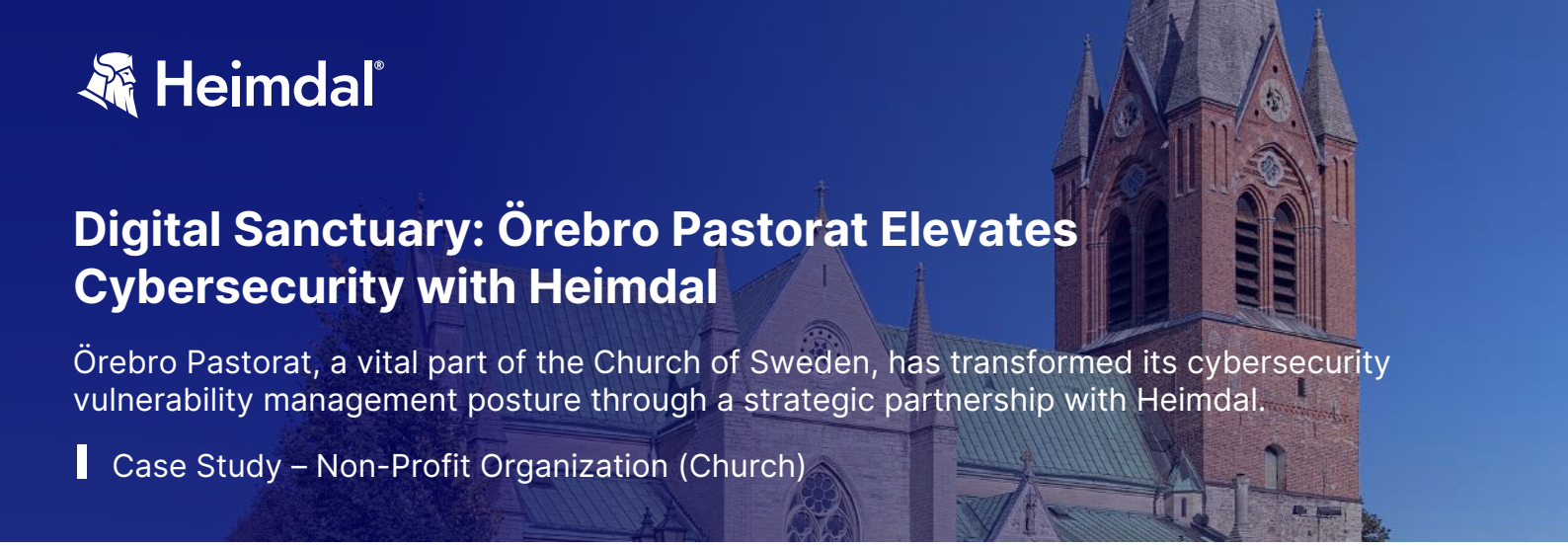

Digital Sanctuary: Örebro Pastorat Elevates Cybersecurity with Heimdal

Örebro Pastorat, a vital part of the Church of Sweden, has transformed its cybersecurity vulnerability management posture through a strategic partnership with Heimdal.

Case Study – Non-Profit Organization (Church)

Facing the complexities of managing numerous computers without direct domain control and securing a distributed workforce, Örebro Pastorat leveraged Heimdal's unified platform to achieve greater control, efficiency, and robust protection.

COMPANY OVERVIEW:

Svenska kyrkan

Örebro Pastorat is integral to the Church of Sweden, administering eight parishes. This religious organization, with approximately 250 staff members, manages around 250 computers and engages in a diverse range of activities, including counseling, youth engagement, crisis support, and cemetery management. Their work extends beyond traditional religious services, embedding them deeply in community welfare and support.

CHALLENGES

- **Lack of Centralized Device Control:** Örebro Pastorat was responsible for managing 250 computers but lacked control over their own domain, which had been handed over to the national level. This resulted in significant loss of visibility and control over their devices.
- **Inefficient Software Management & Updates:** Before Heimdal, IT technicians frequently received calls from users requesting help with program updates. There was no effective and automated way to manage patching across their 250 computers, leading to significant time expenditure.
- **Securing Remote & Off-Network Devices:** A key concern was how to secure devices used by staff at home and when operating outside the pastorate's network. They specifically aimed to block access to inappropriate content like gaming and pornography.
- **Complex Script & Program Distribution:** The need for effective computer management implied difficulties in efficiently distributing scripts and applications, such as critical Wi-Fi security upgrades, without manual user intervention.

SOLUTION

Örebro Pastorat initially sought a sensible way to manage their computers, prioritizing patch management and remote access. While other cybersecurity functionalities were initially a bonus, Heimdal's comprehensive platform proved to be the right fit, standing out due to its breadth of features, particularly in the DNS space.

Heimdal's deployed solution includes:

- **Patch & Asset Management:** This was the primary justification for their purchase. It now auto-patches almost everything, virtually eliminating calls about program updates and saving "several hours each week" in IT work hours. It also provides a much clearer overview of outdated versions running on devices.
- **Infinity Management (Add-on to Patch Mgmt.):** Primarily used for scripting tasks, it proved "extremely effective". It was successfully used to upgrade Wi-Fi security from WPA2 to WPA3 on 250 machines without requiring users to manually enter new security keys.
- **Remote Desktop:** Enabled essential remote access capabilities for IT support.
- **DNS for Endpoint:** This was an initial draw for Örebro Pastorat, providing a way to protect devices outside their network. It helped secure devices used at home and blocked access to unwanted content, also notifying the IT team of suspicious or risky network activity, thereby restoring crucial visibility and control.

The consolidation aspect of Heimdal's platform was also highly valued, as fewer third-party applications needed to be installed, resulting in less endpoint overload.

Heimdal®

Digital Salvation: Securing the Sanctuary with Heimdal® at Örebro Pastorat

IMPACT AND BENEFITS

Post-implementation, Örebro Pastorat experienced significant and transformative benefits:

- **Significant Time Savings & Enhanced Efficiency:** IT support calls for software updates dropped to zero, saving "several hours each week". Patch management alone justified much of the initial cost in terms of saved work hours.
- **Improved Control & Visibility:** Gained a much clearer overview of outdated software versions and overall device status. The DNS solution provided crucial notifications for suspicious network activity, restoring visibility and control lost after domain transfer.
- **Robust Security for Distributed Devices:** Off-network and home-used devices are now securely protected through DNS for Endpoint, which effectively blocks access to unwanted content.
- **Streamlined Operations:** Infinity Management enabled the seamless deployment of scripts, such as Wi-Fi security upgrades across 250 machines, ensuring uninterrupted workflow without manual user intervention.
- **Consolidated Security Management:** The unified Heimdal platform reduced the need for multiple third-party applications, leading to less endpoint overload and more streamlined management.

> ***"We definitely saved several hours each week just on updating software. The overview is much clearer now."***
>
> **Joakim Öjerteg,** IT Technician

CONCLUSION

Örebro Pastorat discovered Heimdal through a combination of a Google search and a strong recommendation from a Norwegian security event, noting that no other evaluated vendor could offer the same breadth of features, especially in the DNS space. Heimdal's patching capabilities primarily justified the purchase, leading to immediate time savings. The support received has been consistently excellent, quick, helpful, and highly competent. Both IT Technicians, Joakim Öjerteg and Anders Persson, strongly recommend Heimdal to their industry peers.

> ***"I would absolutely recommend it. It's a stable product backed by a professional company."***
>
> **Anders Persson,** IT Technician

> ***"I agree with Anders—and it doesn't hurt that the company is based in the Nordics, especially in times like these."***
>
> **Joakim Öjerteg,** IT Technician

WHY HEIMDAL FOR NON-PROFIT ORGANIZATIONS (RELIGIOUS INSTITUTIONS)

Religious organizations often operate with lean IT teams while managing extensive networks across diverse locations and serving various community functions. 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 sensitive community data and operations.
- **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 governance.
- **Operational Continuity:** Real-time threat prevention, ransomware defense, and secure remote access help maintain vital services and community engagement without disruption.

Learn More →

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