VECTRA
SECURITY THAT THINKS.®

CASE STUDY

International Private Healthcare Group Achieves Real-Time Threat Detection

With more than a 100 hospitals and clinics globally, an international private healthcare group decided to use artificial intelligence to tackle the challenges of timely detections and effectively manage active cyberattacks to reduce their cyber risk.

The attack on healthcare

The healthcare industry today increasingly delivers patient care centered around science-based knowledge and expertise, innovative technology, and empathetic clinicians. At the same time, healthcare providers must ensure that their operations, data and patients are protected from the growing threat of cybercrime.

Sophisticated hackers target their victims and have a wide range of advanced attack techniques and tools at their disposal. Healthcare providers have been a favorite target for ransomware attacks, in which all healthcare data on the network is encrypted until a ransom is paid.

Cybercriminals also attempt to disrupt clinical services by exploiting backdoors in vulnerable internet-of-things (IoT) medical devices such as imaging systems, drug infusion pumps, monitors and pacemakers.

Once attackers evade network perimeter defenses and controls, they often go after patient records that contain substantial amounts of private and sensitive information. Harvesting and selling them in darknet markets can be an extremely profitable activity for criminal groups.

In addition to the risk of data loss, ransomware attacks have the potential to disrupt and deny control over key digital services like biomedical devices and vital systems, putting the provider and the safety of patients at risk.

> “Cognito detects and prioritizes in-progress attacks that pose a very real danger to the key assets we must protect”
>
> **Group Security Architect**
> *International Private Healthcare Group*

Organization

International Private Healthcare Group

Industry

Healthcare

Challenge

Timely detection, understanding and management of active cyberattacks

Selection criteria

Nonstop automated threat surveillance that deploys easily and integrates with existing security tools

Results

- 360-degree visibility into cyberattackers in the network
- Integrates with existing security technologies and processes
- Faster threat detection and response across global locations
- Meets healthcare patient data protection regulations

> “Cognito proved its value from Day 1. After a short period of machine learning across our network, Cognito immediately detected a threat and notified our security team about an attack”
>
> **Group Security Architect**
> *International Private Healthcare Group*

Defense alone was not enough

Most healthcare organizations have robust cybersecurity protections in place, but this healthcare group realized it needed to expand its ability to quickly spot and manage attacks, and was mindful of the rapidly evolving threat landscape.

The security team knew traditional signature-based approaches could only detect know threats, yet at the same time attacks that can cause the most damage are often targeted at victim organizations and largely unknown and customized by attackers.

With a growing number of digital connections to clinical systems and the risk of IoT medical devices, actionable insight into attacker behaviors was needed to detect and respond fast.

Proactively closing the gap

To narrow its detection window and accelerate incident response, the organization identified the Cognito network detection and response platform from Vectra. After an intensive product evaluation – including a battery of simulated attacks and brute force attempts – Vectra proved it had the key capabilities to solve this challenge.

Cognito appealed to the security team for a number of reasons, including its resiliency, success under testing, the simplicity of the user interface, and the quality of insight it generated.

Using artificial intelligence, Cognito automates the hunt for hidden cyberattacks inside networks, data centers and the cloud, and detects active threats in real time with always learning behavioral models. Cognito provides high-fidelity visibility into the entire network as well as all applications, operating systems and devices, including BYOD and IoT.

The security team also valued Cognito’s ability to automatically prioritize detected threats that pose the highest risk, correlate threats with hosts that are under attack, and provide unique context about what attackers are doing and where they are hiding.

Immediately stopped an attack

“Cognito proved its value from Day 1. After a short period of supervised and unsupervised machine learning across our entire network, Cognito immediately detected a threat and notified our security team about an attack,” said their group security architect.

Cognito’s ability to continuously monitor all network traffic, while at the same time prioritize the highest-risk threats with a high degree of certainty gave the security team a confident approach to automating threat surveillance.

“Other solutions only classify behaviors as normal or abnormal. Instead of wasting time on ambiguous security events, Cognito detects and prioritizes in-progress attacks that pose a very real danger to the key assets we must protect,” their group security architect continued.

An easy fit with the security ecosystem

The security team wanted a cybersecurity platform that would work with its other security technologies. Cognito easily integrates with next-generation firewalls, endpoint detection and response and other enforcement points to automatically block unknown and customized cyberattacks.

Cognito provided the security team a simple and straightforward installation, using a non-disruptive out-of-band approach that didn’t require a massive effort to integrate with the company’s current security infrastructure.

Additionally, Cognito gave the security team a clear and definitive starting point to launch deeper threat investigations, which accelerates the efficiency of its SIEM and forensic analysis tools.

Prepared for anything

With Cognito, this healthcare provider significantly reduced the time it takes to detect and respond to threats and has brought consistency to its global cybersecurity operations. The result is an overall security capability that moved from reactive to proactive.

Being an international care provider requires a consistent approach to cybersecurity, which can be a real challenge. Especially under the deadline pressures of compliance with the EU General Data Protection Regulation and other regulatory mandates.

However, with Cognito the company was enabled to establish a consistent approach to cyberattacker detection and incident response worldwide as well as expedite compliance with security and privacy protection regulations.

Cognito gives consistent, real-time visibility to detect and respond to cyberattack regardless of location. Allowing for a quicker, faster response time.

Looking ahead

With Cognito automating the hunt for cyberattacks, detecting threats in real time and speeding-up incident response, the company's security team can focus on the most important parts of the job: threat mitigation, regulatory compliance and safeguarding patient privacy.

With Cognito automating the hunt, the company's security team can focus on threat mitigation, regulatory compliance and safeguarding patient privacy.

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai