VECTRA
SECURITY THAT THINKS.®

CASE STUDY

AI put threats in the can

Metal and glass packaging maker Ardagh Group finds and stops hidden attackers

If you have ever popped open a frosty beverage, peeled back the lid of a can of tasty tuna or spiced up your meal with hot sauce, chances are you've encountered the Ardagh Group.

The Ardagh Group makes metal and glass packaging for the world's biggest brands. It's a leader in sustainable business, and the company has grown rapidly in the last several years. It produces 35 billion containers a year for food, beverages, spirits and pharmaceuticals.

Protecting a global business

The Ardagh Group operates more than 100 metal and glass manufacturing facilities in 22 countries. As a highly distributed company, the Ardagh Group is both agile and efficient, but its reach also creates risk that must be managed.

"Our challenges are geographical," says David Whelan, group IT director at the Ardagh Group.

The Ardagh Group network is well-secured – firewalled, protected against intrusions, and highly segmented. Endpoints are protected. Threat intelligence provides advanced warning.

But in an era where mobile and cloud have shattered perimeter defenses and sensitive information is spread across the world, traditional security is not enough. The IT security team needs clear visibility into in-progress attacks that have slipped past its well-crafted defenses.

ArdaghGroup

Organization

The Ardagh Group

Industry

Manufacturing

Challenge

Find hidden and unknown attackers in its geographically-dispersed global operations network

Selection criteria

AI-powered threat detection platform that keeps pace with the evolving threat landscape

Results

- Conclusively detect hidden threats, especially attacks targeting executives and payments
- Gain visibility into the normal patterns of network traffic worldwide
- Reduce threat investigation workload by automating manual, time-consuming attacker detection

"With Cognito, we can stop threats before they cause damage."

David Whelan
Group IT Director
The Ardagh Group

"If someone has access to one of our workstations in London, they might as well be in the head office in Dublin," Whelan says. "The network is highly segmented, but employees also have necessary access to shared applications and services."

Cloud apps further complicate cybersecurity. "Moving to Office 365 creates a different set of challenges," he says. "You don't have the same visibility that you do on your own network. It's no longer within your direct control to see risk."

AI-powered threat hunting

AI-powered threat hunting Automation and AI are critical for cybersecurity, contends Whelan. "If there are automated techniques in an attack, you must automate your defenses," he says.

Whelan and his team conducted a proof-of-concept test of the Cognito® threat-detection and hunting platform from Vectra®. The test, which coincidentally took place during the 2018 World Cup, quickly proved the value of Cognito.

"Cognito identified anomalous traffic, where 10 IP addresses visited the same website at the same time," says Whelan. "It was harmless, but it really showed us the value of Cognito."

Powered by AI, Cognito automates the real-time detection of hidden attackers in cloud and data center workloads and in user and internet-of-things devices. Cognito instantly triages detected threats across the Ardagh Group global network, correlates them to compromised host devices, and prioritizes attacks that pose the greatest risk. This high-fidelity visibility enables the security team to respond quickly and decisively to threats.

"When Cognito detects a threat, we're able to identify where it is and determine how to best respond quickly," says Whelan.

Follow the money

The manufacturing industry is a favorite target for cybercriminals. Intellectual property, trade secrets and human resources information are alluring, and the steady flow of business with suppliers and customers can result in a big payoff.

"Every attack we've seen involved an attempt to steal," says Whelan.

"Rerouting a single invoice between us and our customer could result in the loss of millions of euros," says Whelan. "It's not surprising that every attack we've seen involved an attempt to steal."

"We have controls that ensure invoices are approved and bank account details aren't modified, but we also need to make sure that someone can't access that data through a different path and make changes," Whelan notes. "That's where Cognito steps in."

For a company with €8.6 billion in revenue, a single compromised invoice might be a drop in the bucket. But hackers also raise the risks of reputational damage and supply-chain attacks, which could cause more complex, long-term consequences.

"Cognito offers a better way of identifying if an attacker got past Stage 1," says Whelan. "If someone is determined to get in, they will. But with Cognito, we can stop threats before they cause damage."

Know what's normal

"Cognito allows us to better understand the patterns of our network behaviour," says Whelan. "This has given us the confidence that we would identify potential attacker behaviour in real-time."

For example, suppose a senior manager from the Netherlands office regularly comes to the Dublin office, and Cognito identifies the server connections as unusual.

"Cognito ignores normal network traffic and instead focuses on exposing potential attacker behaviours," he says.

> Cognito provides this real-time visibility by extracting the metadata from packets, rather than performing deep packet inspection.

For more information please contact a service representative at sales-inquiries@vectra.ai.

Email info@vectra.ai vectra.ai

Protection without prying

Cognito provides this real-time visibility by extracting the metadata from packets, rather than performing deep packet inspection. This enables protection without prying and without performance penalties associated with deep packet inspection.

That's very important at the Ardagh Group.

"We have a very strong history of data privacy," says Whelan.

The company must comply with the General Data Protection Regulation, European Works Council, and many other national and international data privacy laws.

"Cognito is non-intrusive," he says. "It collects and examines network metadata for attacker behaviors instead of tracking users."