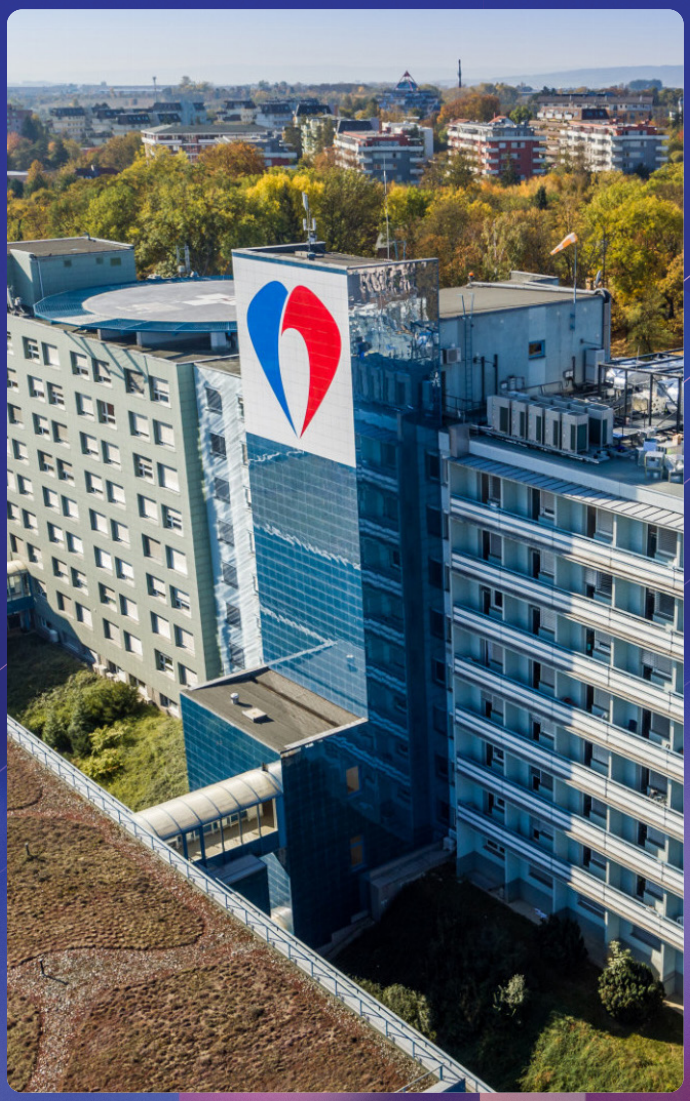
CASE STUDY – **HEALTHCARE**

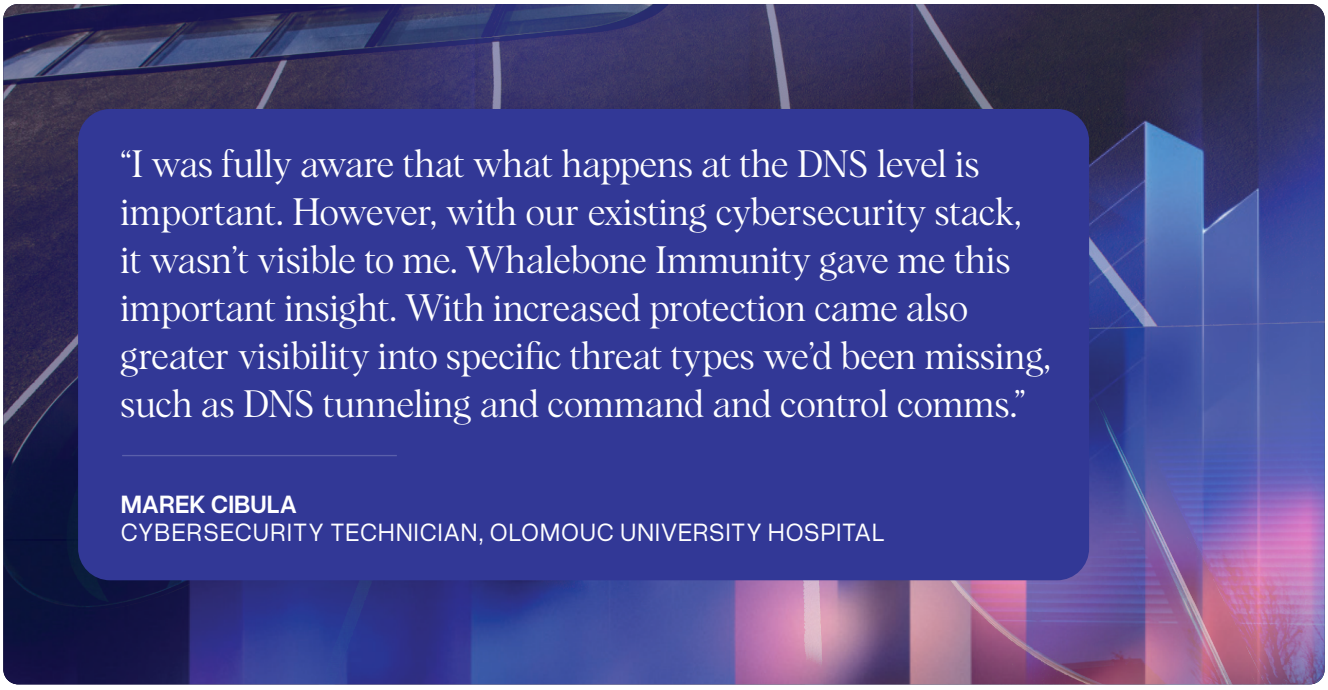
Securing 4,000+ Devices: Olomouc University Hospital Deploys DNS Protection Across Critical Healthcare Systems



Olomouc University Hospital is one of the largest and most advanced medical centers in the Czech Republic, the second biggest employer in its region, and the sixth largest hospital nationwide.

Serving over a million outpatients each year and managing more than 4,000 devices, the hospital faces complex cybersecurity challenges typical of critical healthcare infrastructure. Protecting sensitive patient data and ensuring uninterrupted access to electronic health records are top priorities.

In this environment, **operational efficiency** and **proactive threat prevention** are **essential to maintain trust** and **compliance** with strict regulations such as GDPR and NIS2.



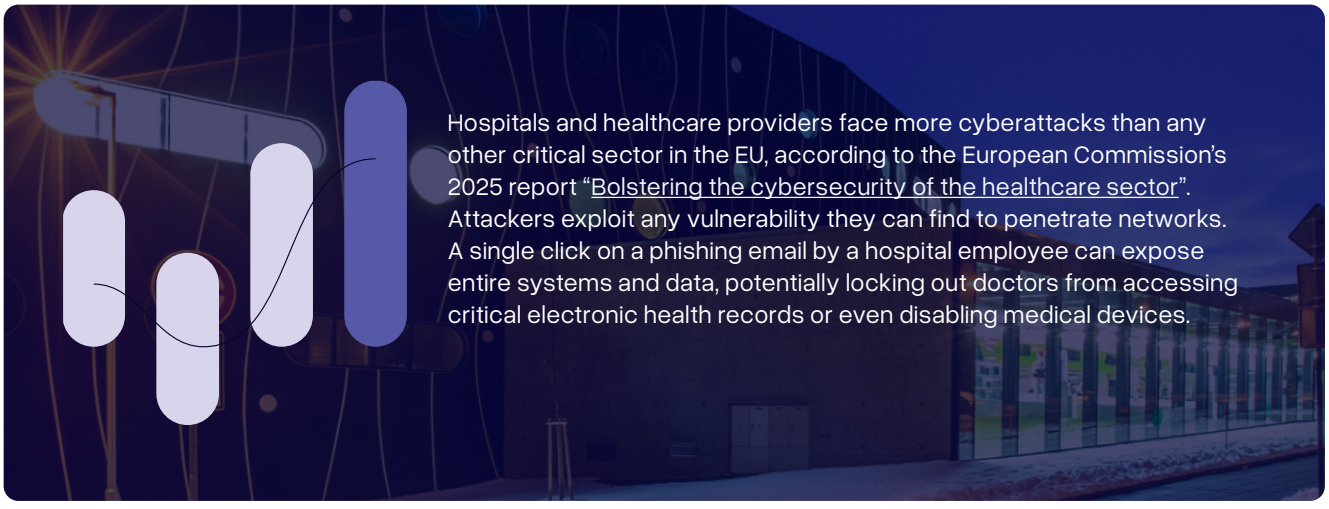
> “I was fully aware that what happens at the DNS level is important. However, with our existing cybersecurity stack, it wasn’t visible to me. Whalebone Immunity gave me this important insight. With increased protection came also greater visibility into specific threat types we’d been missing, such as DNS tunneling and command and control comms.”

MAREK CIBULA
CYBERSECURITY TECHNICIAN, OLOMOUC UNIVERSITY HOSPITAL

Challenge

Limited visibility into DNS traffic left critical systems exposed to hidden threats

The hospital’s IT team struggled with limited visibility into DNS traffic, which made detecting phishing and other DNS-based attacks difficult. Phishing incidents occurred roughly every two months, posing a constant risk to patient data and hospital operations. Managing a diverse network that includes medical devices, servers, and mobile endpoints added complexity. With a small cybersecurity team, the hospital needed a solution that would integrate smoothly with existing systems, and provide real-time threat detection without disrupting clinical workflows or adding manual workload.



Hospitals and healthcare providers face more cyberattacks than any other critical sector in the EU, according to the European Commission’s 2025 report “Bolstering the cybersecurity of the healthcare sector”. Attackers exploit any vulnerability they can find to penetrate networks. A single click on a phishing email by a hospital employee can expose entire systems and data, potentially locking out doctors from accessing critical electronic health records or even disabling medical devices.

Solution

Protective DNS delivers seamless, on-premises defense for 4,000 hospital endpoints

The implementation began with a Proof of Concept covering 500 client computers, which quickly demonstrated value and was subsequently extended to protect 4,000 client devices across the network. The PDNS solution was deployed on-premises, aligning with the hospital's preference for greater control and data security. Whalebone Immunity automatically blocks malicious DNS requests, effectively preventing phishing, malware communication, and data exfiltration attempts. The system also provides centralized logging and alerting, enabling the IT team to respond quickly to emerging threats without adding significant operational overhead.

"The initial deployment took less than an hour, and expanding to all 4,000 endpoints was just as seamless. Our users didn't even notice the change – except when a dangerous site was blocked, which is exactly what we want."

PAVEL GARTNER
CYBERSECURITY MANAGER, OLOMOUC UNIVERSITY HOSPITAL

Results

New security layer reveals hidden threats while maintaining uninterrupted hospital operations

Since implementing Whalebone Immunity, University Hospital of Olomouc has strengthened its network security significantly. During the proof of concept, Whalebone Immunity blocked 1,434 phishing-related DNS requests alone — with thousands more malicious queries stopped across all threat categories. The system also detected dozens of compromised devices, including endpoints infected with malware that had evaded other security tools. The most valuable improvement came from gaining visibility into DNS traffic — an area previously unmapped in their security architecture.

This enabled rapid identification of sophisticated threats.
The solution's non-intrusive design ensured critical hospital services remained uninterrupted, allowing the IT team to focus on genuine threats without being overwhelmed by false positives.

"When evaluating a new security layer for our hospital infrastructure, we had three non-negotiable requirements:

> ***Seamless Implementation***
> *We can't afford downtime or complex deployments. Whalebone delivered, implementation was completely trouble-free.*
>
> ***Crystal-Clear Visibility***
> *Our security team needs intuitive tools, not another system to decipher. The interface is straightforward and logical.*
>
> ***Minimal False Positives***
> *During our entire POC, we saw virtually zero false positives. The tool didn't generate nonsense alerts.*

All three requirements were met 100%. That's why Immunity is now a permanent layer in our security stack."

MAREK CIBULA
CYBERSECURITY TECHNICIAN, OLOMOUC UNIVERSITY HOSPITAL

Next Steps

Scaling DNS–layer protection across other hospital networks to reinforce cyber resilience

The hospital is now considering extending DNS protection to medical devices connected to their network. These devices often run on legacy systems that cannot be easily updated due to concerns about disrupting operational capability. *"Medical devices require specific regulatory certification. Every software change — whether to the operating system, firmware, or applications — could mean going through the entire certification process again. That's why many devices run on outdated software without security patches,"* explains Pavel Gartner, Cybersecurity Manager at the hospital. While medical devices already operate on isolated network segments, DNS–layer security would provide comprehensive protection across all connected equipment — regardless of their operating system, age, or patch status.

Additionally, while the hospital's public Wi–Fi network for patients operates on a completely separate segment and poses no direct risk to internal systems, the IT team is considering extending Whalebone Immunity's protection there as well.

Extending DNS protection to public Wi–Fi would enable the hospital to secure patient and visitor devices seamlessly — without software installation or network disruptions. This expansion demonstrates how DNS–layer security scales across the entire hospital ecosystem, from critical medical devices to guest networks, while reinforcing the hospital's commitment to comprehensive protection.

ADDITIONAL REFERENCES

Easily redirect part of your network traffic to Whalebone resolvers and try out our trial.

immunity@whalebone.io

We will be more than happy to answer any questions. Mutual satisfaction is our main goal and we will do our best to fulfill your requests.

www.whalebone.io

Learn more about our products at: **whalebone.io/immunity**

Follow us on LinkedIn