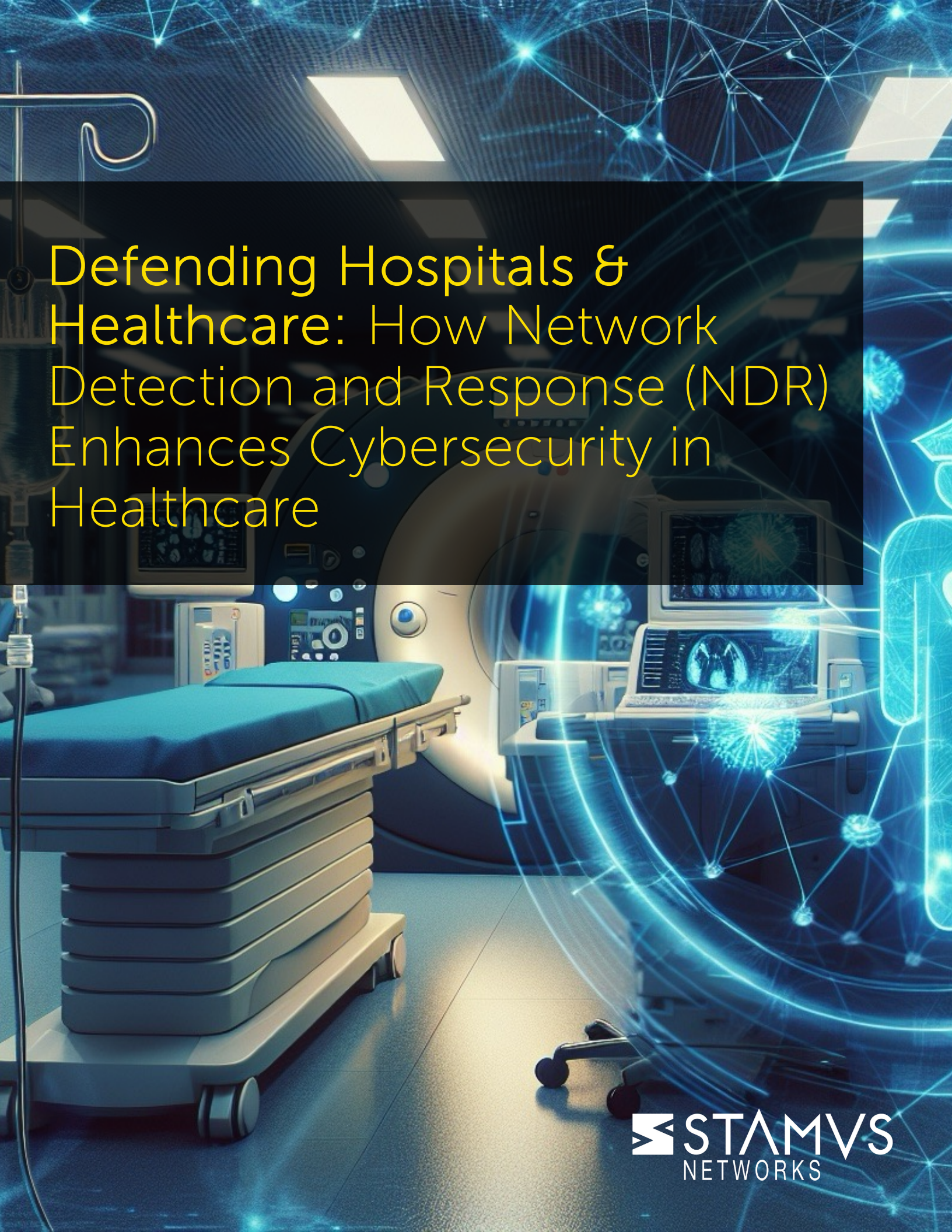


Defending Hospitals & Healthcare: How Network Detection and Response (NDR) Enhances Cybersecurity in Healthcare

STAMUS NETWORKS

Executive Summary

Healthcare organizations face an increasingly complex cybersecurity landscape marked by sophisticated threats targeting sensitive patient data and critical hospital operations. With patient records commanding high prices on the black market and the growing complexity of interconnected medical systems, traditional security measures alone are no longer sufficient.

Given these threats, traditional security controls like firewalls and endpoint protection are no longer sufficient to ensure comprehensive protection. Network Detection and Response (NDR) has emerged as a vital component in healthcare cybersecurity, offering:

- Continuous monitoring across all network traffic, including medical devices
- Real-time threat detection and response capabilities
- Seamless integration with existing security infrastructure
- Support for regulatory compliance requirements

This white paper explores how Clear NDR™ addresses the unique security challenges facing healthcare organizations while enhancing threat visibility, accelerating incident response, and protecting patient data.

Note: while NDR is a critical tool, a multi-layered defense strategy—including robust access controls, encryption, employee training, and regular security assessments—is essential for comprehensive protection.

TABLE OF CONTENTS

Introduction and overview 4

Challenges facing financial institutions 5

- High value of patient data on black market 5
- Reliance on interconnected partners and systems 6
- Regulatory compliance 7
- Rapid pace of technological advancements 9
- Increasing connectivity of medical devices not protected by existing controls 10
- Limited resources and the human element 12

Introducing Clear NDR from Stamus Networks 14

How Clear NDR addresses these challenges 15

Securing the future of hospitals and healthcare 18

INTRODUCTION AND OVERVIEW

Hospitals and other healthcare organizations face an increasingly complex cybersecurity landscape due to the sensitive nature of patient data and the criticality of hospital operations.

The value of patient data on the black market, the reliance on interconnected partners and systems, and the rapid pace of technological advancements all contribute to a heightened risk of cyberattacks.

Furthermore, the increasing connectivity of medical devices, which may not be subject to traditional security controls, introduces new vulnerabilities and potential threats to patient safety.

These factors, combined with limited resources and the human element, create a complex and challenging cybersecurity landscape for healthcare providers.

This paper explores the critical role of NDR in strengthening healthcare cybersecurity, demonstrating how it enhances threat visibility, accelerates incident response, and mitigates risks to patient data and hospital operations.

Top cybersecurity challenges facing hospitals and healthcare organizations:



High value of patient data on black market



Reliance on interconnected partners and systems



Regulatory compliance



Rapid pace of technological advancements



Increasing connectivity of medical devices not protected by existing controls



Limited resources and the human element

CHALLENGES FACING HOSPITALS AND HEALTHCARE

In the following sections, we review each of the challenges in more detail and identify ways that NDR can help healthcare security teams mitigate each.



High Value of Patient Data on the Black Market

Patient data holds immense value on the black market, making it a highly attractive target for cybercriminals. This sensitive information, which includes names, addresses, Social Security numbers, medical diagnoses, and insurance details, can be exploited in various ways. Identity thieves can use this data to open fraudulent accounts, apply for loans, or even commit medical identity theft, leading to significant financial and emotional distress for patients.

Furthermore, medical records can reveal valuable insights into an individual's health status and treatment history, which can be exploited for financial gain through fraudulent insurance claims or the sale of prescription drugs. The high financial incentives associated with patient data breaches create a strong motivation for cybercriminals, making it imperative for healthcare organizations to implement robust security measures to protect this sensitive information.

High-value patient data includes

- Personal Identifiable Information (PII): Names, addresses, social security numbers
- Protected Health Information (PHI): Medical histories, diagnoses, treatment information
- Financial Information: Insurance details, payment information

According to the IBM and Ponemon Institute's 2024 Cost of a Data Breach Report, the average cost of a healthcare data breach is $9.8 million, significantly higher than the average across all industries. This high cost reflects the significant financial and reputational damage resulting from these breaches.

Stolen patient data can be used for identity theft, medical fraud, and blackmail, causing severe financial and emotional distress for individuals.

Furthermore, the report emphasizes that "the value of health records on the black market far exceeds that of credit card data," highlighting the significant financial incentives driving cybercriminals to target healthcare organizations.

How NDR Can Help

Network Detection and Response (NDR) systems can help detect and prevent data exfiltration by monitoring network traffic for suspicious activities, such as large or unusual data transfers, and alerting security teams to potential threats. Specifically, NDR can play a crucial role in securing sensitive patient data.

- **Real-time Threat Detection:** NDR continuously monitors network traffic for suspicious activity, detecting unauthorized access attempts and exfiltration of sensitive patient data.
- **Anomaly Detection:** Using advanced correlation and analytics, NDR can identify unusual patterns of data access or transfer that may indicate insider threats or external breaches.
- **Incident Response & Evidence:** NDR provides deep visibility into network activity, helping security teams quickly trace and respond to potential data breaches before attackers can monetize stolen data.



Reliance on Interconnected Partners and Systems

Modern healthcare heavily relies on a complex network of interconnected systems, creating a significant cybersecurity challenge. Electronic health records (EHRs), medical devices, billing systems, and other critical applications are increasingly interconnected, forming a vast and intricate network.

The increasing reliance on interconnected systems within healthcare organizations significantly expands the attack surface and increases the potential for cyberattacks. As noted in the American Hospital Association's report, *Current and Emerging Healthcare Cyber Threat Landscape*, "The interconnected nature of modern healthcare systems, including electronic health records (EHRs), medical devices, and billing systems, creates a complex and vulnerable environment."

This interconnectedness allows attackers to move laterally within the network, potentially compromising multiple systems and disrupting critical operations. A breach in a single point within this network can have cascading effects, impacting patient care, financial stability, and the overall reputation of the healthcare organization.

How NDR Can Help

NDR systems can provide visibility into the entire network, allowing security teams to identify and respond to threats that may be moving laterally across the network. Specifically, NDR can play a crucial role in protecting interconnected systems.

- **Network Visibility & Segmentation:** NDR maps traffic flows across interconnected healthcare systems, helping identify weak points and enforce segmentation policies to prevent lateral movement.
- **Threat Intelligence Integration:** By correlating network events with threat intelligence, NDR can detect known attack vectors targeting interconnected IT and OT (Operational Technology) environments.
- **Automated Response:** NDR can integrate with endpoint detection and response (EDR) and security orchestration tools (SOAR, XDR, SIEM) to isolate compromised systems and prevent infections from spreading across interconnected hospital networks.



Regulatory Compliance

Hospitals and healthcare organizations face stringent regulatory requirements to safeguard patient data and protect against evolving cyber threats. With compliance mandates such as HIPAA, HITRUST, GDPR, NIS2, NHS DSP Toolkit as well as cybersecurity guidance for medical devices from FDA and MDR, hospitals must adopt proactive security solutions.

While the Health Insurance Portability and Accountability Act (HIPAA) sets a benchmark in the United States, similar data protection laws are proliferating across the globe. The European Union's General Data Protection Regulation (GDPR) establishes stringent requirements for data privacy and security, impacting any organization that processes the personal data of EU residents. In Asia, countries like Singapore (Personal Data Protection Act

- PDPA) and Japan (Act on the Protection of Personal Information - APPI) have enacted comprehensive data protection frameworks. Latin American nations are also increasingly adopting data privacy regulations, reflecting a global trend towards stronger data protection standards.

In addition, regulatory compliance extends beyond traditional data protection. Medical devices, integral to modern patient care, introduce a unique layer of complexity. Healthcare organizations must navigate the intricate landscape of medical device compliance, governed by bodies such as the U.S. Food and Drug Administration (FDA) and the European Union's Medical Device Regulation (MDR). These regulations emphasize both the safety and cybersecurity of medical devices, demanding rigorous risk assessments, post-market surveillance, and adherence to evolving cybersecurity guidance. In this landscape,

Meeting these regulatory demands presents numerous challenges. The dynamic nature of regulations requires continuous monitoring and adaptation of security practices.

How NDR Can Help

Regulatory compliance is not merely a checkbox, but an ongoing imperative.

Network Detection and Response (NDR) systems offer a critical layer of defense, providing capabilities that directly address key compliance mandates. By offering continuous monitoring of Protected Health Information (PHI), enabling rapid incident detection and response, securing vulnerable medical devices, facilitating detailed audits and forensics, and addressing third-party and supply chain risks, NDR solutions empower healthcare organizations to meet the stringent requirements of HIPAA, GDPR, PCI, FDA, MDR regulations, NIS and NIST frameworks, HITRUST, and other vital compliance standards.

- **Continuous Monitoring for Protected Health Information (PHI:** Security and regulatory frameworks like HIPAA and GDPR require healthcare entities to protect electronic Protected Health Information (ePHI). NDR solutions continuously monitor network traffic to detect unauthorized access, data exfiltration attempts, and insider threats.
- **Incident Detection and Response to Meet Reporting Requirements:** The HIPAA Breach Notification Rule and HITRUST standards mandate timely detection and reporting of security incidents. NDR systems use multiple detection technologies such as anomaly

detection and behavioral analysis to identify breaches early and trigger automated responses, minimizing damage and response time.

- **Securing Medical Devices to Align with FDA, MDR, and HITECH Act Regulations:** Connected medical devices (IoMT) are prime cyberattack targets. The FDA recommends proactive risk management to ensure device security. NDR systems monitor traffic to and from medical devices, detecting vulnerabilities, unauthorized access, and malicious activity.
- **Enabling Audit and Forensics Capabilities for Regulatory Investigations:** Healthcare organizations must maintain detailed logs of security incidents to comply with regulations. NDR solutions provide deep forensic capabilities, allowing security teams to analyze threats and generate automated compliance reports.
- **Addressing Third-Party and Supply Chain Risks for NIS2, NIST and HITRUST Compliance:** Hospitals rely on third-party vendors, increasing the risk of supply chain attacks. NDR solutions monitor east-west traffic, detecting unauthorized movements within the network and preventing lateral attacks..



Rapid Pace of Technological Advancements

The rapid pace of technological advancements in healthcare introduces new cybersecurity challenges and vulnerabilities. The emergence of technologies such as telemedicine, the Internet of Medical Things (IoT), and artificial intelligence (AI) offers significant opportunities for improved patient care but also presents unique security risks.

For example, the widespread adoption of IoT devices in healthcare settings, such as connected medical devices and wearable health trackers, expands the attack surface and increases the potential for data breaches.

The integration of AI and machine learning algorithms into healthcare systems raises concerns about data privacy, algorithmic bias, and the potential for manipulation. As the World Health Organization (WHO) emphasizes in its report, "Artificial intelligence in health," the increasing use of AI and machine learning algorithms in healthcare raises concerns about data privacy, algorithmic bias, and the potential for manipulation. These advancements necessitate a continuous and proactive approach to cybersecurity, requiring healthcare organizations to adapt their security strategies to address emerging threats and vulnerabilities.

How NDR Can Help

NDR systems can adapt to new technologies and threats by continuously monitoring network traffic for emerging patterns and anomalies. Specifically, NDR can play a crucial role in protecting interconnected systems.

- **Adaptive Security Posture:** NDR solutions use machine learning to adapt to evolving network behaviors, ensuring new technologies and workflows are monitored without requiring constant manual updates.
- **Zero Trust Verification:** By continuously verifying all network communications, NDR helps enforce Zero Trust principles, even as new medical technologies and applications are introduced.



Increasing Connectivity of Unprotected Medical Devices

The increasing connectivity of medical devices presents a significant cybersecurity challenge, particularly for devices that were not designed with security as a primary consideration. Many older medical devices lack robust security features, making them vulnerable to exploitation by cybercriminals.

These devices can be compromised to manipulate treatment parameters, disrupt critical functions, or even steal sensitive patient data. Furthermore, the integration of these devices into hospital networks can introduce new vulnerabilities, particularly if proper security protocols are not in place. Addressing these challenges requires a multi-pronged approach, including the development of secure medical device design standards, the implementation of robust security controls for connected devices, and the regular assessment and remediation of vulnerabilities.

The increasing connectivity of medical devices presents a significant challenge, as many older devices were not designed with cybersecurity as a primary consideration. As highlighted by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), "Medical devices are increasingly connected to hospital networks, creating new vulnerabilities and potential attack vectors for cybercriminals." These devices, often lacking

robust security features, can be exploited to manipulate treatment parameters, disrupt critical functions, or even steal sensitive patient data. This underscores the critical need for medical device manufacturers to prioritize cybersecurity in the design and development process, incorporating security features from the outset.

In fact, there are numerous Common Vulnerabilities and Exposures (CVEs) associated with medical devices. Many of these vulnerabilities arise from outdated software, weak authentication mechanisms, unencrypted communications, or a lack of security updates.

Here are a few examples:

- CVE-2024-10412 - A cross-site scripting vulnerability in the Poco-z Guns-Medical 1.0 application, which could be exploited remotely
- *CVE-2024-10301* - A critical SQL injection vulnerability found in PHPGurukul Medical Card Generation System, making it possible to launch an attack remotely.
- *CVE-2022-26393* – Found in Baxter Spectrum Infusion System's Wireless Battery Module (WBM) infusion pumps, allowing remote attackers to modify medication dosages.
- *CVE-2021-27410* – A vulnerability in a widely used Welch Allyn patient monitoring system, allowing unauthorized remote access.
- *CVE-2020-25179* – A flaw in a connected GE Healthcare Imaging and Ultrasound products that could allow specific credentials to be exposed during transport over the network.

The common issues leading to medical device CVEs include:

- **Lack of Encryption:** Many older medical devices transmit data without proper encryption, making them vulnerable to interception.
- **Hardcoded Credentials:** Some devices ship with default or hardcoded passwords that are easy for attackers to exploit.
- **Delayed Patching:** Many medical devices run on legacy operating systems that no longer receive security updates.

When these devices are compromised, it can pose significant risks to patient safety. Therefore, it's crucial for healthcare organizations to stay informed about current vulnerabilities and implement robust cybersecurity monitoring and controls to protect both devices and patient data.

How NDR Can Help

NDR systems can help detect and respond to threats originating from medical devices by monitoring network traffic for unusual communication patterns or behaviors. Specifically, NDR can play a crucial role in monitoring and securing networks containing medical devices and other systems that cannot be guarded by other security controls.

- **IoT & Medical Device Monitoring:** NDR detects anomalous behavior in connected medical devices, such as unusual data transmissions or unauthorized remote access.
- **Device Profiling & Risk Assessment:** By identifying unmanaged or vulnerable devices as well as the use of weak encryption or other insufficient controls, NDR enables security teams to prioritize remediation efforts and apply compensating controls.
- **Threat Containment:** If an NDR system detects activity associated with a compromised medical device, it can trigger an automated escalation response such as opening a ticket in a rapid response system. Optionally, in an extreme case, the NDR could even initiate a quarantine action, isolating the device from the network to prevent further damage.



Limited Resources and the Human Element

Limited resources and the human element pose significant challenges for cybersecurity teams in healthcare organizations. Many healthcare organizations face budget constraints, making it difficult to invest in adequate cybersecurity measures, such as hiring skilled cybersecurity professionals, implementing robust security technologies, and conducting regular security assessments. Furthermore, staffing shortages can exacerbate these challenges, limiting the ability of organizations to effectively manage and respond to cyber threats.

Additionally, the human element plays a critical role in cybersecurity. Phishing attacks, social engineering techniques, and accidental data disclosure by employees can all lead to security breaches. Addressing these challenges requires a multifaceted approach, including employee training and awareness programs, robust access controls, and a strong cybersecurity culture that emphasizes the importance of security at all levels of the organization.

Limited resources and the human element pose significant challenges for healthcare organizations in their efforts to combat cyber threats. As noted in the HIMSS Cybersecurity Framework, "Many healthcare organizations struggle to adequately invest in cybersecurity due to budget constraints and staffing shortages." This lack of resources can hinder the ability to implement robust security measures, hire skilled cybersecurity professionals, and conduct regular security assessments. Furthermore, human error, such as accidental data disclosure or the misuse of employee accounts, can significantly impact an organization's security posture.

Source: HIMSS Cybersecurity Framework (https://gkc.himss.org/news/cybersecurity-framework-implementation-guide-helps-healthcare-organizations-manage-risks

How NDR Can Help

NDR systems can help automate the detection and response process, freeing up security teams to focus on other critical tasks. Additionally, NDR systems can provide valuable insights into the threat landscape, allowing security teams to prioritize their efforts and allocate resources more effectively.

- **Automated Threat Detection & Response:** Through integration with other systems in your security tech stack, NDR reduces the burden on understaffed security teams by automating detection, alert triage, and response actions.
- **Prioritized Alerts & Incident Response:** Instead of overwhelming analysts with alerts, NDR prioritizes threats based on severity and risk, allowing teams to focus on the most critical incidents.
- **Advanced Behavioral Analytics:** NDR monitors for insider threats and compromised accounts by identifying deviations from normal network and user activity, reducing the risk of human errors leading to security breaches.

INTRODUCING CLEAR NDR™

Clear NDR™ from Stamus Networks delivers transparent, multi-layered network security that has proven its effectiveness in protecting some of the world's most critical enterprises and organizations, including hospitals and insurance companies.



Clear NDR's strength lies in its four fundamental capabilities that address the unique security needs of healthcare organizations:

Clear Visibility – monitor activities across your entire attack surface — so you won't miss threats that evade your other controls

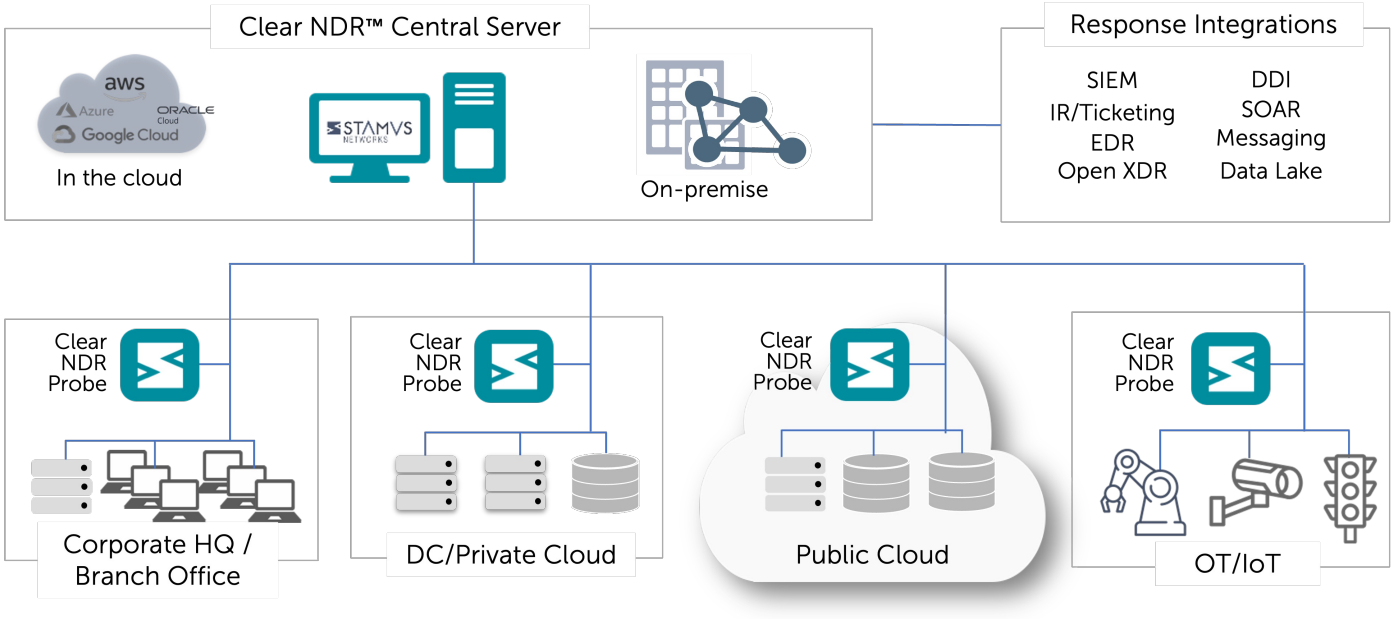
Clear Detection – multi-layer, transparent detections you can understand — so you can accelerate your triage and response

Clear Evidence – detailed attack timeline and complete evidentiary artifacts — so you can quickly resolve the incident

Clear Response – ultra high-fidelity threat declarations - so you have confidence you need to automate response

Implementation is streamlined through flexible deployment options — including cloud, on-premise, and hybrid environments — with immediate threat monitoring capabilities upon installation.

Clear NDR complements and connects with existing security infrastructure through ready-to-deploy SOAR, XDR, and EDR platform integrations, ensuring that financial institutions can maintain operational continuity while enhancing their security posture



HOW CLEAR NDR ADDRESSES HEALTHCARE CHALLENGES

With the ongoing threat of ransomware, medical IoT threats, and compliance challenges, hospitals need full visibility into their networks. Clear NDR delivers advanced detection, automated threat declaration, and seamless integration—empowering your team to prevent, detect, and respond to threats before they impact patient safety.

Clear NDR uniquely addresses key challenges facing hospitals and healthcare organizations:



High Value of Patient Data on the Black Market

- Clear NDR continuously monitors network traffic for suspicious activity, detecting unauthorized access attempts and exfiltration of sensitive patient data.
- Clear NDR can identify unusual patterns of data access or transfer that may indicate insider threats or external breaches.
- Clear NDR provides deep visibility into network activity, helping security teams quickly trace and respond to potential data breaches before attackers can monetize stolen data.



Reliance on Interconnected Partners and Systems

- Clear NDR can monitor all network segments, including vendor access points, and can detect anomalous activities originating from third parties.
- Clear NDR maps traffic flows across interconnected healthcare systems, helping identify weak points and enforce segmentation policies to prevent lateral movement.
- By correlating network events with threat intelligence, Clear NDR can detect known attack vectors targeting interconnected IT and OT (Operational Technology) environments.
- Clear NDR can integrate with endpoint detection and response (EDR) and security orchestration tools (SOAR, XDR, SIEM) to isolate compromised systems and prevent infections from spreading across interconnected hospital networks.



Regulatory Compliance

- Clear NDR continuously monitors network traffic to detect unauthorized access, data exfiltration attempts, and insider threats.
- Clear NDR uses multiple detection technologies such as anomaly detection and behavioral analysis to identify breaches early and trigger automated responses, minimizing damage and response time.
- Clear NDR monitors traffic to and from medical devices, detecting vulnerabilities, unauthorized access, and malicious activity.
- Clear NDR collects and organizes extensive evidence associated with incidents, allowing security teams to analyze threats and generate automated compliance reports.
- Clear NDR monitors east-west traffic, detecting unauthorized movements within the network and preventing lateral attacks.



Rapid Pace of Technological Advancements

- Clear NDR uses machine learning and other detection technologies to adapt to evolving network behaviors, ensuring network changes, new technologies, and workflows are monitored without requiring constant manual updates.
- Clear NDR helps enforce Zero Trust principles, even as new medical technologies and applications are introduced.



Increasing Connectivity of Unprotected Medical Devices

- Clear NDR detects anomalous behavior in connected medical devices, such as unusual data transmissions or unauthorized remote access.
- By identifying unmanaged or vulnerable devices as well as the use of weak encryption or other insufficient controls, Clear NDR enables security teams to prioritize remediation efforts and apply compensating controls.
- If Clear NDR detects activity associated with a compromised medical device, it can trigger an automated escalation response such as opening a ticket in a rapid response system. Optionally, in an extreme case, Clear NDR could even initiate a quarantine action, isolating the device from the network to prevent further damage.



Limited Resources and the Human Element

- Clear NDR detects anomalous behavior in connected medical devices, such as unusual data transmissions or unauthorized remote access.
- By identifying unmanaged or vulnerable devices as well as the use of weak encryption or other insufficient controls, Clear NDR enables security teams to prioritize remediation efforts and apply compensating controls.
- If Clear NDR detects activity associated with a compromised medical device, it can trigger an automated escalation response such as opening a ticket in a rapid response system. Optionally, in an extreme case, Clear NDR could even initiate a quarantine action, isolating the device from the network to prevent further damage.
- Through integration with other systems in your security tech stack, Clear NDR reduces the burden on understaffed security teams by automating detection, alert triage, and response actions.
- Clear NDR prioritizes threats based on severity and risk, allowing teams to focus on the most critical incidents.
- Clear NDR monitors for insider threats and compromised accounts by identifying deviations from normal network and user activity, reducing the risk of human errors leading to security breaches.

SECURING THE FUTURE OF HEALTHCARE

As cyber threats continue to evolve, and regulatory requirements become more stringent, hospitals and healthcare organizations must adopt security solutions that provide both comprehensive protection and operational efficiency. Hospital and healthcare's unique position at the heart of global health and wellness infrastructure demands security solutions that can adapt to emerging threats and help maintain the operational resilience you depend on.

Network Detection and Response technology has proven to be highly capable of meeting these challenges, providing the visibility, detection capabilities, and automated response mechanisms needed to protect critical healthcare systems.

By providing deep network visibility, real-time threat detection, and automated response capabilities, NDR systems significantly enhance the security posture of hospitals and healthcare organizations, helping them defend against evolving cyber threats.

Clear NDR™ takes these capabilities further, delivering transparent, multi-layered protection that enables truly autonomous security operations.

The stakes have never been higher for hospitals and healthcare, with cyber incidents capable of causing billions in damages and disrupting critical health functions. Clear NDR provides the technology foundation needed to face these challenges, combining proven success in the critical infrastructure with innovative capabilities that address both current and emerging threats.

CONTACT STAMUS NETWORKS TODAY

Clear NDR™ from Stamus Networks delivers transparent, multi-layered network security that has proven its effectiveness in protecting some of the world's most critical infrastructure, financial institutions, major insurance providers, hospitals and healthcare organizations.


Hospitals and Healthcare


Central Banks


Government Institutions


Educational Institutions


Insurance Providers


Critical Infrastructure


Financial Institutions


Government CERTs

Don't wait until a breach forces change. Clear NDR serves as the ultimate source of truth, enhancing your security posture and transforming healthcare defense against modern threats. Schedule a demo today to see how Clear NDR can enhance your organization's security posture and streamline security operations. Our engineers are ready to demonstrate how Clear NDR can strengthen your defenses today: contact@stamus-networks.com

ABOUT STAMUS NETWORKS

Stamus Networks believes that cyber defense is bigger than any single person, platform, company, or technology. That's why we leverage the power of community to deliver the next generation of open and transparent network defense. Trusted by security teams at the world's most targeted organizations, our flagship offering – Clear NDR™ – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Clear NDR helps defenders see more clearly and act more confidently through detection they can trust with results they can explain.

STAMUS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com

Copyright © 2025