AGRAVIS Protects Critical Networks for Agricultural Solutions With Proofpoint

The Challenge

- Strengthen email security and minimise false positives
- Protect people and data from insider threats
- Continuously update security best practices to keep pace with change

The Solution

- Proofpoint Enterprise Email Protection
- Proofpoint Targeted Attack Protection (TAP)
- Proofpoint Threat Response Auto-Pull (TRAP)
- Proofpoint Email Fraud Defense (EFD)
- Proofpoint Security Awareness Training (PSAT)
- Proofpoint Insider Threat Management (ITM)

The Results

- Reduced false positives maximise productivity of small IT team
- Augmented technology with improved best practices using Security Awareness Training

The Company

The agricultural trading services business is part of a unique industry. AGRAVIS Raiffeisen AG is a leader in this arena. Based in Germany, the company supports its cooperative distribution partners, agriculture, and people in rural areas with a wide variety of products. And these offerings are backed by its expert consultancy services and extensive knowledge and experience. But to keep its data safe and adapt to changing business needs, the organisation needed an advanced cybersecurity solution.

The Challenge

Secure an updated business email platform

AGRAVIS provides plant cultivation support, livestock feed, agricultural technology and machinery, and more. With its growing business, it was critical to maintain the security and integrity of the company's network infrastructure and data. To keep its employee, customer, and business data safe, AGRAVIS dedicated five IT professionals to secure its workforce of 6,300. And like most organisations, the company constantly evolved and upgraded its infrastructure to keep up with new business needs. But when its existing email security gateway began experiencing issues, AGRAVIS saw an opportunity. It needed to update its communications—and strengthen its security posture.

"Our new IT strategy included a switch to Office 365 and Microsoft Exchange Online for business email," said David Wydrinna, security engineer at AGRAVIS. "However, we had some issues with our on-premises email security gateway in Münster. We saw performance problems, dropouts and time outs for no apparent reason. So we set up a proof of concept with top vendors to determine the email security solution that would best meet our needs."

The Solution

Proofpoint provides complete, nimble email protection
After evaluating several solutions in its POC, AGRAVIS chose a comprehensive, integrated email solution from Proofpoint. Proofpoint Email Security and Protection protects staff from the latest email threats, including credential phishing, ransomware and email fraud. Using machine learning and multilayered protection, it identifies and blocks malicious email. And Proofpoint Threat Response Auto-Pull (TRAP) lets the security IT team analyse emails and move malicious messages to quarantine after they are delivered.

"One of the strongest points of the solution was the ability of the TRAP server to identify emails that got through, and then automatically remove them from the postbox data," said Patrick Hemsing, security engineer at AGRAVIS.

"The Proofpoint solution is great, and has been much more effective at enabling us to identify phishing and spam attacks compared to our previous solution. It has enabled us to reduce the number of threats that reach our network endpoints by about 95%."

David Wydrinna, security engineer, AGRAVIS

For added protection for its cloud-based business email environment, Proofpoint Targeted Attack Protection (TAP) uses static and dynamic techniques to perform sandboxing and analysis to detect threats early in the attack chain.

"The sandbox capability was one of the key differentiators as we compared solutions in our POC," said Hemsing. "Proofpoint also provided a higher level of stability and ease of use compared to other solutions."

Many security threats come from the people inside an organisation. This holds true whether they're acting negligently, maliciously or unknowingly. To make sure its organisation was protected, the AGRAVIS IT team deployed Proofpoint Insider Threat Management (ITM). This solution correlates user activity and data movement. And it allowed the team to accurately determine user risk, spot insider-related breaches, and respond to incidents fast.

The Results

Building security insights and freeing up staff for priority tasks
Proofpoint delivers the threat protection AGRAVIS requires to keep its most important business processes safe. At the same time, it automates processes and minimises time-consuming false positives that take up valuable staff time.

"We had daily problems with our old solution," said Hemsing. "Every day we might have 50 emails quarantined, and a member of our staff had to spend hours manually evaluating them to determine whether they were spam, a spear phishing attack, or an appliance error. With Proofpoint, we don't have to do that anymore—so we have more time to focus on other tasks."

Partnering with Proofpoint has also given AGRAVIS access to a trusted advisor that can offer new levels of insight into threats. This can inform the company's IT priorities and decisions.

"We received a call from our Proofpoint customer success manager, who told us how many phishing emails the solution had intercepted, and for the first time we could report it to our CIO," said Wydrinna. "Our manager shared a document showing all our configurations, statistics on attacks we didn't know about, and advice on what we could do better in the future."

Proofpoint solutions are built to evolve and scale, and AGRAVIS is already in the process of extending its solution. The company is adding Proofpoint Email Fraud Defense (EFD), which simplifies Domain-based Message Authentication, Reporting & Conformance (DMARC). This helps stop fraud and protect the organisation's trusted domain. Proofpoint EFD also monitors and analyses DMARC forensic reports. This gives AGRAVIS insights into how to block malicious emails that are spoofing domains.

AGRAVIS is also moving to provide Proofpoint Security Awareness Training (PSAT) to its employees to proactively keep pace with the changing threat landscape. As attacks change, the organisation wants to ensure that its employees are always aware of the most current best practices. This will keep protection as strong as possible.

"In the past, it might take us four weeks to manually configure such a campaign," said Wydrinna. "Now with PSAT, we can set it up in minutes."

With its Proofpoint solutions and services in place, AGRAVIS is confident that it will continue to stay ahead of emerging security threats well into the future.

LEARN MORE
For more information, visit **proofpoint.com**.

proofpoint.