

# How Global Limestone Leader Schaefer Kalk Overcame their EDR Visibility Gaps



**Organization**  
Schaefer Kalk

**Industry**  
Construction and Materials

**The Challenge**  
Schaefer Kalk's existing EDR system lacked complete visibility, hindering their ability to protect against sophisticated cyberattacks.

**The Solution**  
To overcome this, the company chose Vectra's AI-driven Attack Signal Intelligence platform, which offered improved visibility, threat detection, and streamlined incident response, complemented by MDR services and Microsoft 365 monitoring.

**The Results**  
Implementing Vectra AI provided the team with comprehensive visibility and threat detection, resulting in enhanced operational efficiency and significant cost savings. Notably, the Vectra MDR team prevented a serious ransomware attack, avoiding potentially critical losses.

Schaefer Kalk, a family-owned company with a rich history of over 160 years, is a premier provider of high-quality lime products. With a global presence spanning Europe and Asia, their commitment to sustainability and innovation has made them a trusted partner for various industries. Recognizing the growing threat of cyberattacks, Schaefer Kalk has intensified its efforts to build a resilient security infrastructure.

---

## The Challenge

### Overcoming the EDR visibility gap

The company faced a formidable challenge: safeguarding its network and hybrid environment against increasingly sophisticated cyberattacks. Although Schaefer Kalk's existing Endpoint Detection and Response (EDR) system, Cybereason, provided a baseline level of security, it had its limitations.

"Our EDR system couldn't provide complete visibility," explained Dr. Martin Klais, Department Manager IT at Schaefer Kalk,

**"We were missing critical attack chains and couldn't monitor all of our systems."**

To enhance their overall security posture, the team began their search for a solution that could provide greater network, identity and cloud visibility, improved threat detection, and a streamlined incident response process.

---

## The Solution

### Finding the right fit

After evaluating various options, including Darktrace, Schaefer Kalk ultimately chose Vectra's AI-driven Attack Signal Intelligence platform. Vectra AI's capability to monitor their virtual environments, detect attacks at various stages of the kill chain, and minimize false positives, coupled with its intuitive user interface and Managed Detection and Response (MDR) team, made it the ideal choice.

### Securing cloud identity and Microsoft M365

Additionally, the Vectra AI Platform provided the necessary visibility into their cloud environment, which was critical given the growing reliance on cloud-based services for daily operations. Vectra AI's coverage of Microsoft M365 and Entra ID enabled their security team to gain insights into account activities and identify suspicious activities that might indicate potential cyber threats.

“Vectra AI’s M365 detection capabilities allows us to monitor accounts for irregular behavior and receive proactive alerts, which helps us focus on the most relevant issues,” said Klais.

## Extra eyes, enhanced protection with MDR

For Schaefer Kalk’s small but mighty IT team of nine members, Vectra AI’s MDR service acts as an extension of their in-house resources, providing expert threat hunting, analysis, and response capabilities without the need for additional headcount.

In one instance, this proved invaluable when the Vectra AI MDR team flagged a serious cyberattack that evaded the company’s EDR system, saving them from potentially devastating losses.

“The MDR team’s proactive alerts allowed us to neutralize the attack before it caused serious damage,” noted Klais.

## Partnership with SVA

A key contributor to the success of this adoption was the collaboration with partner SVA, System Vertrieb Alexander GmbH, one of Germany’s leading IT service providers. “A huge thank you to SVA, for providing onboarding process support and fostering a close relationship with Vectra AI throughout our deployment,” shares Klais. Known for their expertise in combining top-quality IT products with extensive project knowledge, SVA played a crucial role in facilitating Vectra AI’s Proof of Value (POV) and their contributions were instrumental in ensuring a smooth implementation process.

### The Results

## The gold standard

Since implementing Vectra AI, Schaefer Kalk has experienced incredible results on multiple fronts, including:

- **Reduced Threat Exposure:** Enhanced Visibility & Early Threat Detection: Vectra AI provided the team with comprehensive visibility into their network, cloud, and hybrid environments, empowering them to identify and respond to threats early on.
- **Removed Detection Latency:** Cost Savings and Increased Efficiency: By averting a ransomware attack and reducing the need for additional internal staff, the company achieved substantial savings. The Vectra AI MDR team’s intervention in stopping a potential cyberattack prevented serious losses.

In reflecting on their successful partnership with Vectra AI, Klais remarked, “We are very glad to have Vectra AI on board and to have successfully mitigated a serious attack together.”

### About Vectra AI

Vectra AI is the leader in AI-native security and observability. Vectra AI delivers organizations real-time visibility into their network, clear insight into which behaviors matter, and the ability to act before risk becomes impact. By connecting on-premises, multi-cloud, identity, SaaS, edge, and IoT/OT infrastructure, Vectra AI helps organizations reduce exposure, accelerate detection and response, and automate security operations with AI. With over a decade of AI and ML innovation, 39 patents and a Leader in the 2025 and 2026 Gartner Magic Quadrant for Network Detection and Response, Vectra AI empowers security teams to stay ahead of emerging AI powered attacks, increase operational efficiency, and prove resilient in an increasingly complex, AI-driven world. For more information, visit [www.vectra.ai](http://www.vectra.ai).

**“Vectra AI’s M365 detection capabilities allows us to monitor accounts for irregular behavior and receive proactive alerts, which helps us focus on the most relevant issues.”**

**DR. MARTIN KLAIS**  
Department Manager IT  
Schaefer Kalkh

[Read more customer stories](#)

**For more information please contact us:** Email: [info@vectra.ai](mailto:info@vectra.ai) | [vectra.ai](http://vectra.ai)

© 2026 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, and Security that thinks are registered trademarks and the Vectra Threat Labs, Threat Certainty Index and Attack Signal Intelligence are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders. Version: 061126