CUSTOMER STORY

Egress and Spear Shield enable Hopkins Homes to remediate email security threats in real-time and enhance cyber awareness training

Property developer | East Anglia, UK | Egress Defend

The challenge

With a rapidly expanding workforce, and construction site locations across the South-East, Hopkins Homes was growing rapidly and had more people accessing its systems and data than ever before. With new people joining the organization, accessing company systems from multiple locations and devices, email security was a board-level priority.

"Our original email security solution combated potential phishing threats by indicating when an email was from outside the company. It would add 'external' to the email's subject line. And over time, as emails went back and forth, all the user could see on the subject line was numerous 'external' denotations, making it impossible for people to see the initial subject. We were frustrating our users more than anything — I was getting lots of complaints," said Jenny Carter, IT Systems and Development Manager at Hopkins Homes.

In addition, Carter wanted a solution to help augment Hopkins Homes' security awareness and training (SA&T) program. "We have some cybersecurity training and phishing simulations; typically, employees would participate in that training during their onboarding process and then not encounter it again. We wanted a solution that would help our users become more security-aware."

The solution

Working closely with leading cybersecurity specialist, Spear Shield, Hopkins Homes undertook a technical assessment of Egress Defend. It was felt that the solution would not only complement their existing Microsoft 365 environment, but that the real-time, interactive, color-coded banners perfectly aligned with the organization's SA&T strategy.

Hopkins Homes decided to undertake a proof of concept with Defend to ensure the solution met its needs. "The initial PoC to a subset of employees ran for two weeks and in that time we saw immediate benefit. We were really impressed with the solution, which highlighted and warned users of potentially dangerous emails. As a result, we made the decision to roll out Defend site wide. With the support of Spear Shield, the deployment took less than an hour. In fact, we spent more time talking about setup than it actually took to do it!" Carter said.

Not only does Defend help Carter's team mitigate potential attacks, but through the real-time teachable moments, it helps train users to spot potential email threats, therefore raising security awareness across the organization. "Egress warns users when an email is potentially dangerous and makes them think about it — and that continuous reinforcement is so powerful. To have that enhanced protection on the email when it comes in — having those extra layers to try and stop users from clicking through to potentially malicious links is extremely useful," said Carter.

In addition, Defend's sophisticated reporting and analytics platform ensures the Hopkins Homes security team can immediately identify and remediate email threats in one simple step. "I leave on the default administer notifications for when someone receives a dangerous or suspicious email. And if a user clicks on it, I get notified. From that point of view, it's great to get an overview of what's coming in," Carter explained.

"If users get something like an impersonation email, I get notified and can immediately click into it and review it before it gets sent to everyone else. Attackers are notorious for sending impersonation emails to multiple people in a company. Previously, if we saw an email impersonating one of our executives, I'd email around the company and say, 'We received this email — if you receive it, watch out for it and delete it.' Now, with Defend, I can stop it straightaway, remediating the issue and blocking the sender from our other systems. I'm able to remediate dangerous emails from everyone's inbox, potentially before they've even opened them," said Carter.

> "If users get something like an impersonation email, I get notified and can immediately click into it and review it before it gets sent to everyone else. (With Egress Defend) I'm able to remediate dangerous emails from everyone's inbox, potentially before they've even opened them.

Jenny Carter, IT Systems and Development Manager, Hopkins Homes

> I think it's good to put the ownership of these emails back on to the user. Because ultimately, we're just one team, regardless of size, you can't see everything, and you have to trust your people not to click. Defend's banners and the rewriting of the links are invaluable. There's just that extra layer of protection.
>
> Jenny Carter, IT Systems and Development Manager, Hopkins Homes

The results

Working with Spear Shield, Hopkins Homes has been running phishing simulations and Egress Defend in tandem, and metrics show that the company's two-prong approach has had a positive impact. "The first simulation we did after Defend had been in place for a few months showed that only about 3% of all staff clicked on links," Carter shared.

Hopkins Homes' IT team appreciates that Defend helps empower users to make smarter email security decisions. "I think it's good to put the ownership of these emails back on to the user. Because ultimately, we're just one team, regardless of size, you can't see everything, and you have to trust your people not to click. Defend's banners and the rewriting of the links are invaluable. There's just that extra layer of protection," said Carter.

"I've been onboarding new staff recently, and I told them, 'If Defend tells you not to click through, then unless you know with 100% certainty where it comes from, just listen to what Defend is telling you and don't click through.' Having that extra layer of protection and putting the onus of it back on the user is a weight off my mind," she concluded.