CASE STUDY

Australian Private Health Fund Gains Full Visibility Using Vectra

Ensuring a lifetime of health and wellbeing of families is a big responsibility, especially today where in addition to prioritizing physical healthcare needs, cyber hygiene for everyone continues to be an area of concern. This is exactly why the Digital Operations Manager at an Australian Private Health Fund, stays proactive in his approach to cybersecurity by prioritizing visibility across the organization's environment to ensure the cyber wellness of members isn't compromised.

Operating as a non-profit company for nearly 50 years, this Australian Private Health Fund is focused on making healthcare stress-free for members, leaving no room for the risk of any member's information being compromised in a cyberattack. One of the ways their security team ensures that members remain protected online is with the Vectra AI-based network detection and response platform so they can leverage real time threat detections and gain a clear understanding about any potential threat activity or security incident.

> "It has given us an increased level of confidence in our information security, that we have a tool like Vectra."
>
> **Digital Operations Manager**
> *Australian Private Health Fund*

Organization

Australian Private Health Fund

Industry

Healthcare

Challenge

Needed a new solution that would replace Darktrace and reduce their number of alerts

Selection criteria

Selecting Vectra as their preferred network detection and response (NDR) solution for its ability to monitor hybrid environments, increase visibility and reduce unnecessary alerts

Results

- Now receive 80% less critical alerts
- Can combine on-prem packet data that they were watching with the cloud data
- Have a deeper understanding of each anomaly and increased level of confidence in their information security

By taking this approach, they are not only able to eliminate the security risks posed by potential outside threats but also reduce overwhelming security alerts and quickly spot unusual employee behavior that could result in possible vulnerabilities. In addition, Vectra helps the security team at the Australian Private Health Fund align policy enforcement with the pre-planned controls they've identified for any possible security risk.

Returning from the Dark Side

Before deploying Vectra, the Australian Private Health Fund was using Darktrace. They decided to reevaluate the deployment to determine if another solution was a better fit and ultimately selected Vectra as their preferred network detection and response (NDR) solution for its ability to monitor hybrid environments, increase visibility and reduce unnecessary alerts.

“One of the main things that Vectra has brought to the table for us, over what we were previously using, was the ability to combine our on-prem packet data that we were watching with the cloud data that we needed to start including,” says the Operations Manager.

Detect uses AI machine learning models to deliver real-time attack visibility and make attack details easily accessible. “With Vectra AI, it is all about combining the detections and getting a more complete picture,” the Operations Manager explains. “When you are looking for more than just one indicator of compromise, and you are not viewing these things in isolation, you start to realize that one indicator oftentimes doesn't mean critical. That is what Vectra does pretty well.”

The security team has found that the threats Vectra places in high priority align with what they would consider critical as a business, compared to the high risk triggers they previously received, reducing alert fatigue. “For critical alerts, there has been a huge reduction compared to our previous solution, approximately 80% less,” the Operations Manager notes.

“For critical alerts, there has been a huge reduction compared to our previous solution, 80% less.”

Digital Operations Manager
Australian Private Health Fund

Seeing A Clear Path

Detect applies AI-derived machine learning algorithms to automatically detect and respond to in-progress cyberattack behaviors in cloud/SaaS, data center, IoT, and enterprise networks.

“Because it provides more context and raises things in a way that make it more actionable, it does help you understand the anomaly on a deeper level,” states the Operations Manager.

“The analysts at the SOC have more information to work from, it has reduced wasted time and improved the path that we are taking to a resolution, if there is a problem,” continues the Operations Manager.

Visibility into the whole attack lifecycle gives the entire team confidence that they can shut down attacks and prevent further risks and damage across their entire environment. The time it takes for this team to sort through and review alerts can now be spent investigating and resolving high-risk anomalies.

By triaging threats and correlating them with compromised host devices, “Vectra AI has done a lot to reduce the noise and combine multiple detections into more singular or aggregated alerts that we can then investigate.”

Securing All Around

The security team at the Australian Private Health Fund has also deployed Detect for O365 to monitor their O365 environment. Detect for Office 365 ingests activity logs from multiple Office 365 SaaS services like Azure Active Directory, SharePoint, OneDrive, Exchange, and Teams.

With a deep understanding of Office 365 application semantics, Detect for Office 365 applies AI-derived machine learning algorithms to proactively detect and respond to hidden cyberattackers and stop data breaches.

To identify credential abuse and account takeovers, Detect for Office 365 analyzes malicious behavior patterns in logins, file creation and manipulation, data loss protection configuration, and mailbox routing configuration and automation changes.

With greater trust in their security tools, they can efficiently keep their environment safe. “It has given us an increased level of confidence in our information security, that we have a tool like Vectra to back up some of the incidents that could take place,” says the Operations Manager.

> “[Vectra] has reduced wasted time and improved the path that we are taking to a resolution.”
>
> **Digital Operations Manager**
> *Australian Private Health Fund*

For more information please contact us at sales-inquiries@vectra.ai.

Email info@vectra.ai vectra.ai