24/7 MXDR and Automated Patching: Porsanger Kommune Improves Compliance with a Lean IT Team

Case Study - Public Sector, Local Government (Norway)

CHALLENGES

- **Strict national security guidance:** Meeting requirements for logging, visibility, and the ability to isolate users and devices quickly when needed.
- **Lean resources:** A small IT team cannot staff a 24/7 security function internally.
- **Operational complexity:** The previous security setup involved multiple separate management consoles, adding overhead and friction.
- **Patching and software rollout reliability:** Legacy update deployment methods were prone to failures and required manual troubleshooting.
- **Containment without disruption:** The team needed to block compromised devices from the internet while still maintaining internal monitoring for investigation and compliance.

SOLUTION

Porsanger Kommune conducted a competitive procurement review and selected Heimdal for two decisive reasons: reliable automated third-party patching and a strong multi-year commercial fit. The municipality standardised on Heimdal to automate routine security operations, consolidate visibility, and enable rapid containment actions when incidents occur.

Heimdal solutions deployed:

- **Heimdal MXDR (Managed Detection & Response)**
  24/7 monitoring and response support to cover out-of-hours threats for a lean IT team.
- **Heimdal XDR Platform**
  Unified visibility, investigation, and containment actions from one place.
- **Heimdal Patch & Asset Management (Vulnerability Management)**
  Automated OS and third-party patching, plus fast and reliable software deployment.
- **Heimdal Privileged Access Management (PEDM)**
  Controlled elevation and admin protection to reduce misuse of privileged access.

Also includes: DNS and web protection, email security, endpoint prevention controls, ransomware protection, and remote administration.

INTRODUCTION

Porsanger Kommune needed to strengthen security and compliance without growing the team. With a very small IT function supporting a broad mix of endpoints, the priorities were clear: automate patching, improve visibility for audits, and ensure there is always monitoring and response capability, even outside working hours. Heimdal was selected to reduce day-to-day operational load and make security controls easier to run and prove.

Porsanger kommune
Porsáŋggu gielda-Porsangin komuuni

ABOUT PORSANGER KOMMUNE

Porsanger is a Norwegian municipality supporting hundreds of employees. A super-lean IT team manages a mixed estate of over 1,000 devices, including a combination of computers, mobiles, and tablets.

KEY DECISION DRIVERS

- **Third-party patching capability:** A core requirement that alternatives did not meet to the same standard.
- **Automation that removes daily burden:** Patch deployment and software rollout that works consistently, with fewer failures and less troubleshooting.
- **Simpler operations:** Reduced complexity by avoiding multiple consoles and disconnected workflows.
- **Budget alignment:** A cost-effective multi-year agreement compared with the next best option.

IMPACT AND BENEFITS

- **Automated patching at speed:** Updates can be deployed in seconds, helping the team stay current across key third-party applications and operating systems.
- **Major time savings:** Reduced hands-on effort compared with older deployment methods, especially where rollouts previously failed and needed rework.
- **Stronger compliance posture:** Improved logging and visibility, plus the ability to isolate users and devices quickly when required.
- **Practical containment during incidents:** In response to phishing activity, the municipality isolated the affected user in its identity system, then blocked the impacted device from internet access while continuing internal monitoring to investigate safely.
- **24/7 coverage without hiring:** MXDR provides always-on monitoring and response, removing the need to build an in-house round-the-clock function.

WHY HEIMDAL FOR EU & NORDICS LOCAL GOVERNMENT

Local government teams are expected to meet high security and compliance standards with limited resources and fixed budgets. Heimdal supports that balance through:

- **Automation-first security operations:** Reliable patching and software deployment that reduces manual workload.
- **Compliance-ready visibility and control:** Centralised oversight and rapid isolation actions to support audits and incident handling.
- **Always-on protection for lean teams:** 24/7 monitoring and response without building a full internal SOC function.
- **Unified platform efficiency:** Reduced complexity versus running multiple disconnected tools and consoles.
- **Budget-conscious value:** Broad coverage that respects public sector procurement realities.

CONCLUSION

By standardising on Heimdal, Porsanger Kommune reduced operational friction and improved its ability to meet strict security guidance with a super-lean IT team. Automated patching became the backbone of day-to-day security hygiene, while MXDR added essential 24/7 coverage. Together, these capabilities help the municipality stay compliant, respond faster, and spend less time troubleshooting routine deployment issues.

Heimdal keeps us safe at night, and I don't think about it when I go home. The automation is a huge help for us, and it takes a lot of the day-to-day pressure off a very small team.

- Jan-Ove Pedersen,
IT Manager

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

Learn More