CASE STUDY

egress

Crawford selects Egress Defend and Prevent to enhance Microsoft 365 email security

The client

Crawford & Company® is the world's largest publicly listed independent provider of claims management and outsourcing solutions to carriers, brokers and corporates, with an expansive global network serving clients in more than 70 countries.

Founded in 1941, Crawford has continually expanded its product offering, and today pairs traditional services and technology-driven innovations to handle clients claims quickly and affordably.

Egress products:

- Defend
- Prevent

M365 EMAIL CLIENT

LEGAL

11,000 EMPLOYEES

> We selected Egress Defend and Prevent as added security layers in our Microsoft 365 environment to ensure we are minimising our risk profile.
>
> DANIEL VOLK, CIO, CRAWFORD & COMPANY

As part of building trusted and long-lasting relationships with their clients, Crawford is dedicated to preserving confidentiality and protecting sensitive and proprietary data. As a result, the provider's Security team continually analyses the cyber-threat landscape and evaluates new technologies that can help them to reduce risk.

With the ongoing evolution of phishing attacks and the increase in advanced threats targeting all organisations, the Crawford team undertook a project to ensure they had the highest levels of email security within their Microsoft 365 environment. This included detection and mitigation of all types of phishing attacks, including business email compromise (BEC) and impersonation attempts, supply chain compromise, and highly targeted spear phishing.

Enhancing Microsoft 365 threat detection with Egress

As part of this process, Crawford engaged with Egress, the leading provider of human layer security solutions designed to intelligently mitigate inbound threats and protect outbound data as it's shared by employees. With Exchange Online Protection already deployed within their Microsoft 365 environment, Crawford wanted to determine the benefits offered by adding an intelligent anti-phishing solution to their security software stack, and consequently began evaluating Egress Defend.

Defend is the only anti-phishing solution globally to utilise a zero-trust model for inbound phishing detection. The solution uses machine learning and natural language processing (NLP) technologies to analyse the content and context of every email before it is delivered to a recipient's inbox, including the sender and their domain, all hyperlinks and attachments, and the language used within the message. Defend also analyses hyperlinks at the point of click, meaning it can detect malicious links that are weaponised after delivery.

Additionally, the solution provides active learning through a traffic-light warning system and interactive banners that offer insight into phishing attacks, improving employee engagement and effectively contributing to their security awareness training in real time.

ENHANCE MS EXCHANGE ONLINE PROTECTION

ZERO-TRUST MODEL FOR ADVANCED PHISHING DETECTION

PREVENT EMAIL DATA LOSS WITH CONTEXTUAL MACHINE LEARNING

With Exchange Online Protection already deployed within their Microsoft 365 environment, Crawford wanted to determine the benefits offered by adding an intelligent anti-phishing solution to their security software stack, and consequently began evaluating Egress Defend.

Preventing outbound email threats

While evaluating Defend, the Crawford team also examined how Egress Prevent could reduce the risk of outbound data loss as employees use email to communicate with clients and third parties. Recognising that human error is the primary cause of email data loss for organisations, Crawford examined how Prevent's use of intelligent machine learning technology could provide added security for their employees.

Prevent leverages contextual machine learning and social graph technologies to analyse the real-time risk to data as it is shared by email. This includes analysis of the recipient and their domain, as well as understanding relationships between the sender and their recipients, including the types of data they normally share. This enables Prevent to detect and mitigate instances of outbound email loss such as adding the wrong recipient, attaching the wrong document, or failing to use the Bcc field.

The solution's unobtrusive prompts only display when risk is detected, providing explanations to employees to increase their understanding and enable them to correct their mistakes. Prevent can also block risky behaviour and exfiltration attempts.

Selecting the Egress Intelligent Email Security platform for added security in Microsoft 365

After a robust evaluation, in June 2021 Crawford selected Defend and Prevent to enhance their email security.

Daniel Volk, CIO at Crawford, commented: "We selected Egress Defend and Prevent as added security layers in our Microsoft 365 environment to ensure we are minimising our risk profile as much as possible. Protecting our clients' data is of the highest importance to us, and by using Defend and Prevent we aim to enhance that security through the detection of advanced phishing attacks and the reduction of human error."

About Egress

Our mission is to eliminate the most complex cybersecurity challenge every organisation faces: insider risk. We understand that people get hacked, make mistakes, and break the rules. To prevent these human-activated breaches, we have built the only Human Layer Security platform that defends against inbound and outbound threats.

www.egress.com
info@egress.com
0203 987 9666
@EgressSoftware