proofpoint.

CUSTOMER STORY

Finning International Stops Email Fraud, Restores User Trust by Building on Proofpoint Investment

FINNING

THE CHALLENGE

- Managing a deluge of suspicious email reaching users' inboxes
- Lack of trust in legitimate email
- Operational struggles due to high volume of suspicious email reports, holding up legitimate business
- A surging volume of hard-to-detect business email compromise (BEC) and email account compromise (EAC) attacks

THE SOLUTION

- Proofpoint Targeted Attack Protection
- Proofpoint Cloud Account Defense
- Proofpoint Security Awareness Training
- Proofpoint Email Protection
- Proofpoint Email Fraud Defense
- Proofpoint Threat Response Auto-Pull
- Proofpoint Closed-Loop Email Analysis and Response

THE RESULTS

- Regained trust in email
- More efficient security operations
- Faster analysis and incident response
- Within first three months:
  - 46 million unsafe or unwanted emails blocked
  - 11,933 malicious attachments blocked
  - 24,992 unsafe URLs blocked
  - 387 impostor attacks stopped

The Company

Finning International Manager of Security Operations, Brian Uhreen, knew he had a problem when his users stopped trusting the email they were getting from their own colleagues.

Finning is the world's largest dealer of Caterpillar heavy equipment and diesel engines. With more 12,000 workers spread across six countries, the 88-year-old company relies on email to keep business humming. Whether its ordering parts, answering customers' questions, paying invoices or selling equipment, Finning uses email in almost every part of the business.

But in 2017, a growing volume of fraudulent messages was taking a toll on operations. Employees, trained to be on the lookout for fraud, were questioning normal day-to-day requests. Legitimate business was being held up. And the IT department was overwhelmed with reports of suspicious email.

"We needed to be able to verify that email between our suppliers, partners and our employees was legitimate and free of threats," Uhreen said.

The Challenge

The company had already deployed email defenses to stop malware, unsafe URLs and phishing attacks. But attackers were shifting tactics. Instead of just trying to exploit vulnerabilities in Finning's infrastructure, they were now targeting its people. Employees began receiving emails impersonating vendors, customers and even coworkers.

In one situation, a Finning executive got an email instructing him to wire a large sum of money to the sender—someone impersonating the CFO. The attacker had registered the domain "fjinnjng.com," which in many email clients looks like "finning.com." Fortunately, the executive was able to identify the phishing email and immediately reported it to the security team as per company protocol.

Lookalike email domains like this are just one of the techniques used in so-called business email compromise (BEC) attacks. In BEC, attackers use email to pose as someone the recipient trusts, including colleagues, busines partners, suppliers and customers. The sender might send a fake invoice, ask for a wire transfer or instruct the recipient to change banking details to divert payments.

Losses due to BEC and a closely related attack known as email account compromise (EAC) have reached $26 billion worldwide, according to the FBI.[1] (In EAC, attackers take over a legitimate email account to impersonate that person.)

Fortunately, Finning had invested in Proofpoint Security Awareness Training, so the executive knew to double-check the request. His training kicked in and stopped what would have been a costly mistake.

But as the volume of fraudulent email grew, the risk was getting harder to manage. Following up on suspicious email reports was turning into an operational nightmare for the security team. Normal transactions were getting held up in a cloud of doubt. In short, one of Finning's most essential business tools—email—was becoming a business liability.

> "When we bought into Proofpoint, it wasn't just at one moment for one product. We're a company that believes in strong partner relationships. Proofpoint came out the winner just on overall flexibility."
>
> **Brian Uhreen,** manager of security operations, Finning International

"When people can't tell right (emails) from wrong, there's a fundamental issue," Uhreen said.

So far, the company's employees had done a good job "catching live grenades," as Uhreen puts it. But the approach wasn't scaling. What Finning really needed was a way to lob those grenades away before they reached users' inbox.

Unlike malware attacks, BEC and EAC attacks rely on social engineering, not technical vulnerabilities. There's no payload to scan, making them much harder to detect—nearly impossible with conventional security tools.

The Solution

Uhreen, who already relied on Proofpoint to help him stop malicious attachments and unsafe URLs, approached the cybersecurity company about its email fraud problem.

The Proofpoint team first made sure that Finning's was getting the most out of its existing deployment, which included Proofpoint Email Protection and Proofpoint Targeted Attack Protection. The solutions stop advanced malware attacks and help Finning manage spam and bulk mail. After a thorough health check, Uhreen determined that he needed an additional layer of security for BEC and EAC attacks.

He understood that attacks were evolving. And he needed a cybersecurity vendor that was evolving with them.

1 FBI. "Business Email Compromise: The $26 Billion Scam." September 2019.

"This is where Proofpoint has stepped up," he said. "Proofpoint's roadmap is really aligned with where Finning as an organization is going."

Proofpoint enhanced Finning's email security with defenses that can stop a wide range of email fraud tactics. Proofpoint Email Security detects and stops domain spoofing, lookalike domains, email account takeover and more.

Proofpoint Threat Response Auto-Pull and Proofpoint Closed-Loop Email Analysis and Response automates key parts of the threat response. They help Uhreen's team quickly resolve suspicious email reported by users. When unsafe email is delivered (or becomes malicious after being delivered), Threat Response Auto-Pull can remove it from users' inbox along with any copies that are forwarded to colleagues.

Because Finning had already deployed Proofpoint for security awareness training and other types of email threats, adding email fraud defenses was an easy choice, he says. And just as important in the decision, Proofpoint's technical partnerships with other leading cybersecurity vendors meant a more efficient security operations.

As Finning migrated to the cloud, the company added Proofpoint Cloud Account Defense, which helps protect against account takeovers and EAC attacks.

The Results

Finning began reaping the benefits of the added security layers right away. In three months, the number of malicious and unwanted email that Finning stopped increased substantially. Such as, malicious attachments, unsafe URLs blocked through TAP and impostor attacks that would have further undermined users' trust in email and bogged down business.

"When you can say 'Here is a system that is automatically taking care of attacks,' it's an honest narrative on our organization's approach to protecting our data, people and customers," he said.

While quantifying the value of potential fraud that didn't happen isn't an exact science, Uhreen says Proofpoint has helped the company avoid financial fraud—including a $750,000 fraudulent wire transfer request.

But for Uhreen, one of the biggest benefits of the Proofpoint solution is one that can't be quantified at all. With Proofpoint helping stop threats in real time as they unfold, Uhreen can scale up his security efforts without adding additional people—or stretching them too thin.

"Because of this, our people are able to be more efficient, sleep better at night and even find time to take off for vacation," he said.

LEARN MORE

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