KnowBe4

KnowBe4 Defend™

Behavior-Based Email Security That Detects and Prevents Advanced Phishing Attacks

KnowBe4 Defend uses AI to detect and prevent the full spectrum of advanced phishing attacks. Leveraging machine learning, natural language processing, and natural language understanding, Defend detects the attacks that get through native security and Secure Email Gateways, including business email compromise.

Part of the KnowBe4 Cloud Email Security portfolio, Defend leverages an adaptive security architecture, automatically improving its security detection based on real-time risk assessments.

Defend's self-learning detection technologies require minimal configuration and ongoing maintenance from admins.

Intelligent Anti-Phishing Detection

KnowBe4 Defend inspects emails using a combination of intelligent technologies, including machine learning, social graph and natural language processing. By learning email behavior patterns, it detects anomalies that are indicative of advanced phishing threats that get through native email security and secure email gateways.

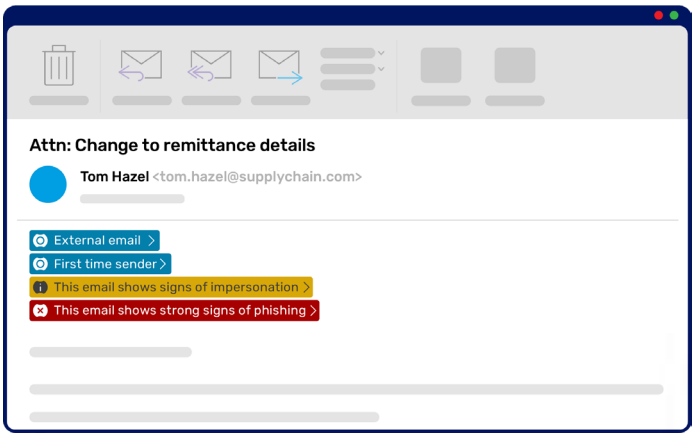
This allows Defend to detect email attacks early in the cyber kill chain, protecting against threats such as ransomware. Defend's self-learning detection technologies require minimal configuration and ongoing maintenance from admins. Plus, Mail Security Orchestration, Automation and Response (M-SOAR) capabilities provide actionable intelligence for rapid incident response and remediation to reduce Mean time to repair (MTTR).

Dynamic Anti-Phishing Controls That Lower Admin Overheads

The Cloud Email Security Center provides campaign-level remediation to ensure administrators, with one click, can remove thousands of threats from the inbox after investigating just one email. Subsequently, Defend will dynamically improve its detection to prepare customers for phishing threats before they materialize.

Key Benefits

- Protects organizations against the full spectrum of phishing attacks
- Uses an adaptive secure architecture to automatically improve inbound security detection based on risk
- Real-time teachable moments augment security awareness and tangibly reduce risk
- Significantly lowers administration overhead with intelligent self-learning threat detection
- Increases employee productivity with automatic classification and relocation of graymail
- Augments M365 native security to detect advanced phishing attacks
- Automated deployment in the mail flow to avoid the risks inherent in API-only implementations
- Lowers time to respond and remediate email-related incidents



Reduce User Friction By Engaging Only When Risk is Evident

KnowBe4 Defend only quarantines the most dangerous phishing emails, while neutralizing and presenting contextual, color-coded educational banners within the email itself to other threats for real-time teachable moments to your users. These real-time teachable moments reinforce security awareness training at the point of risk using real threats, increasing its effectiveness and helping to realize a better ROI. People are educated on why a phishing email has been flagged as suspicious, instead of it being automatically quarantined.

Key Features

- **AI-enabled phishing detection:** Defend delivers the highest efficacy of threat detection for your organization through a combination of self-learning techniques, pre-generative modeling, behavioral intelligence, language processing engines, and automation.
- **Adaptive security architecture:** Defend automatically improves security detection for each of your users based on calculations from all emails processed by Defend.
- **Machine learning and linguistic analysis:** Self-learning technology develops baselines for your users' behavior to detect and flag anomalous activity. Natural language processing (NLP) and natural language understanding (NLU) determine the emotion, intent, and context behind every email, enabling the detection of unusual, suspicious, and threatening behavior.
- **Holistic detection:** All aspects of an inbound email are analyzed in unison, enhancing detection efficacy for your organization versus traditional anti-phishing and malware products that analyze these in isolation.
- **Contextual warning banners:** Dynamic color-coded banners change based on the level of risk, offering clear explanations and engaging your users through real-time teachable moments.
- **Neutralize malicious code:** Active and malicious code is automatically disabled from HTML message body and attachments in your emails.
- **SSO enabled:** Integrates directly into your organization's Single Sign On (SSO).
- **Sender analysis:** Sender policy verification lookup and validation are performed on every message for SPF, DKIM and DMARC to protect your organization.
- **Link rewriting:** Stops time-based attacks by rewriting links and checking at time-of-click. Unsafe links are redirected to a warning page with easy-to-understand contextual details and used as teachable moments for your users.
- **QR code detection:** Detects QR codes within email to warn your users of quishing attempts.
- **Abuse mailbox automation:** Reduce your security overhead and time to respond with advanced AI-powered phishing investigation and remediation.
- **Intelligent graymail detection:** Improve your users' productivity and reduce your admin burden by automatically filtering graymail to a separate folder.
- **Seamless integration with Microsoft 365:** Integrates seamlessly into your MS Outlook apps on Windows Desktop, Mac, iOS, and Android, including integration with MS Safelinks. Defend operates after your SEG, and/or Microsoft 365 has performed any analysis at the perimeter.
- **Detailed analytics:** The Security Center provides you with a single portal for risk analysis, reporting and incident triage, investigation and response for all your KnowBe4 Cloud Email Security products (Defend, Prevent, Protect), including a live threat feed.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com