

Elevating Cyber Resilience Across Municipal Operations

Vaggeryds Kommun has enhanced its cybersecurity posture through a strategic partnership with Heimdal Security. With 1,000 employees and 1,800 students across 2,800 devices, and a lean IT team, the commune needed a security platform that could simplify protection, reduce risk, and scale alongside its digital transformation goals. Heimdal provided the right combination of unified tools, proactive defense, and operational efficiency.

Case Study – Public Sector, Municipality



CHALLENGES

Lean IT Team

With only 6–7 staff managing cybersecurity, infrastructure, and user support, efficiency was essential. The commune needed a platform that could operate autonomously while offering full visibility and control.

Ongoing Cloud Transition

Vaggeryds Kommun is currently undergoing a transition from Office 2016 to Microsoft 365, a project that presents both opportunity and complexity.

Strategic Procurement

The commune favored European-rooted solution vendors and had to make high-impact decisions under strict budget parameters.



SOLUTION

To meet its operational and security needs, Vaggeryds Kommun adopted Heimdal's unified cybersecurity platform. This comprehensive solution protects users, devices, identities, and communications—all managed through a single dashboard.

Key components include:

- Next-Gen Antivirus and Firewall: Delivers behavioral threat detection and centralized control over workstation devices.
- DNS Security: Blocks access to malicious websites and phishing domains before threats reach endpoints, forming a critical first line of defense.
- Ransomware Encryption Protection: Monitors for unauthorized encryption attempts in real time, preventing file lockout and data loss.
- Remote Desktop Access: Enables secure internal support sessions without exposing the network to unnecessary remote access risks.



ABOUT VAGGERYDS KOMMUN

Vaggeryds Kommun is a local government authority in southern Sweden, responsible for delivering critical services to approximately 15,000 citizens. As part of its modernization strategy, the municipality has embarked on an ongoing transition to Microsoft 365, reshaping its digital infrastructure while navigating security, compliance, and budget considerations.

- Application and Privilege Control: Ensures only authorized software runs on municipal systems, while minimizing unnecessary administrative access.
- Patch and Asset Management: Automates updates across third-party applications to eliminate vulnerabilities and reduce maintenance workload.
- Email Security ATP: Defends municipal inboxes from spam, spoofing, and targeted email-borne threats.
- Privilege Elevation and Delegation Management:
 Empowers the IT team to enforce least privilege
 policies and mitigate insider or lateral movement
 threats.

This streamlined security stack helps Vaggeryds Kommun stay secure and compliant while reducing complexity, freeing up internal resources to focus on strategic IT initiatives.





RESULTS & IMPACT

Reduced Cyber Risk

Heimdal's DNS Security and ransomware protection features have helped the commune reduce exposure to phishing, encryption-based attacks, and unauthorized remote access. Proactive blocking prevents incidents before they disrupt operations.

Seamless Support During Digital Transformation

As the municipality progresses with its Microsoft 365 rollout, Heimdal helps maintain consistent protection across both legacy and new systems—ensuring users and data remain secure throughout the transition.

Simplified IT Operations

By consolidating multiple capabilities into a single platform, Heimdal enabled Vaggeryds Kommun to strengthen security without increasing the workload. The IT team can act quickly, resolve issues faster, and manage risk more effectively.



CONCLUSION

Vaggeryds Kommun's partnership with Heimdal highlights how local governments can elevate their cybersecurity posture without compromising on simplicity or scalability. With Microsoft 365 as an ongoing foundation for future operations, Heimdal continues to serve as a trusted security ally—keeping systems resilient, citizens protected, and IT empowered.

"Heimdal gives us peace of mind. With a small team, we can't afford to manage dozens of tools. Their platform handles email, endpoint, patching, and user access in one place—while keeping us aligned with our M365 rollout."

Tobias Karlhager,

Head of IT and Digitalization, Vaggeryds Kommun



WHY HEIMDAL FOR PUBLIC SECTOR?

Local government and public sector bodies face growing pressure to modernize IT systems while defending against evolving cyber threats—all with limited internal resources. Heimdal delivers a unified platform designed for operational resilience, regulatory readiness, and stretched IT teams.

- Purpose-Built Protection Heimdal defends public sector networks from phishing, ransomware, and endpoint threats across municipalities, councils, and local agencies.
- Supports Regulatory Frameworks Helps meet GDPR, NIS 2, Cyber Essentials, CAF, and other public sector standards through automated tools and auditable policies.

- **Operational Continuity** Real-time threat prevention, ransomware defense, and secure remote access help maintain vital services without disruption.
- Unified Platform, Lower Workload One dashboard to manage identity, email, device, and access security—reducing tool sprawl and enabling faster response.
- Scalable & Budget-Conscious Flexible enough for any municipality size, Heimdal provides maximum protection without the cost of complexity.

Learn More →















