Case Study

European glassmaker sees threats clearly

Artificial intelligence gives Vetropack a fast, efficient way to detect and respond to cyberattacks

For more than 100 years, Vetropack has been making glass bottles and glasspackaging for food and beverages. Today, 3,000 people in seven countries work to produce 4.5 billion tons of glass a year.

With state-of-the-art process engineering, Vetropack is a leader in producing topquality, sustainable glass packaging for everything from wine to baby food.

An obscured view of threats

As highly-skilled cyberattacks achieve heightened levels of sophistication, Vetropack knew it had to transform and strengthen its approach to cybersecurity.

Modern attackers can easily evade firewalls, intrusion detection and other prevention-based perimeter security. This would place Vetropack's innovative glass packaging designs, sustainable manufacturing processes, and other valuable intellectual property at risk.

"Network perimeter security alone is not effective at stopping cyber threats," says Markus Müller-Fehrenbach, Chief Information Security Officer at Vetropack.

"We knew that if we had visibility inside our network, we could detect and stop cyberattackers quickly, before they have a chance to damage or steal important data and assets," he adds.

Seeing more clearly

Vetropack realized that the only way to meet this challenge was to monitor all network traffic for active threats. And in doing so, it was important to avoid disrupting network operations and creating more work for its overburdened security team.

vetropack

Organization

Vetropack Group

Industry

Glass packaging manufacturer

Challenge

Unable to see threats that evade perimeter security and spread inside the network

Selection criteria

Improve visibility and automate the hunt for cyberattackers in the network

Results

- Blindspot-free visibility to detect and stop attackers in the network
- Automation reduced the workload on overburdened security teams
- Faster threat detection and incident response at all locations

VECTRA®
Security that thinks®

"We wanted to eliminate the time-consuming process of finding cyberattackers inside the network," says Müller-Fehrenbach. "Our security team was spending countless hours manually investigating security events that were too often inconclusive."

Vetropack worked with Zurich-based systems integrator Ontrex AG to select and deploy the Cognito® network detection and response platform from Vectra®.

"Vectra offered exactly what we needed," says Müller-Fehrenbach. "It automates attacker detections and allows us to respond faster to the most serious threats."

Cognito is based on a simple principle for finding hidden threats: Use an authoritative source of data and seek out the fundamental threat behaviors that attackers simply can't avoid.

To do this, Cognito relies on the only source of truth during a cyberattack – network traffic. Only traffic on the wire reveals the truth with complete fidelity and independence. Low-fidelity sources, such as analyzing logs, only show what you've already seen, not the hidden attacks that were missed.

Instead of relying on threat signatures or traditional payload inspection, Cognito combines data science, machine learning and behavioral analysis to expose the fundamental behaviors of attackers as they spy, spread, and steal inside networks.

In addition to automating the tedious, painstaking work of threat hunting and speeding-up incident response, Cognito now provides Vetropack with full, unobstructed visibility inside the network.

This enables the Vetropack security team to see in real-time where attackers are, what they are doing, what critical assets they have compromised, and how long they have been in the network.

"Vectra even shows us the highest-risk threats so we can better prioritize our efforts to stop and mitigate attacks faster," Müller-Fehrenbach added.

Cognito analyzes all traffic on Vetropack's physical and virtual networks, providing blindspot-free visibility into the actions of all devices – including IoT and BYOD – in the company's headquarters, manufacturing facilities, data center, and distribution centers throughout Europe.

Using artificial intelligence, Cognito reveals all phases of a cyberattack – command-and-control communications, internal reconnaissance, lateral movement (north/south and east/west traffic), and data exfiltration – as well as the early signs of ransomware, insider threats, botnet monetization, remote access tools, hidden tunnels, backdoors, credential abuse, and misconfigured devices.

Improves operational efficiency

After its installation at Vetropack, "Vectra brought several important procedural improvements and structural workflow efficiencies to our security operations," says Müller-Fehrenbach.

Cognito delivers a wide range of communication and automated response mechanisms that improve situational awareness, expedite information sharing, and support incident response activities, helping to make overall cybersecurity operations more efficient.

"The entire triage process is automated, from detections to threat and host scores to incident response," says Müller-Fehrenbach. "Our security team always knows what is happening inside the network at any given time and what steps to take to remediate a threat."

Cognito assimilates all available information to provide context about the larger attack campaign – not just the individual events. In addition to tracking the progression of every attack over time, Cognito shows the underlying events and historical context that led to a detection, possible triggers, root causes, business impacts, and steps to verify.

"Now that we have actionable and contextual information to quickly stop in-progress cyberattacks, our security team can proactively concentrate on threat containment, remediation, forensics and other critical areas," says Müller-Fehrenbach.

> *"We needed to offload our security team, which was spending countless hours manually hunting for threats and investigating security events that led nowhere."*

Markus Müller-Fehrenbach
Chief Information Security Officer
Vetropack

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020 www.vectra.ai