proofpoint

CUSTOMER STORY

Medical Device Innovator Teams With Proofpoint to Protect Operations and Save Time

The Challenge

- Protect email from phishing and other threats
- Minimise manual processes to help IT team do more
- Strengthen company security best practices

The Solution

- Proofpoint Email Protection
- Proofpoint Email Fraud Defense
- Proofpoint Targeted Attack Protection
- Proofpoint Domain Discover
- Proofpoint Threat Response Auto-Pull
- Proofpoint Closed-Loop Email Analysis and Response
- Proofpoint Security Awareness

The Results

- Up-to-the-minute email security minimises phishing and other threats
- Automated email security minimises manual processes
- Security awareness training strengthens global security posture

The Organisation

With over 20 locations worldwide and close to 8,000 associates, this medical device innovator knows how important it is to maintain digital trust in communications. The global service provider has a sterling reputation for developing innovative, life-enhancing medical devices. And it is committed to protecting its customers, employees, and brand. It also offers a unique combination of small-company service and attention with big-company resources.

The Challenge

Protecting healthcare customers and employees

The medical device company keeps its sharp competitive edge through its breadth of capabilities, end-to-end integration, technical expertise, and relentless focus on its customers and operational excellence. Like any global enterprise organisation, it relies on a secure network infrastructure to power all its business processes.

However, as the threat landscape evolved, the company's security team found it was spending too much of its time protecting company communications. The company's existing email security system was difficult to set up and align to its needs. And wasn't effective at stopping the latest threats.

"Our email security was not meeting the needs that we had," said the security manager at the medical device company. "We were getting a lot of threats coming through, including phishing and credential harvesting. We couldn't trust our existing solution the way we needed to, so it cost us a lot of time and resources to manually block the attacks. And to make matters worse, we realised our security awareness training wasn't really up to par."

The company decided to upgrade its system to provide more complete protection against advanced threats, including phishing, email fraud detection, and malicious domains that were misusing its brand. It wanted not only strong email security, but analytics and reporting to help make smarter, more strategic decisions.

The Solution

Moving toward a human-centric approach to security

The company considered several email security products to find what would best fit its needs. It chose Proofpoint, which offered the most complete and best-supported solution.

"We did custom reviews with competitive products, and the choice came down the support and the level of care we could get with Proofpoint," said the security manager. "Proofpoint provided us with a human-centric view of our organisation's security posture."

"Proofpoint delivers real resource time savings. It enables our team to be more proactive in our approach to security, instead of reactive as we had been in the past. In a certain way, we can use Proofpoint as another team member."

Security manager, medical device company

The security manager and his team deployed several solutions that work together smoothly to stop malware, phishing and fraud, while automating security operations and threat response.

"Proofpoint Email Protection, along with Proofpoint Targeted Attack Protection (TAP), Proofpoint Threat Response Auto-Pull (TRAP), and Proofpoint Closed-Loop Email Analysis and Response (CLEAR), work together to close the whole loop for automated response," said the security manager. "They eliminate the need for us to do a lot of manual work investigating threats."

The security manager and his team took advantage of Proofpoint training to ensure a smooth onboarding process and painless migration to the new solution.

"The experience definitely made a difference," said the security manager. "Proofpoint has a playbook approach. You run through it, and it makes sense. We could progress as fast or slow as we needed to go."

The migration process also helped the company strengthen its Domain-based Message Authentication, Reporting, and Conformance (DMARC) policies for better defence against email spoofing and fraud attacks.

"Our DMARC policies were generally quarantine, because I didn't have good visibility into all my senders," said the security manager. "We got a better understanding of it during our migration process. We gained visibility into all emails sent using our domain. And this drastically helped us with our Proofpoint Email Fraud Defense implementation."

Proofpoint Email Fraud Defense also gives the organisation visibility into lookalike domains that could be used for phishing websites and email attacks. To further protect the organisations' reputation, the security manager recently added Proofpoint Virtual Takedown. This is an additional service that helps the company manage the process of blocking and shutting down malicious domains.

The team also knew the pivotal role that employees play in defending the organisation. To strengthen that, the security manager purchased Proofpoint Security Awareness, which uses a data-driven approach to training to foster a culture of security best practices.

"We run a quarterly training programme for all associates, and we require 100 percent participation," said the security manager. "We are really strict on that."

The Results

Minimising risk, while developing insights

The full portfolio of Proofpoint Email Security and Protection solutions has enabled the company to strengthen and automate its analysis, protection, and remediation of email threats, such as phishing and malware. The solution helps keep the organisation and its customers safe, but also reduces the workload on its security team.

"Every time we get any sort of security incident it all has to be recorded and categorised in our system," said the security manager. "We went from 800 to 1,000 tickets a month for issues, down to under 150. It was a vast reduction, and it freed up our resources from manual tasks."

Proofpoint TAP has also been useful in giving the security manager and his team real-time visibility and insights into threats and their targets, which are consolidated into a dashboard view. The solution has been especially effective at safeguarding employees in sensitive positions who were subject to the most threats. The analysis provided by Proofpoint helps the company understand the threat patterns, trends and targeting of its Very Attacked People (VAPs)™.

"We've taken that information from the most targeted and attacked people and built some custom Microsoft conditional access policies to make sure that they're being protected as much as possible," said the security manager.

The security manager also appreciates the solution's reporting capabilities, which save the security team time, and help them keep executives informed about the company's overall security posture.

"The level of support we get from Proofpoint has really been one of the one of the main benefits for us," said the security manager. "The reporting saves us time and gives us a view of all the data. And it's put together in a way that enables us to change our behaviours and take a more proactive approach to security. We can also use it to create different presentations for our executive leadership meetings to help them understand email threats and how we are managing them. We use the Proofpoint Security Awareness reporting as well, to drive awareness and education."

With Proofpoint products, services and training in place, this medical device innovator can now progress from simply responding to new threats to a more strategic security approach – one that brings together the best of people and technology.

LEARN MORE

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