Case Study

VECTRA
Security that thinks®

International private hospital group

Mediclinic International uses artificial intelligence to reduce cyber risk

With 73 hospitals and 43 clinics worldwide, Mediclinic International is a fast-growing private hospital group with operations in South Africa, Namibia, Switzerland and the United Arab Emirates. Mediclinic also holds a significant stake in the UK private healthcare group Spire 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. Hospitals have been a particular favorite target for ransomware attacks, where 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. IoT-enabled medical devices can include 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.

Defense alone was not enough

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

MEDICLINIC
INTERNATIONAL

Organization
Mediclinic International

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

For this task Mediclinic recognized that traditional signature-based approaches could only detect known threats, yet at the same time attacks that can cause the most damage are often targeted at victim organizations and are largely unknown and customized by attackers.

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

Proactively closing the gap

To narrow its detection window and accelerate incident response, Mediclinic considered the Cognito™ cyberattack detection and threat hunting platform from Vectra®. After an intensive product evaluation – including a battery of simulated attacks and brute-force attempts – Mediclinic chose Vectra.

"Cognito appealed to the security team for many reasons, including its resiliency, success under testing, the simplicity of the user interface, and quality of insight it generates," said Marais Coetzee, group security architect at Mediclinic.

Using artificial intelligence, Cognito automates the hunt for hidden cyberattackers 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.

Mediclinic 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," said Coetzee. "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 at one of our regional hubs."

"We were very impressed with Cognito's ability to continuously monitor all network traffic while at the same time prioritize the highest-risk threats with the greatest degree of certainty," said Coetzee.

"Other solutions only classify behaviors as normal or abnormal," he added. "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."

An easy fit with the security ecosystem

The Mediclinic 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 was simple to install and didn't require a massive effort to integrate with our security infrastructure," said Coetzee. "The implementation was straightforward and its out-of-band approach is non-disruptive."

Additionally, Cognito provides the Mediclinic security team with 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, Mediclinic 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.

"As an international care provider, maintaining a consistent approach to cybersecurity can be a real challenge, especially under the deadline pressure of complying with the General Data Protection Regulation and other regulatory mandates," Coetzee said.

However, Cognito enabled Mediclinic 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 us consistent, real-time visibility to detect and respond to cyberattacks, no matter where they occur," said Coetzee. "The quality of this instant feedback allows us to respond faster and more decisively."

Looking ahead

With Cognito automating the hunt for cyberattackers, detecting threats in real time and speeding-up incident response, the Mediclinic security team can focus on threat mitigation, regulatory compliance and safeguarding patient privacy.

"Cognito is crucial to keeping our patients and networks safe and healthy," Coetzee concluded.

> *"Cognito proved its value from Day 1."*
>
> Marais Coetzee
> Group Security Architect
> Mediclinic International

VECTRA®
Email: info@vectra.ai
Tel: 1 408-326-2020
vectra.ai