



# Armis Centrix™ for Early Warning for Healthcare

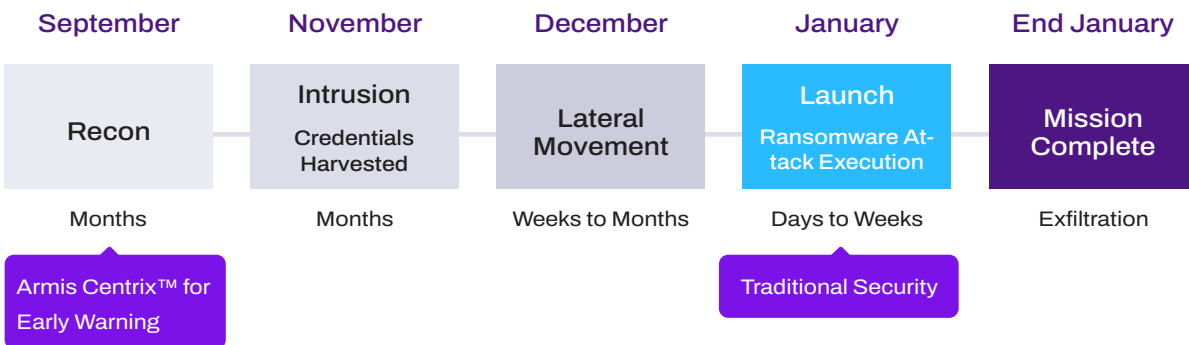
Take a proactive approach to the threat before it impacts your organization. Revolutionary AI technology and machine learning algorithms that leverages dark web, smart honeypots and HUMINT to stop attacks before they impact your organization and protect critical assets with confidence.

## Redefining Healthcare Security by Preempting the Attack

Protect essential patient care services with enhanced attack surface visibility and prevention. Armis Centrix™ for Early Warning empowers you with proactive intelligence to anticipate threats, understand their potential impact, and take preemptive action to neutralize them, effectively moving the security posture from defense to offense.

## Protect Against Ransomware Attacks with Proactive Vulnerability Intelligence

With Armis Centrix™ for Early Warning, you can ensure your healthcare organization is always leveraging the most up-to-date protection. Transcend traditional security measures and proactively identify preparatory indicators of attacks and exploits.



## Protect Against and Prevent Healthcare Cyberattacks with Armis Centrix™ for Early Warning Use Cases:

### Leverage AI-powered Early Warning Intelligence

to anticipate threats, understand their potential impact, and take preemptive action to neutralize them, effectively moving the security posture from defense to offense.

### Protect Against Weaponized Threats

by understanding the global attack surface and real-time hacker behaviors and techniques on other healthcare environments.

### Preempt Threat Actors

and stop them before they impact your organization, thanks to HUMINT and AI intelligence, scouring dark web chatter.

### Detailed Analysis of Ransomware Attacks

including intelligence on what credentials and hacking tools are being sold and leveraged.

### Address Ongoing Vulnerabilities

that are actually being exploited by threat actors with Armis Labs intelligence, listening posts, trends, and expertise.

### Preventive Security Guidelines

to notify of potentially exploitable vulnerabilities or faults and begin remediation workflows before an attack happens.



# Key features that make Armis the go-to platform for Total Exposure Management.

**Early Warning** included with Armis Centrix™ allows you to leverage our dark web insights, AI-powered pre-attack threat hunting, and create an early warning system.

**AI Capabilities** that can predict attack behavior, tactics, and likely targets; with proactive adjustment to each customer’s needs and current threat environment.

**Notifications** of impending threats via the channels you use within your organization.

**Smart Honeypots** crafted for healthcare environments and other deception technologies to learn hacker behaviors and techniques.

**Human Intelligence Integration** leveraging advanced listening posts to scour Telegram channels, the dark web, and attacker forums for actionable intelligence and reverse engineering attacks.

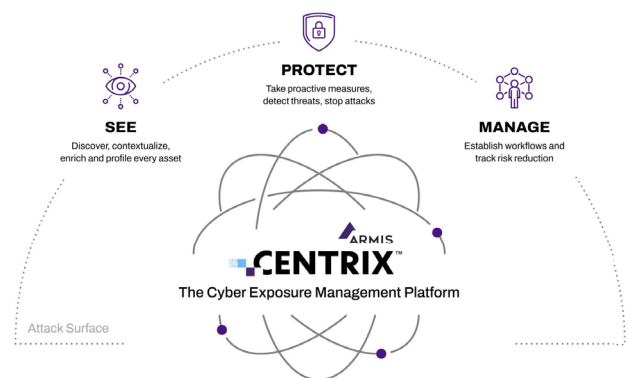
**Machine Learning** of current methods and tactics being discussed to understand the context of the conversation and identify the threat for contextual risk determination.

**Integration with existing tech stacks**, enabling a comprehensive and cooperative view across the security stack.

**Dashboards** give your teams the information most important to their work, reducing the overall clutter.

# Why Healthcare Organizations Trust Armis to Deliver Better Outcomes

- 1 Superior Threat Detection. 98% reduction in the number of threats organizations need to worry about with early warning detection.
- 2 Reduced Clinical Risk with significantly improved security posture and preventive security maintenance.
- 3 Reduce Attack Likelihood and minimize clinical disruptions and impacts to patient care.
- 4 Accurate Reconciliation allows for faster time-to-remediation and instantly identify affected assets, for 20-40x fewer patches and outages.
- 5 Reputation and Trust. Healthcare organizations using Armis are industry leaders upholding best cybersecurity practices.
- 6 Speed of Deployment is critical in healthcare environments where quick resolution and reduction of patient risk is a top priority.
- 7 Optimized Medical Device Utilization. Time and usage statistics help determine better maintenance schedules, avoiding downtime and facilitating efficient patient scheduling.



Intelligence Centre	Dynamic Honeypots
Dark Web	HumINT

