KnowBe4

Case Study

SHIELDS
HEALTH SOLUTIONS

1491	743
phishing attacks bypassed Microsoft 365	attacks sent from compromised accounts

82

potential data loss incidents prevented in 90 days

Beyond the SEG

KnowBe4 transforms email security at Shields Health Solutions

The need to protect patient privacy in a remote environment

As a leading pharmaceutical organization, it is crucial for Shields Health Solutions (Shields) to guarantee the safety and confidentiality of sensitive patient data on email.

With most Shields employees working remotely, Rob Fountaine, Principal Security Engineer at Shields, explains: "Email is an essential but ultimately dangerous tool we use every day. Whether it's interacting with targeted phishing emails like business email compromise, sending sensitive information to a personal email address or not applying the right security – any mistake puts our sensitive data at risk."

Observing the limited detection capabilities of secure email gateways (SEG) and the overlap in functionality offered by Microsoft 365's native security controls, Rob concludes: "We wanted a single platform to plug the gaps in Microsoft 365 and defend against the entire range of advanced inbound and outbound threats over email. In addition, we wanted the platform to provide in-the-moment prompts to enhance employee's security awareness without disrupting workflow."

KnowBe4 intelligently eliminates the full spectrum of email-based threats

Following a successful pilot, Shields implemented the full KnowBe4 Cloud Email Security platform across all 2,000 users to address the security limitations they recognized in their native security platform. Comprised of KnowBe4 Defend™, KnowBe4 Prevent™, and KnowBe4 Protect™, the platform seamlessly integrates with Microsoft 365, utilizing AI models and an adaptive security architecture to detect and respond to threats, as well as providing real-time nudges to alert users before security incidents can occur.

> *"The Defend banners have been game-changing. Not only are users stopping to pay attention to the banners and understand the threat, but ... we have seen a dramatic decrease in click rate."*
>
> Rob Fountaine, Principal Security Engineer, Shields

At a glance

▶ Recognizing gaps in their Microsoft 365 email security, Shields Health Solutions (Shields) wanted to implement an integrated cloud email security platform to eliminate email-based threats that could put patient data at risk.

▶ Shields now leverages KnowBe4's Cloud Email Security platform to detect and neutralize sophisticated inbound attacks, prevent misdirected emails and attachments, and ensure the appropriate security is applied to sensitive communications.

Defend leverages pre-generative and zero-trust models, as well as linguistic, contextual, and behavioral analysis to detect sophisticated phishing attacks such as business email compromise. On the outbound, Prevent and Protect combine contextual machine learning, intelligent DLP and encryption to ensure emails are sent to the correct recipients, containing the right information, and are appropriately protected relative to the level of risk.

"The Defend banners have been game-changing," explains Rob. "Not only are users stopping to pay attention to the banners and understand the threat, but since we incorporated them into our phishing simulation campaigns, we have seen a dramatic decrease in click rate. In addition, the Prevent prompts allow users to make an educated decision when sending an email, and I know that every single time a user accepts advice, we may have just avoided a serious data loss incident."

Defend detects 1491 more attacks than Microsoft 365

In a 90-day period, 1491 phishing emails bypassed Microsoft 365 and were identified and neutralized by Defend, with 743 attacks that evaded native security came from compromised accounts.

In the same period, Prevent stopped 82 potential data loss incidents.

"If you are using Microsoft 365, it makes perfect sense to move towards a best-of-breed platform like KnowBe4 that can eliminate the full spectrum of inbound and outbound threats over email." says Rob. "Another thing we like about utilizing an ICES over a traditional SEG vendor is that we didn't have to alter our MX record, meaning there are less publicly available indicators for threat actors to exploit."

Rob and the security team at Shields were particularly impressed with KnowBe4's remediation capabilities. "With Defend, the dashboard gives us a holistic view of the types of threats targeting our organization which we can then use to tailor our internal phishing campaigns. Conversely, Prevent and Protect analytics give us granular insights into what type of advice is being accepted to continually assess email security policies."

Rob concludes: "We were looking for a new platform that went above and beyond the SEG – and that's exactly what KnowBe4 has given us. KnowBe4 has optimized every aspect of our email security, from detection and remediation to security awareness training."
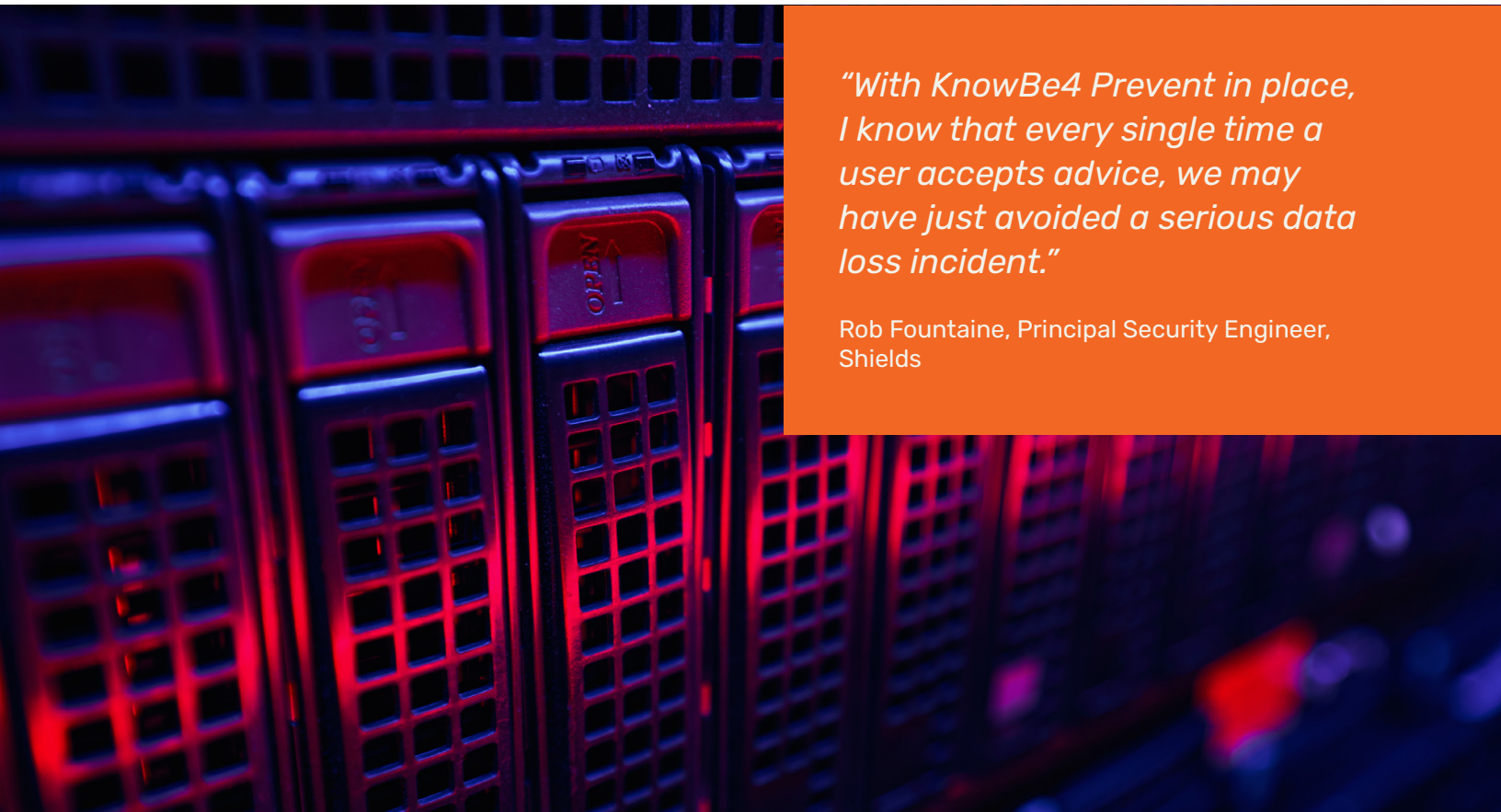
> *"With KnowBe4 Prevent in place, I know that every single time a user accepts advice, we may have just avoided a serious data loss incident."*
>
> Rob Fountaine, Principal Security Engineer, Shields

KnowBe4

01F01K3