Heimdal®

Simplifying Security for Senior Tech: Doro Group Elevates Cyber Control with Heimdal

Case Study - Technology, Consumer Electronics

CHALLENGES

- **Local Administrator Rights Gap:** External customer audits identified a significant security risk due to the presence of local administrator rights on company computers and clients.
- **Small IT Department & Application Distribution:** With a very small IT department, Doro Group was unable to centrally package and distribute all applications, necessitating a solution where users could install their own programs, including tailor-made applications requiring local installation.
- **Inconsistent Third-Party Patching:** Before Heimdal, frequently updated third-party applications (like Adobe and Chrome) had to be centrally packaged and pushed out, a process that was difficult to keep up with, sometimes resulting in updates falling "months behind".
- **OS Patching Flexibility & Enforcement:** Managing operating system (OS) patching on client machines lacked flexibility, making it difficult to enforce mandatory reboots while also accommodating users' needs to postpone updates when timing wasn't right.
- **UAC Prompt Obstacle with Remote Support:** Their previous remote desktop solution (TeamViewer) could not bypass User Account Control (UAC) prompts without user intervention, causing delays and requiring the user to be present for assistance.

SOLUTION

Doro Group initially sought a new cybersecurity solution primarily to address the glaring gap in local administrator rights, seeking a simple and effective management method. Having seen Heimdal in use as a consultant, Mathias Thulin, IT Operations Manager recognized its value and ease of implementation. Doro Group adopted Heimdal's platform, later expanding its use to include comprehensive patching and enhanced remote support capabilities. Heimdal's deployed solution includes:

- **Privilege Elevation and Delegation Management (PEDM):** This was Doro Group's first Heimdal module. It effectively closed the local administrator rights vulnerability, enabling users to install necessary software through automated or approval-based flows. Crucially, no one at Doro Group is a local administrator today, including Mathias Thulin.
- **Patch & Asset Management:** It enabled Doro Group to patch third-party applications like Adobe and Chrome directly from Heimdal, eliminating the need for central packaging and ensuring apps are always on the latest version for improved security and stability. It also provides flexibility for OS patching, allowing users to postpone updates while enabling IT to enforce mandatory reboots for security and hardware longevity.
- **Remote Desktop:** This solution proved more affordable than TeamViewer. A key benefit is its ability to bypass UAC prompts remotely using an authorized account, which resolved a significant issue that arose after removing LAR. This allows IT to assist users without delay and even without the user being present.

INTRODUCTION

Doro Group, Europe's market leader in senior mobile phones, has significantly enhanced its cybersecurity posture through a strategic partnership with Heimdal. Facing critical challenges related to local administrator rights, inefficient patching, and streamlined remote support for its lean IT team, Doro Group leveraged Heimdal's unified platform to achieve robust control, efficiency, and simplified security management.

doro®

ABOUT DORO GROUP

Doro is a Swedish technology company that develops products and services specifically for seniors, focusing on supporting an active and independent life. The company is the market leader in Europe in senior mobile phones, headquartered in Malmö, and is listed on Nasdaq Stockholm.

IMPACT AND BENEFITS

Post-implementation, Doro Group experienced significant and transformative benefits:

- **Enhanced Security & Audit Compliance:** The PEDM module immediately closed the local administrator rights vulnerability, resolving a critical security hole flagged during audits. Consistent patching ensures systems are always on the latest, most secure versions.
- **Streamlined IT Operations & Time Savings:** Automating third-party patching saved considerable time and money, eliminating the need to hire personnel for application packaging. Users no longer need to contact IT for update assistance.
- **Improved Patching & System Stability:** Doro Group now consistently runs the latest software versions, enhancing system stability and security. OS patching gained necessary flexibility, allowing user postponements while ensuring mandatory reboots for critical updates.
- **Efficient Remote Support:** The Remote Desktop solution proved more affordable and, critically, enabled IT to bypass UAC prompts remotely. This significantly sped up support processes, as IT technicians no longer have to wait for users or require their presence to perform administrative tasks.
- **Ease of Use & Implementation:** Heimdal was a smooth, simple, and non-invasive solution to implement, essentially acting as an add-on. Internal feedback confirms it's "easy to use and hard to mess up" even for non-tech-savvy users.

WHY HEIMDAL FOR CONSUMER TECH

Organizations in the Technology and Consumer Electronics sector often face the dual challenge of rapid innovation and maintaining robust security across diverse user bases and endpoints. With lean IT teams and a constant need for efficiency, they require solutions that simplify complex cybersecurity tasks and scale without hindering operations. Heimdal delivers a unified platform designed for operational resilience, regulatory readiness, and stretched IT teams.

- **Purpose-Built Protection:** Heimdal defends networks from phishing, ransomware, and endpoint threats, crucial for safeguarding intellectual property and user data in a fast-paced environment.
- **Supports Regulatory Frameworks:** The platform helps meet various industry standards (e.g., GDPR, ISO 27001) through automated tools and auditable policies, essential for data privacy and compliance.
- **Operational Continuity:** Real-time threat prevention, ransomware defense, and secure remote access help maintain vital development and support services without disruption.
- **Unified Platform, Lower Workload:** A single dashboard to manage security reduces tool sprawl and enables faster response, empowering lean IT teams to manage security more effectively.
- **Scalable & Budget-Conscious:** Heimdal is flexible enough for organizations of any size, providing maximum protection without the cost of complexity, crucial for optimizing IT budgets.
- **Outstanding Product Quality and Support:** The outstanding product quality and support are exactly what organizations in this sector look for in a partner, ensuring reliable assistance and minimizing downtime.
- **Continuous Development:** Heimdal shows a commitment to continuous development, always pushing forward on the security front, ensuring long-term protection against emerging threats and technologies.

CONCLUSION

Doro Group strategically chose Heimdal after evaluating its proven effectiveness, ease of use, and non-invasive integration. The platform's advanced capabilities, combined with its remarkable simplicity, proved to be a crucial factor for Doro Group's environment. The implemented modules have seamlessly integrated into their operations, delivering reliable performance and straightforward deployment.

> *"We've strategically chosen the Heimdal modules that best address our critical attack vectors and surfaces, and they work incredibly well, never have any issues, simple to implement, and we've found it to be a solution we would absolutely recommend to other organizations."*

- Mathias Thulin,
It Operations Manager

Capterra ★★★★★ 4.8/5 | Expert Insights ★★★★★ 4.8/5 | Gartner peerinsights ★★★★★ 4.8/5

Learn More