proofpoint.

CUSTOMER STORY

MHA Keeps Critical Information Safe for Residents and Employees

mha
Live later life well

The Challenge

- Protect sensitive healthcare and financial data
- Minimize email security threats to keep operations running smoothly
- Help employees save time managing cybersecurity issues

The Solution

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

The Results

- Minimized business email compromise and blocked malicious URL and attachments, along with other malware and credential phishing lures
- Reduced spam volumes free up time and resources
- Proactive threat management and visibility improves IT efficiency

The Organization

The residents of MHA trust the organization with some of the most sensitive information about their lives, including healthcare and financial data. As the largest charity care provider in England, MHA considers its responsibility for this data an essential part of its mission to help its clients live the best lives they can. MHA offers a unique blend of care homes, retirement living and community groups embedded in local communities.

The Challenge

Keeping residents and their data safe and secure

Supporting more than 19,200 older people each year, MHA relies on its network infrastructure to keep its healthcare and administrative services running smoothly—and to provide services for residents. To maintain its sterling standard of excellence, the organization's IT team is continually improving the systems and processes.

"We offer technical support for a variety of organizational projects to make life easier," said Norman McKeown, associate director of IT at MHA. "For example, if they need connectivity for their smart TV, an Amazon Alexa device, or a PC to keep in touch with family members, we can implement, support and fix the technology."

MHA routinely handles a great deal of confidential data, so maintaining cybersecurity is top of mind.

"We hold residents' billing data and health data, which is very sensitive—and critical to securely manage," said McKeown. "To support healthcare and other services, our colleagues need technology that is easy to use, but highly functional."

To keep its operations and technology fully up to date, MHA was in the process of

moving to a new, cloud-based set of work applications. As part of the migration, the IT team also took a close look at its security posture.

"We did have some email protection, but being on legacy systems, it was fairly rudimentary," said McKeown. "We were getting a lot of the typical attacks, including spam and phishing attacks as well attacks impersonating our CEO and our finance director. We didn't have the level of protection we needed, so one of our first focuses was on an email security platform to improve that."

"Proofpoint has helped us progress from firefighting to being proactive. We don't have to worry about users clicking on malicious links, of putting the credentials into false websites—and all the remediation that those issues require."

Norman McKeown, associate director of IT, MHA

The Solution

A core solution for email security

MHA evaluated several different solutions, but chose Proofpoint because of its strong rating by Gartner, its advanced capabilities, and understanding of its mission.

"Proofpoint was one of the vendors who really understood what we were trying to do as an organization," said McKeown. "They were willing to work with us, not just in terms of the services they were providing, but in keeping us informed about what's coming next that could benefit us."

The organization chose the Proofpoint Core Email Security Solution, including Proofpoint Targeted Attack Protection (TAP) and Proofpoint Threat Response Auto-Pull (TRAP). Proofpoint Email Security helps the organization detect and block malicious and non-malware email threats, using Proofpoint Nexus® technology. Proofpoint Nexus combines semantic and behavioral AI, machine learning and real-time threat intelligence to offer multilayered protection. For example, Nexus Language Model (LM) for BEC carefully examines email content to detect common threats found in business email compromise (BEC) threats, such as transactional language or urgency. Nexus LM identifies suspicious emails before they can cause harm to the organization.

"Proofpoint was easy to configure and easy to integrate into our Microsoft 365 platform," said McKeown. "We didn't have to do any training for users, except advise them to hit the 'report spam' button if spam comes in. So users don't even have to think about it. And the solution is simple for us to support as an IT organization."

The Proofpoint solution also helps McKeown, his IT team and the organization gain better visibility into threats.

"The reporting that we get from the online portals is useful," said McKeown. "Whether it's the volume of email blocked, or the top 10 addresses that are attacked, it is clear and easy to interpret. You don't need to be an expert in the system."

The Results

Security aligned to business outcomes

The Proofpoint bundle, including Proofpoint TAP, has proven effective at helping the organization defend against business email compromise (BEC) and supplier account compromise threats. By ensuring the integrity of email communications, the solution has freed the MHA team from worrying about security issues, so employees can spend more time focusing on their jobs.

"We don't need to worry about people impersonating our finance director, saying 'I need this payment sent urgently,'" said McKeown. "It allows us to then focus on critical problems—not having to deal with the routine chance attacks on our organization. That's absolutely the number one benefit—it has given the whole organization peace of mind."

"With Proofpoint TAP, we don't need to have people sitting scanning email every day," he added. "It picks up threats, and we are automatically alerted. The drop in the volume of both malicious and spam communications has been significant. We're blocking anywhere from 75,000 to 125,000 emails a month coming into our system—which is a significant volume."

By automating and blocking more threats, the organization has also dramatically reduced the workload on its IT organization. This is an important achievement for a lean, budget-conscious charity organization.

"We've gone from averaging 14,000 to 15,000 tickets open at the end of every month—some being several months old—to between 50 and 100, which has given us the time to be proactive," said McKeown. "A lot of that has been because of the enhanced protection we've put in place. That has been a big improvement and has allowed the team to focus more on what we want to do next."

McKeown is also pleased with the support he has received from Proofpoint, provided by an organization that understands his business operations and priorities.

"The Proofpoint team also helps us address any problems we have and provides valuable guidance on issues," said McKeown. "It's great knowing that we've got a relationship where we can just pick up the phone and get the answers we need."

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. 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 85 percent of the Fortune 100, 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**.