Securing Danish Public Services: Brønderslev Kommune Unifies its Cybersecurity Strategy for NIS2 Compliance with Heimdal

Case Study - Public Sector, Municipality

CHALLENGES

- **Need for Unification:** For a longer period of time, the municipality had a complex security setup and needed to simplify its stack for an easier administration and mitigation. The goal was to free up time and resources in the IT team for other tasks.
- **Regulatory Compliance:** *The municipality needed to live up to new governmental requirements, specifically the NIS2 Directive, as well as demands for 24/7-365 surveillance and a Security Operations Center (SOC).*
- **Resource Constraints:** The IT team was spending too much time, time they did not have, which meant leaving important tasks undone.
- **Vulnerability & Control:** Brønderslev Kommune had a too high number of vulnerabilities in its environment and were lacking control on devices.

SOLUTION

To meet its operational and security needs, Brønderslev Kommune adopted Heimdal's unified cybersecurity platform, which allowed them to consolidate their security products into a single dashboard. With Heimdal's platform, the municipality is able to meet the new demands, has less agents on its devices, and one dashboard for almost everything. The key components deployed include:

- **Next-Gen Antivirus & Firewall:** Provides a proactive, behavioral threat detection approach and centralized control.
- **DNS Security:** Blocks malicious websites and phishing domains before threats can reach endpoints.
- **Ransomware Encryption Protection:** Monitors for unauthorized encryption attempts in real time to prevent file lockout and data loss.
- **Patch & Asset Management:** Automates updates across endpoints and servers to eliminate vulnerabilities and reduce the maintenance workload.
- **Email Security - ATP:** Defends municipal inboxes from spam, spoofing, and targeted email threats.
- **Managed Extended Detection & Response (MXDR):** Provides a SOC for 24/7-365 surveillance, helping the municipality meet its new governmental requirements.

BRØNDERSLEV KOMMUNE

Brønderslev Kommune, a municipality in North Jutland, Denmark, with around 36,600 inhabitants, needed to modernize its cybersecurity infrastructure to meet new government regulations and simplify its operational environment. The municipality provides a wide range of public services, from childcare to environmental protection, and a key focus is on delivering high-quality welfare services to its citizens. As the municipality aimed to live up to new demands, it sought a solution that could unify its security strategy, reduce administrative workload, and elevate its security posture.

RESULTS & IMPACT

- **Enhanced Compliance:** With Heimdal's platform, the municipality is able to meet the new demands set by NIS2. Heimdal's SOC is **more attentive and quicker to respond** than the one they had before.
- **Increased Security & Trust:** After adopting Heimdal, the municipality feels it is in ***"better and safer hands"*** compared to its previous security provider. The strategic procurement of a local, Danish vendor was a crucial consideration, and the team now feels more secure with the Heimdal platform.
- **Streamlined Operations:** Consolidating a large part of their security products into a single platform provides the IT team with a better overview and **saves time and resources.** This has significantly improved their daily administration and reduced the number of uncompleted tasks.
- **Efficient Support:** Brønderslev Kommune has received efficient and fast-reacting support from Heimdal that informs them about potential security incidents. The team feels they get the attention they need and that the relationship is a collaborative partnership.

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:** Heimdal helps institutions meet standards such as GDPR, NIS 2, and Cyber Essentials 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:** A single dashboard to manage security reduces tool sprawl and enables faster response for lean IT teams.
- **Scalable & Budget-Conscious:** Heimdal is flexible enough for any municipality size, providing maximum protection without the cost of complexity.

CONCLUSION

Brønderslev Kommune's partnership with Heimdal highlights how a local government can elevate its cybersecurity posture without compromising on simplicity or scalability. The municipality chose Heimdal because it's a Danish vendor that provides a proactive security approach. With Heimdal, they have fewer agents on their devices, a single dashboard for management, and the ability to get the job done.

"We would recommend Heimdal to any municipality or organization out there that has challenges like ours. Heimdal gets the job done, we get all the support we need and ask for and they are both proactive and easy to work with."

- Peter Søndergaard,
Head of IT / IT Manager, Brønderslev Kommune

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

Learn More