Heimdal®

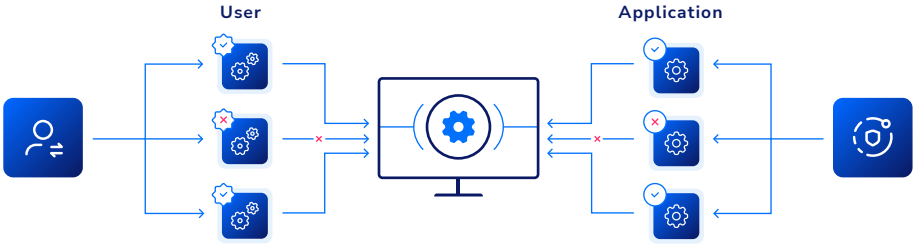
Privilege Elevation and Delegation Management & Application Control

Solution Brief

The Privileges and Application Control line of products is an innovative module offered by Heimdal

Remove permanent rights, give access to temporary elevation and application execution, when users need it – and be NIST AC-1,6 compliant.

Protect your network and endpoints with a revolutionary approach to both PAM and Application Control.



Heimdal Privileged Access Management and Application Control

The Privileges and Application Control line-up effectively secures the three major areas of your IT access infrastructure, ensuring everything works smoothly and threats are kept away: Management of privileges, App control and Auditing.

The auditing functionality is granular and essential for data protection compliance, supporting a full audit trail of Allowed Executions, Blocked Executions and Passive Mode monitored executions, with a 90-day retention for all logs.

Management features:

- Allow or Block requests for escalations in one click;
- Easy to enable Passive Mode for system indexing;
- Easy to enable Auto-approval flow with rules defined and automatic de-escalation on threat;
- Rule based system easy to control and define by the admin(s);
- Define individual rights per AD group.
- Allow or Block execution of apps based on File Path, MD5, Publisher, Certificate or Software Name criteria;
- Ability to use the historic executions history for all future Allow and Block decisions;
- See what users have executed applications in Passive, Allowed or Blocked mode;
- Filter your views of the logs as you wish, by user, by apps requested and so on;
- 90 Days Data retention for all logs.

Our Privileged Access Management and Application Control is the world's only bundled product which offers both functionalities. The line-up proactively secures your entire environment, ensuring compliance, transparency and boosted productivity for all users and admins.

65% **FINANCIAL DAMAGE**

65% of the damages caused by insider threat to an organization are both financial and reputational.

$11 **MILLION IN DAMAGE COST**

$11,45 million was the average cost of a breach caused by insider threat in 2020.

88% **OF ORGANIZATIONS**

88% of organizations surveyed said that insider threat is a cause for alarm.

40% **OF ORGANIZATIONS**

40% of organizations surveyed feel vulnerable to having confidential business information exposed through insider threat.

* ENISA Report for Insider Threat in 2020

Insider threat is one of the most insidious and difficult to control threats to an organization's cybersecurity. Even if most of the time it's not a malicious, intentional threat, it can still lead to exposure of a company's delicate data, financial assets, or, worse, it can lead to cybercriminal getting a foothold in your organization.

Controlling and restricting what applications can be run or accessed and by whom is an essential step into neutralizing insider threat.

With the new Application Control, you ensure compliance, secure your organization against dangerous access requests, liberate time for your admins and increase productivity, minimizing your administrative costs.

Heimdal®

Privilege Elevation and Delegation Management & Application Control

Secures against intentional or non-intentional insider threat

Insider threat and system infiltration by external attackers are a growing threat for organizations of all sizes.

The Zero Trust Principle and limiting admin rights across IT infrastructures have become the only avenue for safety, but without a professional PAM tool, this can create more work and wasted time. Application control also emerges as a crucial component of a healthy security setup.

Step into the future of access management and application control with Heimdal

Cybercriminals won't stop exploiting the existing security holes in your IT network. User accounts can be a major gateway for criminals. Stay one step ahead of them with Application Control and Privileged Access Management!

Privileges & Application Control	
Privileged Access Management	**Application Control**
Easy escalation of rights and files	Includes the ability to White and Blacklist any execution
Full control of the escalation process	Easy control of access to execution of files
World's only de-escalation on threats	Ability to easily manage spawns of any files executed
Auto-approval mode to avoid user support time	World's only Application Control that can be tied with PAM
Mobile approval supported	Handle access by File Path, MD5, Publisher, Certificate or Software Name
Full Audit Trail	Full Audit Trail
Removes 93% of Microsoft vulnerabilities in Windows OS and 100% in Microsoft Browsers	Passive mode for system indexing
Individual rights per group (NIST AC-5 compliance)	Default approval for system applications
Option to remove existing admin rights (NIST AC-1,6 compliance)	Option to remove existing rights and give access to application execution (NIST-6)
Beautiful unified overview and data visualization	Beautiful unified overview and data visualization

When having both the Privileged Access Management and the Application Control components active, they will further enhance each other:

- Define lists of apps which can be accessed only during elevated rights sessions
- Allow access to restricted applications during elevated sessions
- Restrict access to some applications even when user rights are elevated
- Allow access to running certain apps without full elevation necessary

Manage, audit and comply in one easy step with Application Control:

- Easy implementation and configuring.
- Infinitely customizable: Set filters, white and black lists, passive mode as defined by admin, Group Rules and more.
- Benefit from a full audit trail, with data logs stored 90 days.
- See exactly what users executed which applications.
- Be NIST AC-6 compliant in one easy step, just by using the solution.
- Further improve your security with complementary modules, all unified in one agent and dashboard.
- Best protection to investment ratio.

You can benefit from our Application Control as a standalone module, or in conjunction with the Privileged Access Management module, in one unified and cross-functional suite.

- Subscription model, no initial investment needed.
- Continuous updates with no administration or maintenance.
- Unified agent and dashboard with the complementary module,Privileged Access Management.
- A solid security basis for your cybersecurity, upon which you can keep building and scaling according to your organization's needs, in a single dashboard.

Heimdal®

Privilege Elevation and Delegation Management & Application Control

Privileged Access Management and Application Control

Heimdal offers the world's only option to run either or combine Privilege Access Management and Application Control.

Your suite can be further expanded with cross-functional modules, strengthening the intelligence in the Privileges and Application Control and the other EPDR components, and unlocking new functional perks with each further module added.

Add and expand your cybersecurity with customizable modules, all in a single interface and dashboard, fed by unparalleled intelligence.

- Boost productivity and free up resources.
- Beautiful and unified data visualization.
- Don't lose your revenue, intellectual property, and productivity.
- Significantly raise your overall security.
- Minimize your costs.
- Protect your infrastructure.

Heimdal's PEDM (Privilege Elevation and Delegation Management) Approach

Privileged Access Management by Heimdal supports PEDM-type non-privileged user account curation features for AD (Active Directory), Azure AD, or hybrid setups. Curation of lower-privileges accounts befalls on individuals from the IT administration team, empowered by non-exclusive administrative rights (i.e., person or persons fulfilling an administrative role in an RBAC setup can only exercise specific functions within the allotted group policies, thus eliminating over-privileged accounts).

By default, all administrator-type roles that haven't been approved either by company charter or internal Role-based Access Control rules will be reverted to simple user, defined as follows:

- Required reason on elevation.
- Prevent spawning of processes on session end.
- Denied elevation of system files. Exempted are those required to perform actions formulated in the "Reason for elevation request".
- No batch or command scripting. User will not be able to run OS-specific or custom batch or CMD scripts.
- Sub-class affiliation. User can be included in non-privileged sub-groups, an AD or Azure-defined group policy that prevents certain users from requesting and obtaining elevated privileges. This sub-class can be spawned within existing group policies. Sysadmins can also enforce special non-privileged policies, with global enforcement applicability.

Local Admin Rights Elevation

User clustering for the purpose of further curbing L.A.R.E. (Local Admin Rights Elevation) is available and can be enforced by using the "Map users to group" feature under UTD's Group Settings section.

This added granularity will allow members of specific Local Users and Groups to request elevations. Inclusions or exclusions are case sensitive and must be inputted manually. Sysadmins can include or exclude users based on hostname and username.

Under PEDM, Privileged Asset Management allows for the retention of administrative permission for specific users and/or domains groups that can be traced back to specific endpoints or groups.

TIL (Time-to-Live) feature acts as JIT (Just-in-Time) gatekeeper, restricting the access of users and administrators to L.A.R.E.-based activities. If properly configured, the user will be able to request single-file or process elevation only within working hours.

By default, the elevation token will expire within 24 hours if not confirmed by the user. De-elevation behavior can be changed by using the "Enforce token refresh" feature. If enabled globally, the user will automatically be logged off and the processes killed.

The Reporting mode is default enabled; for consistent telemetry, we recommend that you leave it on for at least 2 weeks to monitor the allow and block patterns and whitelist all the blocked processes that you consider necessary, before enabling the full functionality.