

CASE STUDY

Specialty chemicals and advanced materials

Forbes Global 2000 manufacturer protects trade secrets and data with AI-powered network detection and response

As consumers, we scarcely give thought to the role chemistry plays in our daily lives. Innovation is at the heart of this specialty chemical and advanced materials manufacturer of innovative plastics, coatings and adhesives, which are used in every industry from consumer goods and foods to automotive and energy.

Data privacy and integrity must be safeguarded. Research and development work, manufacturing formulas, strategic business information and personal information about employees, customers and suppliers must be protected.

Cyberattacks can grind production operations to a halt, disrupting the company's supply chain, which spans the procurement of raw materials to formulating the plastics and adhesives that are essential ingredients in its own customers' manufacturing processes.

Business disruption, reputational damage and fines for regulatory noncompliance are serious repercussions.

"A single flaw can damage the company and its image," says the security manager at the chemical and advanced materials company.

Speed-up threat detection and response

With the rise of successful attacks against manufacturers and the requirements of the EU GDPR legislation, the company undertook a thorough assessment of its cyber-risks.

"With artificial intelligence, the Cognito dashboard presents accurate details and context about detected threats while being simple to use."

Security Manager
Forbes Global 2000 Manufacturer

Organization

Forbes Global 2000 manufacturer of specialty chemicals and advanced materials

Industry

Manufacturing

Challenge

Ensure its supply chain, from raw materials to finished goods, is not compromised by hidden cyberattacks

Selection criteria

Empower security operations teams to increase productivity by automating cyberattack detection and response using AI

Results

- Safeguard intellectual property and other sensitive data across operations in 50 countries
- Comply with the European Union's General Data Protection Regulation (GDPR)
- Detect complex, multistage attacks faster and with less burden to the security operations team

“Cognito even makes it possible to know the state of health at remote sites that we might acquire in the future, before they connect to our corporate network”

Security Manager
Forbes Global 2000 Manufacturer

As an outcome of the assessment, the company determined it needed a better way to detect and respond to cyberattacks. It wanted clear visibility into advanced attacks at its European headquarters and across operations in 50 countries.

The company wanted to lift the burden from its security operations team, which was weighed down by huge volumes of inconclusive alerts and false positives. The team wanted to detect and respond to hidden attackers that posed the highest business risk, before damage was done.

Use AI to win the race against attackers

The company chose Cognito®, the ultimate AI-powered network detection and response platform from Vectra®.

Cognito’s always-learning behavioral models use AI to efficiently find hidden and unknown attackers in real time. The company’s security analysts now have the most relevant context at their fingertips, enabling quick, decisive action to stop in-progress attacks.

To gain high-fidelity visibility into the actions of all cloud and data center workloads across the company’s global operations, as well as user and IoT devices, Cognito analyzes all network metadata, relevant logs and cloud events from across the enterprise.

Cognito gives the security operations team a unique vantage point. From its European data center, the team has complete visibility into in-progress cyberattacks across all its offices and industrial sites around the world.

“Thanks to the continuous monitoring of all network traffic, Cognito gives us all the necessary visibility so we can easily detect elusive cyberattacks in our network,” says the security manager. “And by collecting and analyzing metadata from this traffic, we are able to protect personal privacy.”

Lift the security operations burden

By automating the tedious, labor-intensive tasks associated with trying to detect threats manually, the company’s security team has been able to respond faster to attacks and conduct more conclusive threat investigations.

Instead of spending hours, days or weeks manually hunting for hidden and unknown threats, the security team can find and stop threats in minutes.

“With artificial intelligence, the Cognito dashboard presents accurate details and context about detected threats while being simple to use,” says the security manager. “Cognito significantly reduces our operational workload.”

Meet regulatory mandates

With Cognito’s AI-powered attacker detection and threat hunting platform, the company can strengthen data protection, ensure compliance with GDPR articles and maintain the trust of its customers.

GDPR gives organizations 72 hours after discovery of a data breach to notify individuals whose data was compromised. Cognito supports GDPR by protecting personal privacy and providing a solid chain of forensic evidence behind every attack.

By enabling the security team to identify and intervene in the earliest stages of an attack and providing real-time reporting capabilities, Cognito reduces the risk of GDPR-reportable data breaches.

Cognito also supports the GDPR recommended use of data encryption and pseudonymization because it analyzes network traffic and its behavior, not the actual data payload itself. With Cognito, intrusive monitoring processes or decryption of traffic is not necessary to find and stop hidden threats.

Instantly part of the security team

Cognito was deployed without any impact to the production network and added immediate value to the company's security operations.

"The results appeared very quickly," says the security manager. "Our security team was able to understand and take action on Cognito's findings, thanks to the intuitive design."

The ability to detect hidden threats has far-reaching consequences as the company continues to innovate and expand, with revenues and profit margins hitting record levels.

As the company opens new production sites around the world, Cognito will continue to perform real-time detection of hidden attackers in cloud and data center workloads and user and IoT devices.

"Cognito even make it possible to know the state of health at remote sites that we might acquire in the future, before they connect to our corporate network," says the security manager. "This will enable us to better evaluate business risk."

Armed with the ultimate AI-powered cyberattack-detection and threat-hunting platform, the security team can protect the company's intellectual property and sensitive information around the world.

Under the watchful eye of Cognito, the company can focus on its core business of creating innovative chemistry that enables its customers to create high-performance sports gear, cleaner water, renewable energy and much more.

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



"Thanks to the continuous monitoring of all network traffic, Cognito gives us all the necessary visibility so we can easily detect elusive cyberattacks in our network."

Security Manager
Forbes Global 2000 Manufacturer

Email info@vectra.ai [vectra.ai](https://www.vectra.ai)

© 2020 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders. Version: 111620