



Customer Case Study

ALCIVIA Enhances Security and Productivity to Benefit Its Co-Op Members

Agriculture and energy group stops more attacks and saves employee time with Abnormal human behavior AI and automation.

ALCIVIA is built on the farming tradition of teamwork for a common goal. The cooperative provides farmers in Wisconsin, Minnesota, Illinois, and Iowa with agronomy, animal nutrition, grain, financial, and energy products and services. ALCIVIA pursues member success through innovation, including technology.

In addition to serving more than 2,500 members of its own, ALCIVIA is part of the vast Land O'Lakes agricultural co-op system, which operates in every US state and more than 60 countries.

The ALCIVIA Email Security Challenge

ALCIVIA's members, vendors, and co-op partners play roles in food production so protecting their data is critical. Despite their Microsoft 365 email security tools and an additional third-party secure email gateway (SEG), the co-op's small IT team struggled to keep up with rising numbers of credential phishing attacks. The team was also trying to keep up with user-reported graymail—and the SEG itself.

"The solution wasn't working well for us," said Peter Wolter, Director of IT. "We were spending too much time adjusting safelists and blocklists." Wolter said the breaking point was the number of false positives caused by the rigidity of the SEG lists, which required the team to divert resources to retrieving missing messages.

"Threat actors are already using AI, so we use Abnormal's human behavior AI to protect our email ecosystem and its data. [When Abnormal makes a fast, accurate decision about an email, based on tens of thousands of threat signals, we're doing our customers a service and protecting ourselves.](#)"

Peter Wolter
Director of IT



Industry
Agriculture

Headquarters
Cottage Grove, WI, USA

Protected Mailboxes
600+

Customer Key Challenges

- Reduce IT time spent on managing email filters and user reports.
- Improve attack detection to protect the entire co-op email ecosystem.
- Find a solution that integrates easily with M365 and CrowdStrike.

Abnormal Solution

- Replaced manual tuning with behavioral AI to detect anomalies, and handled user report responses in real time with automation.
- Made the co-op email ecosystem more secure with real-time detection of advanced credential phishing attacks.
- Integrated quickly with M365 and CrowdStrike due to API-based design.



Customer Case Study

96

Hours saved by employees in 30 days with graymail filtering.

45

Hours saved by the IT team in 75 days on user reports.

2,500+

Co-op members protected by human behavior AI.

The Abnormal Security Solution

The ALCIVIA team heard positive things about Abnormal from some of their co-op partners and from their CrowdStrike representative. Because Abnormal is API-based and designed to work with M365, setting up a proof of value (POV) was a matter of a few clicks.

Upon integration, Wolter received a one-line vendor invoice message with an attachment. He wasn't sure it was safe to open, so he reported it to Abnormal. "The response came within minutes: 'We checked the headers. It's coming from the right company. More than that, the PO number in the email is within the known range of PO numbers for this vendor.' Having that level of confidence was amazing," he said.

Why ALCIVIA Chose Abnormal

Wolter was impressed by the AI capabilities. "The volume of signals Abnormal looks at, we could never do on our own," he said. "And the false positive rate was less than half of 1%. After recovering an important email for our CEO that got falsely flagged and hidden by our old system, I told him what Abnormal's error rate was. He told me to get it done."

The POV made it easy to go live, said Thomas Riffle, Senior Systems Administrator and Service Desk Team Lead. "When we were ready it was very simple, like a flip of the switch."

Abnormal's API integration with Microsoft allows all email to come into the same place from the co-op's three domains. Wolter also liked the platform's account takeover protection tools and graymail sorting capability, which lets each user train the model by dragging promotional messages into a separate folder.

A Solution That Works for the Co-Op's Future

Now ALCIVIA has stronger protection, and integrating Abnormal with CrowdStrike endpoint protection added even more peace of mind. "When Abnormal catches and remediates a message with a malicious attachment, CrowdStrike notifies us," Riffle said. Abnormal also gives ALCIVIA's employees and IT team time back to work on core tasks and to innovate on behalf of their members. "Even if you could train your people to do what Abnormal does, who wants to come to work and do that?" Wolter said. "You need something as smart as Abnormal to protect your co-op."

"My fellow co-op IT people on a very small team or working as a one-man operation have a lot more to do than sift through malicious and suspicious emails. **Let Abnormal do that for you so you can put out fires and take care of the other things you need to do for your cooperative.**"

Thomas Riffle
Senior Systems Administrator and
Service Desk Team Lead

Abnormal Products in use:

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

abnormalsecurity.com →