Heimdal®

PRIVILEGED ACCESS MANAGEMENT

Heimdal Privilege Elevation and Delegation Management (PEDM) & Application Control (AC)

Protect Privileges. Control Applications. Achieve Compliance.

Solution Brief

Get a Demo →

Strengthen Security Leadership with Unified Privilege and Application Control

Privileged accounts, including administrative accounts, and unauthorized applications are prime targets for cyberattacks, with 99% of breaches involving credential abuse in 2024.

Heimdal's Privilege Elevation and Delegation Management (PEDM) and Application Control (AC) offer a unified solution to secure administrative access, enforce least privilege policies, and block unauthorized application executions. This approach ensures compliance with regulations like NIS2 and NIST while streamlining operations and reducing risks.

Unmatched Privilege Control & Security Confidence

93%
of critical vulnerabilities in Windows OS can be mitigated by removing local admin rights.

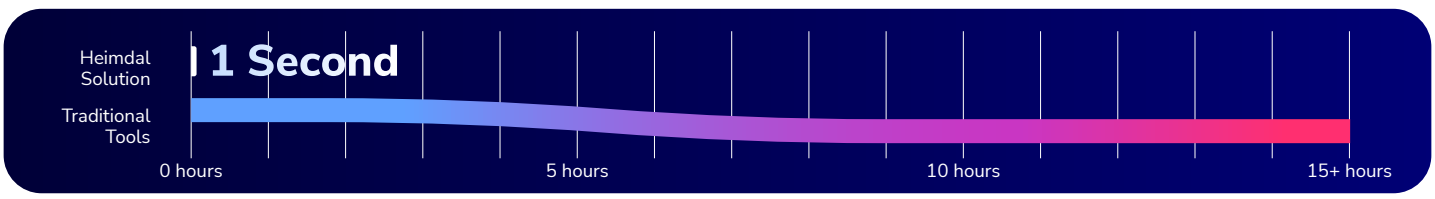
85%
of breaches could be prevented by implementing robust application control and privilege management.

1. Streamline Operations with Heimdal: Faster ROI and Reduced Effort

- Achieve ROI in less than 30 minutes with streamlined setup and faster deployment.
- Reduce manual effort by 75% within the first two months of deployment, freeing resources for critical tasks.

2. Accelerate Privilege Management with Heimdal: Real-Time Automation

- Automated privilege approval workflows reduce manual approval time to as little as 1 second.
- Traditional tools may still take hours for manual privilege escalations.



3. Compliance Simplified: Meet Key Standards Effortlessly

Heimdal ensures streamlined compliance across leading frameworks like NIST AC-6, NIS2, and CAF/Cyber Essentials, enabling secure operations and regulatory adherence without added complexity.

NIST AC-6
Enforces least privilege policies through dynamic privilege management.

NIS2 Directive
Simplifies reporting and compliance audits with real-time tracking and logging.

CAF / Cyber Essentials
Delivers baseline security controls for cyber resilience, ensuring privileged access and application management are aligned with organizational risk management strategies.

Heimdal Privilege Elevation and Delegation Management (PEDM) & Application Control (AC)

Advanced Features for Seamless Privilege and Application Management

Explore the unified capabilities that simplify security, enhance control, and ensure compliance for IT teams and MSPs.

Heimdal's combined Privilege Elevation and Delegation Management (PEDM) and Application Control (AC) solutions empower organizations to enforce zero-trust policies, manage critical privileges, and secure application execution workflows. Designed for IT professionals and MSPs, this unified approach mitigates risks from ransomware and malware while ensuring compliance with global standards such as GDPR, ISO 27001, and NIS2.

By centralizing privilege management and application control, Heimdal simplifies operations, reduces administrative overhead, and enhances security across hybrid environments.

Privilege Elevation and Delegation Management (PEDM)

A robust privilege management solution that dynamically enforces least privilege policies, automates access control workflows, and ensures compliance across hybrid environments.

Key Features	Description
Removal of Persistent Admin Rights	Eliminate local admin rights to comply with NIST AC-1 and AC-6 standards, reducing insider and external threats.
User and File Elevation Management	Dynamically grant elevated privileges for specific users, tasks, or applications, maintaining secure access control.
Escalation Period Control	Set custom durations for elevated privileges and revoke access automatically to minimize risks.
Zero-Trust Execution Protection	Instantly block unauthorized or malicious applications, enforcing zero-trust principles for maximum security.
Advanced ML Auto-Approval	Automatically approve privilege elevation requests based on historical behavior analysis and pre-set thresholds, optimizing workflows with adaptive security.
Detailed Audit Logs and Reporting	Track all privilege escalations, timestamps, and access changes in detailed logs to simplify compliance reporting.
Multi-Channel Approval Workflows	Approve privilege requests via a centralized dashboard, email, or mobile apps (iOS & Android) for flexibility and security.
Auto-Pilot Mode with Pre-Approvals	Automate recurring privilege approvals for streamlined operations without manual intervention.

Application Control (AC) with AppFencing™

Advanced application control solution that enforces Zero-Trust policies, streamlines workflows, and provides granular control to meet diverse security and compliance needs.

Key Features	Description
AppFencing™ with Zero-Trust Execution	Enforces granular Zero-Trust Execution policies to block unauthorized applications, restrict process spawns, and prevent lateral movement attacks, ensuring compliance with standards like NIST and GDPR.
Application Execution Policies	Block or allow applications based on file path, MD5 hash, publisher, or certificate validation to secure environments.
Passive Mode Monitoring	Log all application executions for historical analysis and establish policies based on execution data.
Dynamic App Blocking with Zero-Trust	Instantly block untrusted or malicious applications with proactive enforcement of Zero-Trust execution policies.
Customizable Allow/Block Rules	Set granular application control policies at the group, file, or user level to meet diverse organizational needs.
Audit-Ready Logging	Maintain 90-day logs for all allowed, blocked, and monitored application executions to meet compliance requirements.
Default Approval for System Apps	Pre-approve trusted system applications to reduce unnecessary prompts and improve operational efficiency.
Auto-Elevate Pre-Approved Applications	Automatically grant temporary elevation for applications requiring admin rights without exposing full privileges.

KEY BENEFITS

For CIOs, CISOs & Security Leaders:

- **Proactive Risk Management:** Enforce zero-trust policies and mitigate risks from insider and external threats.
- **Streamlined Compliance:** Meet global regulatory requirements with detailed audit logs.
- **Cost Efficiency:** Reduce operational costs with automated workflows that save time for administrators and minimize delays for end users waiting on approvals.

For IT Professionals & Enterprises:

- **Operational Efficiency:** Automate privileges and application workflows, reducing manual intervention.
- **Enhanced Visibility:** Monitor all activities through a unified dashboard for informed decision-making.
- **Security Optimization:** Dynamically mitigate vulnerabilities and enforce application policies.

For MSPs:

- **Multi-Tenant Efficiency:** Manage multiple clients from a centralized dashboard with custom rules.
- **Compliance at Scale:** Provide built-in reports for clients, ensuring regulatory adherence.
- **Streamlined Workflows:** Automate onboarding and privilege configurations to save time.

PRIVILEGED ACCESS MANAGEMENT

Heimdal Privilege Elevation and Delegation Management (PEDM) & Application Control (AC)

Heimdal PEDM + APP CONTROL: Unified Solution Benefits

Integrated Threat Intelligence & Security

Unify privilege and application control with Heimdal's XDR ecosystem, enabling proactive defense against ransomware, malware, and insider threats through centralized threat intelligence, integrated with modules like DNS Security, Endpoint Detection, and Patch Management.

Compliance-Ready Framework

Align with regulatory standards like GDPR, NIS2, ISO 27001, and NIST AC-6 using detailed audit trails and compliance reporting, supported by data from Heimdal modules such as Ransomware Encryption Protection and Privileged Access Management.

Granular Role-Based Policies

Streamline access management by assigning permissions based on organizational roles and structures, ensuring secure operations across hybrid environments.

Effortless Multi-Tenant Management

Empower MSPs to manage privileges and applications seamlessly across multiple clients from a single, centralized dashboard.

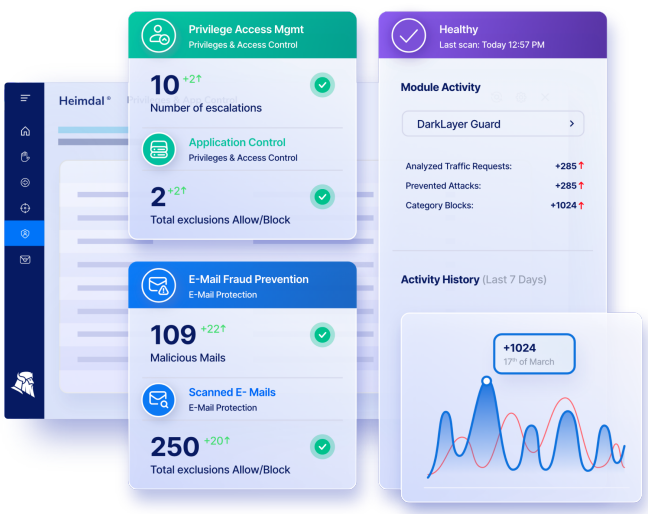
A Unified XDR-Ready Security Ecosystem

Heimdal's PEDM and Application Control (AC) are integral components of its XDR platform, working seamlessly with DNS Security, Endpoint Security, Ransomware Protection, and Patch Management. This unified approach delivers comprehensive threat detection, rapid response, and prevention tailored to the needs of modern IT environments.

Secure Privileges. Protect Applications. Achieve Compliance.

Request a demo today to discover how Heimdal's PEDM and AC can enhance your security, simplify compliance, and optimize your IT operations with cutting-edge efficiency.

Get a Demo →



Why choose Heimdal as your security partner?

Heimdal is an industry-leading unified and AI-powered cybersecurity solutions provider established in Copenhagen in 2014. With an integrated approach to cybersecurity, Heimdal has dramatically boosted operational efficiency and security effectiveness for over 16k+ customers globally.

Heimdal empowers CISOs, Security Teams, and IT admins to enhance their SecOps, reduce alert fatigue, and be proactive using one seamless XDR security platform.

Our award-winning line-up of 10+ fully integrated cybersecurity solutions span the entire IT estate, allowing organizations to be proactive, whether remote or onsite.

> **"Choosing Heimdal® was a strategic move for us. It's not just a security product; it's a smart, efficient way to protect privileges, identity, and access. This solution fits right into our daily operations, offering robust security without adding complexity or hindering our workflow."**
>
> **- Peder Vegborn,**
> **IT Manager**
>
> VINCI ENERGIES

Gartner peerinsights ★★★★★ SOURCEFORGE ★★★★★ Capterra ★★★★★ Expert Insights ★★★★★