proofpoint.

CUSTOMER STORY

FirstPort Enlists Proofpoint to Help Plan Ahead for the Evolving Threat Landscape

FIRST PORT

The Challenge

- A shift in the workforce to remote work, happening almost overnight
- Lack of visibility into who was being targeted, how and when
- Keeping up with the ever-evolving threat landscape

The Solution

- Proofpoint Email Protection
- Proofpoint Internal Mail Defense
- Proofpoint Threat Response Auto-Pull
- Proofpoint Targeted Attack Protection

The Results

- Significantly improved detection rate of potentially dangerous emails
- Increased visibility of threats and who they are targeting
- Increased team productivity, saving days in remediation tasks
- Better customer support

The Organization

FirstPort is the UK's leading full-service residential property manager. Its resume is impressive. With over four decades of experience, it looks after 232,000 homes in England, Wales and Scotland. And it spans more than 4,200 developments. The firm holds a five-star rating from the British Safety Council, has been awarded the British Safety Council's prestigious Sword of Honour, and is the accredited Safe Agent that belongs to The Property Ombudsman. But accolades aside, a company with so much responsibility also needs the ability to scale and evolve successfully.

The Challenge

The security team at FirstPort had a complex challenge on their hands. When the global pandemic forced 3,500 employees into remote working almost overnight, the organization had to scale up its technologies to adapt to the new way of working. At the same time, with the threat landscape evolving like never before, FirstPort also had to upgrade its infrastructure to keep pace with a new generation of cyber threats.

The rapid rise in remote working has created a larger attack surface for cyber criminals. As traditional infrastructure perimeters expanded to more home offices, businesses in every industry needed to take proactive steps to safeguard their employees from potential attacks with comprehensive protections and controls.

FirstPort needed deeper insights into how and when their people were being targeted remotely, through the No. 1 threat vector—email. The company was facing increasingly targeted and sophisticated attacks. And attackers were impersonating its trusted business partners and regulatory organizations. These threats were getting through its existing email security solution, and the FirstPort team realized they needed to implement multiple layers of defense.

> "Proofpoint has ensured that we are always at the forefront when it comes to battling email security threats. It provides us with ample information so we can make well-informed decisions based on real-time insights. And it gives us the capacity to plan ahead."
>
> **Sawan Joshi**, head of information security at FirstPort

"Today's cyber criminal is not just someone in a dark room on a computer. We are seeing a rise in the likes of advanced threats and organized crime organizations. These guys do research before they launch an attack. They get to know your organization, your social presence, your colleagues and employees. They get to know who your partners are and who your customers are. They take the time to understand how your business works before launching an attack. We need extended visibility to enable us to protect against these sophisticated threats," explained Sawan Joshi, head of information security at FirstPort.

FirstPort also continues to grow as a business at an exponential rate, making it crucial that the security team keeps a close eye on the evolving security landscape. And at the same time, they need to continually measure its security posture to ensure their employees and data stay protected. And they also need to train their users to be a strong last line of defense.

The Solution

Email remains the No. 1 threat vector

More than 90% of targeted attacks start with email, according to the Verizon 2018 Data Breach Investigations Report. And these threats are always evolving. As more organizations shift to remote work, threats have even more opportunities to develop across the extended attack surface.

FirstPort deployed Proofpoint Targeted Attack Protection (TAP), an advanced solution that detects, analyzes and blocks advanced threats before they reach users' inboxes.

TAP combats ransomware and other advanced email threats that are delivered through malicious attachments and URLs, zero-day threats, polymorphic malware, weaponized documents and phishing attacks. It also detects threats and risks in cloud apps, connecting email attacks related to credential theft or other attacks. This is increasingly critical as more employees access sensitive corporate data from outside usual office perimeters.

"We carefully researched a variety of solutions, and Proofpoint clearly provided the most robust protection and the maximum bang for our buck," said Joshi.

Innovation to keep pace with the evolving threat landscape

Built on Proofpoint advanced email security and cloud platforms, TAP gives FirstPort a unique architectural advantage. It provides clear visibility into all email communications and files in SaaS file stores. This gives the FirstPort team a far-reaching view of the threat landscape. And with TAP, they can discover and act on everything from banking Trojans and ransomware to targeted attacks, spear phishing, and resulting credential theft. Deep user-level and message-level context across email and SaaS make TAP especially effective at identifying hard-to-catch network threats that other solutions miss. Using TAP, FirstPort can:

- Block and quarantine messages with malicious attachments or URLs. With emails kept out of inboxes, users never click and become compromised.
- Submit attachments and URLs to our cloud-based scanning service to detect and inspect malicious content.
- Transparently rewrite all embedded URLs to protect users on any device or network.
- Track and block clicks to malicious web pages without affecting the user experience or other URL-filtering technologies they're using.
- Detect ransomware and malicious files in SaaS file stores and surface account compromise from brute-force attacks and more.

For an added layer of protection, the FirstPort team deployed Proofpoint Threat Response Auto-Pull (TRAP). This allowed them to analyze and move malicious or unwanted emails to quarantine after delivery. TRAP also follows forwarded mail and distribution lists and creates an auditable activity trail for full accountability.

The FirstPort team also uses Proofpoint Internal Mail Defense to help safeguard their internal email systems and detect compromised accounts. And it gives them the ability to take action to quarantine them.

Going forward, FirstPort also wants to empower its employees to take a more active role in security best practices. The FirstPort team is in the process of deploying Closed-Loop Email Analysis and Response (CLEAR), an integrated solution that streamlines end-user reporting and security response to phishing attacks. This will reduce the time they need to neutralize an active threat from days to minutes.

The Results

Proofpoint has enabled FirstPort to assume a more proactive security posture, taking rapid action to stop malicious activity before it can impact business processes—and its bottom line. For example, a phishing incident that occurred with its previous security solution infected 65 computers, which required 10 days to take offline and re-image. This disruption impacted not only business operations, but IT priorities. Now with Proofpoint TRAP, if an anomaly is detected, the solution will remove it from hundreds of mailboxes in seconds.

“The Proofpoint solution provides in-depth preventative protection, which helps us detect malicious activity,” said Joshi. “Not only does it provide an incredible SOC to track threats at the mail filter level, but it also gives us a fantastic response capability to detect and remove threats from mailboxes. It truly demonstrates the power of automation.”

Proofpoint also provides advanced reporting for visibility into the people most likely to be attacked, and the type of security threats the organization is facing.

“One of the things we like best about Proofpoint solutions and services is the reporting that gives us the ability to demonstrate ROI to our stakeholders,” said Joshi. “The quarterly business reviews with our Proofpoint representative are particularly valuable. They show us the most important risks we face today, and what matters most. These insights help us validate our strategy as we work with our business leaders.”

Migrating to a more automated email security solution also enables the FirstPort IT team to save time, so it can focus on adding more value to the business.

“Proofpoint technology supports and empowers our team. And it helps us to streamline our processes,” said Joshi. “It gives us automated response technology that can reduce any time we dedicate to manual repetitive tasks. This ensures the solution can adapt to changing business scale and allows us to focus on tackling potential threats.”

And with CLEAR, users can now report phishing emails with a single click and receive confirmation of legitimate threats through an email reinforcing their behavior.

“We have configured CLEAR and we like what we see,” said Joshi. “Enabling users to click when they spot a suspicious email and receive a customized acknowledgement is a great way to involve users in the journey. CLEAR lets us provide an easy, smooth user-friendly experience.”

“Proofpoint has ensured that we are always at the forefront when it comes to battling security threats,” said Joshi. “It provides us with ample information so we can make well-informed decisions based on real-time insights. And it gives us the capacity to plan ahead.”

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organizations’ greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.