Industry: Healthcare

Use cases

- Expand visibility
- Improve detection coverage & accuracy

corelight

Case study

Leading biotech firm eliminates critical blind spots and detects advanced threats in sensitive lab environments

Background: Securing the future of cancer detection

A leading biotechnology company operates in a highly dynamic environment. Its labs contain sensitive research, patient data, and specialized Operational Technology (OT) equipment that is critical to its mission.

Challenge: Zero visibility created unacceptable risk

The company's security team faced a critical challenge: they had zero visibility into the network traffic within their labs. Due to regulatory and operational constraints, security agents could not be installed on the specialized OT and lab equipment, creating a massive blind spot. Constant changes to the lab environment made it impossible to deploy and maintain traditional monitoring tools, leaving the organization's most valuable assets exposed.

This lack of visibility meant the security team couldn't hunt for threats, respond effectively to incidents, or ensure the integrity of its core operations. They needed a way to gain visibility into all network activity without disrupting the sensitive work happening in the labs.

Solution: Gaining complete visibility with network evidence

The company turned to Corelight to close its visibility gaps. By deploying a Corelight Sensor, the team began capturing east-west and north-south traffic across its lab and corporate networks. Corelight's Open NDR Platform transformed this raw traffic into high-fidelity, actionable network evidence, providing the deep insight the team previously lacked.

With Corelight, the security team could finally see every connection and protocol in their environment. This comprehensive visibility became the foundation for improved threat detection, faster incident response, and a more resilient security posture.

Results: Uncovering hidden threats and closing security gaps

The impact was immediate and profound. Corelight's network evidence enabled the security team to uncover significant risks and active threats that had bypassed or evaded their existing security stack.

- **Detected advanced credential theft:** Identified Mimikatz activity over SMB, a technique used to dump credentials from domain controllers
- **Uncovered domain compromise techniques:** Found evidence of a DCSync attack, where an attacker impersonates a domain controller to steal password hashes

- **Identified vulnerable protocols:** Discovered the use of weak RC4 Kerberos ciphers, which could allow an attacker to crack service account passwords offline and escalate privileges
- **Exposed data security risks:** Revealed sensitive Protected Health Information (PHI) being sent in clear text over internal APIs
- **Pinpointed exploit attempts:** Detected attempts to exploit a critical Fortinet CVE against network infrastructure, a common tactic for gaining initial access

Why Corelight: Unmatched visibility in a complex environment

Corelight was the only solution uniquely suited to handle the company's constantly changing, high-volume lab environment. The key differentiators were:

- Unparalleled visibility into all network traffic without requiring agents on sensitive endpoints
- Operational analytics and detections that provided immediate, concrete results on previously unknown risks
- Flexible deployment options that integrated seamlessly with their existing infrastructure

Why it matters

The modern attack surface has expanded far beyond the traditional perimeter, creating visibility gaps where tools like EDR fall short—especially in healthcare and OT environments. To effectively defend against modern threats, security leaders must enhance their existing security stack with a solution that provides deep and widespread visibility into all network traffic. This biotech firm's success demonstrates how comprehensive network evidence and complete situational awareness are essential for detecting advanced threats and protecting an organization's most critical assets.

corelight

See how Corelight helps healthcare teams hunt smarter and respond faster

https://corelight.com/solutions/industry/healthcare

info@corelight.com | 888-547-9497