proofpoint.

Ixom Strengthens Protection of Manufacturing Operations from Email Fraud Attacks with Proofpoint

IXOM

The Challenge

- Protect manufacturing operations from ransomware and cyber threats
- Secure email communications
- Protect employee email communications from cyber threats

The Solution

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

The Results

- Threat protection platform helps minimize email fraud and ransomware attacks
- Regular security reporting helps organization measure success and minimize risk
- Ongoing training promotes a culture of security

The Company

Ixom is a market leader in water treatment and chemical distribution in Australia and New Zealand, with an increasing presence throughout South East Asia and America. Formed over 100 years ago, Ixom uses its many years of knowledge and specialist expertise to help keep communities safe and industries operating.

Most drinking water in Australia and New Zealand is treated with Ixom products. Ixom manufactures and imports many of the products industries need, including agriculture, viticulture, construction, electricity, steel, food and beverage, and pulp and paper. It's hard to find an industry that Ixom does not touch.

With more than 1,000 employees and operations in nine countries, cybersecurity is at the forefront of this large and diverse organization.

The Challenge

Protecting a global distribution system from new threats
Ixom maintains a variety of manufacturing plants in Australia, New Zealand and the U.S. Ensuring the integrity of its network infrastructure is top of mind. Even a small breach could impact production, compromise data and finances, or damage its reputation.

"Our number one IT risk is cyber crime," said Greg Leibel, security architect at Ixom. "We are especially concerned about email risks, such as someone pretending to be an internal executive and instructing a manager to authorize a payment for a major investment. Or phishing attacks seeking usernames and passwords."

Ixom needed a solution to strengthen its enterprise security by mitigating threats to email.

The Solution

Comprehensive email security that simply works

To help secure its email channel and make sure that its business communications remained trusted, Ixom deployed Proofpoint Email Fraud Defense. Email Fraud Defense helps to minimize the risks of impostor threats by enabling Ixom to confidently enforce DMARC on its inbound traffic. The solution also goes beyond DMARC to provide insight into business email compromise (BEC) attacks. This includes fraud risks posed by suppliers. Deployment went smoothly and Proofpoint helped simplify the rollout by guiding Leibel and his team through each step of the process.

"One of the things I like most about Proofpoint is the implementation methodology," said Leibel. "The approach was a friendly way of leading us on a journey, which was great."

Email Fraud Defense also includes the Hosted Sender Policy Framework (SPF) service, which helps simplify Ixom's DMARC journey.

"The Hosted SPF service was so easy to implement—it just worked wonderfully," said Leibel.

"Proofpoint simply delivers better email security. It captures more problems, it's more automated, and it provides a much more integrated solution. The way Proofpoint Security Awareness Training integrates with Proofpoint Targeted Attack Protection and Proofpoint Threat Response Auto-Pull gives us a powerful technical solution and an improved process for risk reduction."

Greg Leibel, security architect, Ixom

To defend the organization against ransomware and other advanced threats, Ixom deployed Proofpoint Targeted Attack Protection (TAP). Designed to continually adapt to the very latest cyber attacks, it detects and blocks threats before they reach users' mailboxes. Proofpoint Threat Response Auto-Pull (TRAP) provides an additional layer of protection. It allows Leibel and his team to automatically remove or quarantine malicious emails and unwanted emails post delivery, including those forwarded to other internal users.

Proofpoint Security Awareness Training augments the solution. It gives Ixom the assessments, training, phishing simulation, and tools it needs to help employees identify risks, modify their behavior, and become more resilient to human-activated threats.

"Proofpoint Security Awareness Training is opening people's eyes to the ability to do better," said Leibel. "It reminds us that even if the system and the defenses are really good, the people are the last line of defense, and we need to stay focused."

The Results

Progress on the journey to minimize risk

Ixom is delighted to see the reduction in risk provided by deploying the Proofpoint suite. The solution has also helped IT save time manually responding to email threats.

"With Proofpoint, we just don't see the outbreaks of phishing attacks that we used to, nor the need to manually address them," said Leibel. "With TAP and TRAP, email threats pose much less of an issue, because we can simply click on a suspicious email to pull it. The automation is working extremely well."

The Ixom team understood that technology alone can't fully secure an organization, so they put a strong emphasis on training and user education. With Proofpoint phishing simulations, it is easy to redirect employees to Security Awareness Training, in the event they fail a simulated attack.

"Proofpoint offers not only a technical solution to email security, but a process," said Leibel. "The training offerings are not only useful, but popular. We recently learned that participation in the phishing simulation had gone up 18% over 90 days."

Ixom is constantly digging deeper to better understand its potential risks, and take proactive steps to address them. The TAP dashboard enables administrators to drill down into details about specific threats such as BEC attacks, and also helps them learn more about how people in the organization are targeted. The solution revealed that nearly 3% of total employees had been identified as Very Attacked People. More than 62% of inbound email traffic has been condemned malicious and blocked by Ixom's advanced threat detection stacks; of which, 2% were targeted threats.

Ixom also relies on the Proofpoint Security Awareness Training team to stay ahead of threats and plan strategically.

"We catch up with the Proofpoint team on a regular basis to discuss our vulnerabilities, which individuals are most attacked, and the type of threats the solution is blocking," said Leibel. "It's extremely valuable to us to identify the most vulnerable users and understand how we compare to peers. And we get that level of information from the people who do the Security Awareness Training for us. They provide a monthly report, so we see how we were tracking, and how behavior is changing. Plenty of metrics are available, and we trust Proofpoint to point out the best way of doing things— and we follow that approach."

The Proofpoint solution provides valuable capabilities that are helping Ixom move forward on its path to decreased risk.

LEARN MORE

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

---

proofpoint.