Customer Case Study

Bühler Group Leverages Behavioural AI for Stronger, Streamlined Security

Global technology company uses Abnormal AI and automation to identify and remediate advanced threats in real time.

Industry
Manufacturing

Headquarters
Uzwil, Switzerland

Protected Mailboxes
15,000+

Bühler Group has been making the machines that processors use for more than 160 years. Today, the family-owned Swiss technology company operates in more than 140 countries, serving customers in the advanced materials, food, and animal feed sectors. More than half of the world's new vehicles contain parts made with Bühler equipment, and two billion people each day eat foods processed with Bühler technology. The company also provides installation, maintenance, and training services.

The Bühler Group Email Security Challenge

Bühler relied on Microsoft 365 Exchange plus Defender for email, but rising numbers of phishing attacks were reaching users' inboxes. "Helping our employees avoid getting phished is a challenge because we have so many customers of different sizes and invoicing habits," said Bruno Bedin, CISO. "We were constantly remediating everything from basic phishing to VEC to QR code attacks and CEO impersonations."

New phishing awareness training revealed even more issues. "Our people heavily used the tool's report button," said Patrick Zimmermann, Expert Information Security Specialist. "We were so surprised by how many attacks reached inboxes that we checked for misconfigurations, but there were none."

Customer Key Challenges

- Prevent basic and advanced phishing threats from reaching users' inboxes.
- Free SOC analysts from a heavy investigation and remediation workload.
- Add advanced email security that doesn't require continuous tuning.

Abnormal Solution

- Uses human behaviour AI to learn normal email activity and detect even sophisticated email attacks and account takeovers.
- Leverages automation alongside AI to investigate reported emails and auto-remediate attacks, saving SOC analyst resources for other issues.
- Identifies new threats in real time to avoid lags in detection—mitigating risk for the company and eliminating manual work for the SOC.

> “Filter-based detection doesn't work anymore. While you’re training the filter on one kind of attack, it only takes one user click to cause problems, or the attackers will change strategies. It's better to stop attacks with behavioural AI so users never see them.”

Patrick Zimmermann
Expert Information Security Specialist

Customer Case Study

$120K
yearly SOC savings
from autonomous AI.

330+
SOC analyst hours
saved per month.

1,020
companywide hours saved
on graymail in 30 days.

The Abnormal Security Solution

When Zimmermann first heard of Abnormal, it piqued his interest. He and Bedin wanted an easy-to-integrate solution, and Abnormal's API-based approach seemed promising. They considered several API-based options, including Abnormal.

The Abnormal POV met the team's expectations for ease of use. Zimmermann and Bedin also liked the platform's dashboard, which showed many more attacks reaching inboxes than they had anticipated. The dashboard also made it easy to present their case for investing in a new solution. "The portal showed potential risk reduction in dollars based on real data, which we used to create a slide deck that detailed business value for our management," Zimmermann said.

Why Bühler Group Chose Abnormal

Abnormal's behavioural AI approach to detecting both email attacks and account takeovers was a key factor in Bühler's choice. "A traditional filter might not be able to detect threats past the first or second stage of an email chain, but we've seen that Abnormal can recognise malicious behaviour farther along the chain," Bedin said.

Positive peer feedback from Gartner and other Abnormal customers was also a factor in Bühler's decision. So was the combination of features that saves the company time on email security processes and inbox management. "Inbound Email Security was the base we wanted," Zimmermann said. "But AI Security Mailbox and Account Takeover Protection added more value, and the graymail filtering we receive with Email Productivity is the cherry on top." Together these features have saved Bühler thousands of SOC analyst and employee hours since activation.

More Secure and Efficient Email as Attacks Evolve

In addition to stronger email security and efficiency gains, Abnormal has given Bühler's security leaders confidence about their email security now and in the future. "I'm more comfortable now, knowing that so much less reaches the inbox than before," Zimmermann said. "AI like Abnormal's is the only feasible, reasonable way to defend against advanced threats, especially as more attackers adopt AI for malicious purposes," Bedin agreed. "As the complexity of phishing increases, using AI makes sense, and Abnormal based their solution on AI from the start."

> "It doesn't make sense to adopt a solution with 20 or 30 configuration points that you have to tune instead of a hassle-free, autopilot solution. Abnormal offers low-effort integration and operations with high-quality detection and filtering capabilities. You turn it on and it just works."
>
> Bruno Bedin
> CISO

Abnormal Products in use:

- Inbound Email Security
- Account Takeover Protection
- AI Security Mailbox
- Email Productivity

abnormalsecurity.com →

Abnormal