Privilege Management assigns privileges to applications, not users, allowing you to successfully remove admin rights and protect the operating system. With this flexible approach, individuals can still access the documents, tasks and scripts they need to perform their job roles so that they can be productive without security compromise.

- **Eliminate admin rights**
- **Assign privileges directly to applications**
- **Protect the endpoint from insider threats**

### Technical benefits:

#### Targeted assignment of privileges

Precision targeting rules mean that admin rights can be assigned securely to individual applications, rather than users, so that all users are able to successfully operate with standard user accounts. Every user is granted just the right level of access to suit their specific job role, providing a seamless transition to least privilege.

#### Broad application support

With support for a broad set of application types, Privilege Management adds the flexibility to cater for the needs of all users, and all privileged tasks. Whether it's an application, installation, script or COM task, Defendpoint handles all your diverse user requirements.

#### Works seamlessly with User Account Control

Replace unwanted prompts and specifically target applications that trigger Windows UAC messages. By intercepting and monitoring all exceptions, you can refine policies and provide users with quick and simple ways to request the access they need.

#### Layers of in-built security for added protection

Prevent the creation of rogue admin accounts, with unique privileged account protection. Patented anti-tamper ensures Defendpoint cannot be circumvented, as well as in-built protection against code injection, shatter attacks and token hijacks. The option to digitally sign policies ensures their authenticity on the endpoint.

#### On-demand access to privileges

Grant the ability to elevate applications on-demand, with gated controls such as justifications and password verification. Ensure that even advanced users such as sysadmins have the ability to perform their specific roles without compromising security.

#### Simple to use and manage

Wizard-based workstyles and templates make it faster to get started. A flexible filter engine with targeted control means you can map policies to specific job roles, even developers and sysadmins in the data center. Simple configuration with clear process flows means less clutter and better visibility, keeping it manageable across thousands of users.

#### Clear, customizable messaging

You can create an unlimited number of highly personalized messages for managing exceptions that fall outside standard corporate policies. Depending on the level of control you apply, the user can self-approve access with full audit trails, or request a response code from your IT desk. Prompts can be integrated with helpdesk ticketing systems for ease of use.

#### Seamless integration with Application Control

By combining Application Control with Privilege Management, your corporate applications can be safely elevated without the use of admin rights. System files and folders are automatically protected and therefore can be whitelisted easily. This allows you to focus on unknown or user applications, greatly reducing complexity. A single policy engine across all three Defendpoint modules means there's no risk of conflict.
**Actionable intelligence via advanced reports**
Easily identify privileged users and activity with usable data that enables you to keep admin rights to a minimum. Graphical dashboards and reports with drill-down options provide fast access to as much detail as you need. Reports are built on familiar and trusted SQL Server and SQL Reporting Services, which are fully integrated across all three Defendpoint modules.

**Supported platforms**
- Windows XP
- Windows Vista
- Windows 7
- Windows 8 / 8.1
- Windows Server 2003
- Windows Server 2008 / 2008 R2
- Windows Server 2012 / 2012 R2

32-bit and 64-bit versions are available for all supported platforms.

**Technical features at-a-glance:**
- **UAC targeting and replacement**
  Supress or replace the standard Windows prompts with your own customized messaging with prompts and notifications.
- **Flexible workstyle approach**
  Map privilege management policies to specific roles and groups, depending on individual requirements.
- **Highly customized messaging**
  Fully configurable, branded messages with multi-lingual support and reusable templates.
- **On demand access**
  Empower users with justification and password verification, with the option of ‘Run As’ replacement and on-demand elevation.
- **Advanced exception handling**
  Challenge and response codes allow you to manage access requests, specific to users, apps or machine with optional helpdesk ticket integration.
- **Robust security**
  Built-in anti-tamper mechanisms with privileged account and process protection, policy certification and content validation.
- **Unique privilege monitoring**
  Identify all applications that need admin rights with unique reasons and insight.
- **Patented URL control**
  Ability to track downloads and control privileges based on source and origin.
- **Advanced capabilities for sysadmins**
  Extend protection to the data center with control over services and drivers, targeting of individual management tools and scripts.
- **Auditable reason and request fields**
  Ensure compliance with two-factor authentication.
- **Remote PowerShell management**
  Grant sysadmins the ability to remote manage desktops and servers through PowerShell, without the need for local admin accounts.

---

**About Defendpoint**
Avecto’s proactive endpoint security software, Defendpoint, uniquely combines the technologies of Privilege Management, Application Control and Sandboxing to protect the operating system, software environment and corporate data from unknown cyber threats.