Privilege without the risk from local admin rights

Endpoint Privilege Management

Radically reduce the risk of ransomware attacks while remaining productive

The Challenge

- Too many users have access to powerful administrator rights on their laptops and desktops.
- This exposes a business to major cyber threats, such as ransomware attacks.
- Removing local admin rights reduces the risk of security breaches but causes extra workload for IT and frustrates users.

The Solution

- Remove access to local admin rights while still allowing approved applications and sessions to run with elevated privileges.
- Create and manage policies for easy management of large user communities.
- Monitoring and reporting of elevated sessions.

Benefits

Enhance security

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

Reduce risk

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

Simplify IT operations

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

Reduce workload

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

Boost productivity

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

Enforce governance

Review policies and monitor user activity regularly to prove

Key Capabilities

Simple deployment

Endpoint client is distributed via existing tools, end users run with elevated privileges as before, access is managed via policies, and learning mode makes it easy to create initial rules to get protection as quickly as possible.

Native Azure AD, on-premises AD, or Hybrid

Manage your Windows endpoints in the way that best suits your IT estate and be ready for any move to new technologies such as Azure AD (Entra ID)

Role-based elevation policies

Assign policies on premises 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 applications with elevated privileges using the “Run as administrator with EPM” option.

Online or offline working

Even when not connected to the corporate network, users can elevate permissions on applications and sessions. Azure AD (Entra ID)

Elevate entire Windows sessions

For complete flexibility, the most trusted users can elevate permissions for their entire Windows session for a limited period, even without having to contact IT first.

Monitor elevated sessions

Record all applications and sessions run with elevated privileges, including attempts to elevate non-approved applications.

How endpoint management solutions compare

Capability	Osirium EPM	Leading EPM competitor
Supports Windows 10 and 11	✓	✓
Offers Admin UI	✓	✓
Low cost per user	✓	✗
No extra cost for ongoing technical support	✓	✗
Simple licencing	✓	✗
Rapid to set up and deploy	✓	✗
Easy to manage and maintain	✓	✗
Machine learning to ease deployment	✓	✗
Time-window temporary elevation	✓	✗
Self-Approval mode	✓	✗
Offline access	✓	✗
Supports on-premise Active Directory	✓	✗
Supports a zero trust environment	✓	✓
Lets standard user complete tasks that require elevated privileges	✓	✓

Endpoint management dashboard

IT leaders have visibility into the protection status of Windows endpoints. They have visibility into which applications are being elevated and which have been attempted even if not approved.

Ideal information to show auditors when reporting on cyber security policies

> *EPM is securing my device without me thinking I am losing all my privileges, it's the catch all.*

Endpoint management

Elevation rules are distributed via policies, making it easy to manage even for large estates of Windows endpoints.

The lightweight EPM agent on endpoints can work offline but will collect latest policies and update to latest versions whenever connected.