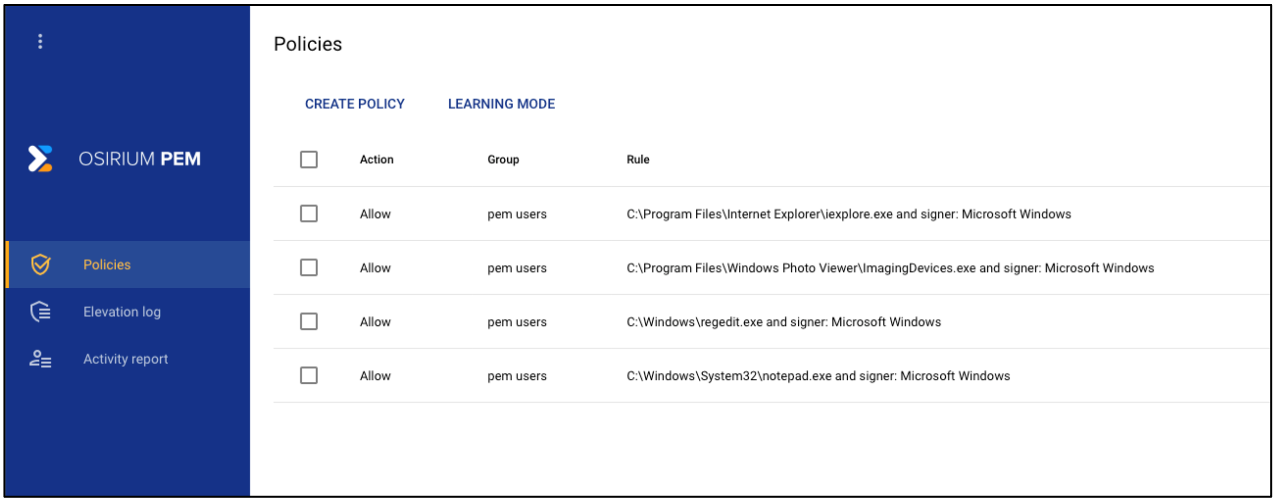
Automatic Policy Creation

The simplest method of deploying PEM is to run in “Learning Mode” to detect which applications user’s need before enforcing the policies. PEM tracks the applications being used and IT Administrators can specify exactly which version is allowed based on software publisher, file size and file footprint to ensure not only the correct versions are used, but also that the application files have not been corrupted by malware.

Using Learning Mode, most applications that users will need will have been pre-approved reducing calls to the help desk when PEM is switched to “Enforce” mode to prevent execution of unapproved applications.

Manual Policy Creation

Alternatively, Administrators can define the specific applications and versions that will be allowed though the PEM Administration console.



□	Action	Group	Rule
□	Allow	pem users	C:\Program Files\Internet Explorer\iexplore.exe and signer: Microsoft Windows
□	Allow	pem users	C:\Program Files\Windows Photo Viewer\ImagingDevices.exe and signer: Microsoft Windows
□	Allow	pem users	C:\Windows\regedit.exe and signer: Microsoft Windows
□	Allow	pem users	C:\Windows\System32\notepad.exe and signer: Microsoft Windows

PEM Capabilities

- With PEM, you can manage users’ privileged access to executables and processes via policies within the PEM server interface.

- Policies enable you to fine-tune exactly which processes users may elevate on an endpoint (i.e. run a process as administrator). You can set a policy as either Allow or Deny, and define each policy by one or more attribute (filepath, signer, hash)
- Create policies one at a time manually or use Learning Mode to automatically create 'Allow' polices based on user activity.
- You may want to explicitly deny a process, such as blocking a single version of an allowed elevation. You may do this by creating a 'Deny' policy specifying the executable's hash. A 'Deny' policy will take precedence.
- Policies are applied to groups of users at the AD user group level.
- Individual end users will have an effective policy set based on their AD group membership.
- Enforce compliance and audit trails: ensure only verified applications are used and full audit trail of escalations is maintained.

Osirium Privileged Access Security

Privileged Endpoint Management is a component of Osirium's Privileged Access Security solution that also includes:

Privileged Access Management – PxM Platform

Modern, easy to deploy management of privileged access to shared devices, services and systems that includes session recording, behavioural analytics and rich audit controls.

Privileged Process Automation – PPA

IT Operations teams are overloaded with user requests, but traditional automation and RPA tools aren't appropriate. PPA securely automates IT processes to enable "shift-left" delegation of tasks.

About Osirium

Osirium is the UK's innovator in Privileged Access Management. Founded in 2008 and with its HQ in the UK, near Reading, Osirium's management team has been helping thousands of organizations over the past 25 years protect and transform their IT security services.

The Osirium team have intelligently combined the latest generation of Cyber-Security and Automation technology to create the world's first, built-for-purpose, Privileged Protection and Task Automation solution.

Tried and tested by some of the world's biggest brands and public-sector bodies, Osirium helps organizations drive down Business Risks, Operational Costs and meet IT Compliance.