DARKTRACE

Why Email Security + Security Awareness Training Are Stronger Together

Darktrace / EMAIL + Darktrace / Adaptive Human Defense

Closing the gap between email protection and security training

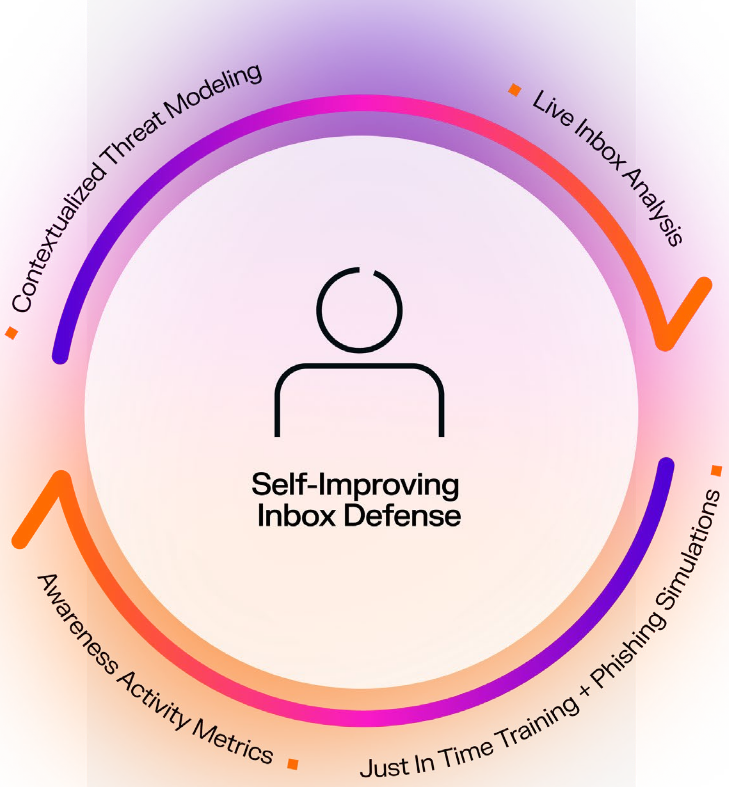
The combined power of Darktrace / EMAIL and Darktrace / Adaptive Human Defense creates the industry’s first self-improving email defense – a continuously adapting system where users learn from real, live threats, and detection becomes more accurate as human behaviors evolve.Every interaction reinforces the next. Every user action becomes intelligence. Every detection event becomes a learning moment. This is the closed-loop of AI-native human defense: security that learns from people, and people who learn from security.

Combining **Darktrace / EMAIL** and **Darktrace / Adaptive Human Defense** with a Closed-Loop that continuously reinforces Email Security and Awareness Training

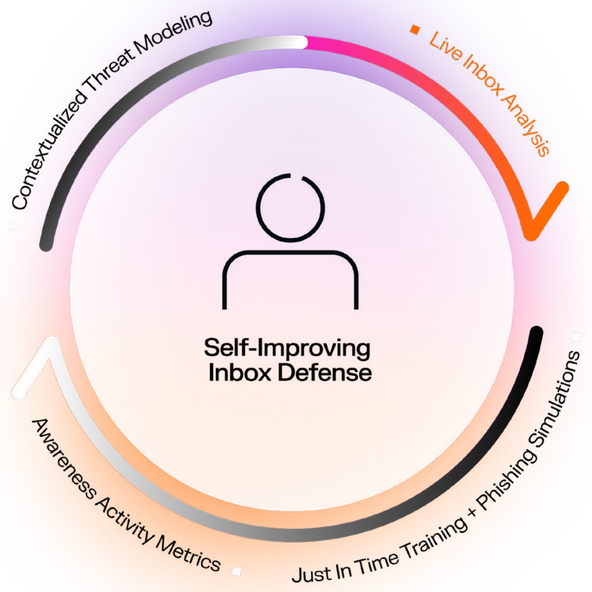
User Benefits

- Personalised Training
- Timely Interventions
- Safer and more organized Inbox
- Faster skill development

Darktrace
/ EMAIL



Darktrace
/ Adaptive
Human Defense


Contextualized Threat Modeling
Live Inbox Analysis
Self-Improving Inbox Defense
Just In Time Training + Phishing Simulations
Awareness Activity Metrics

Value to customer

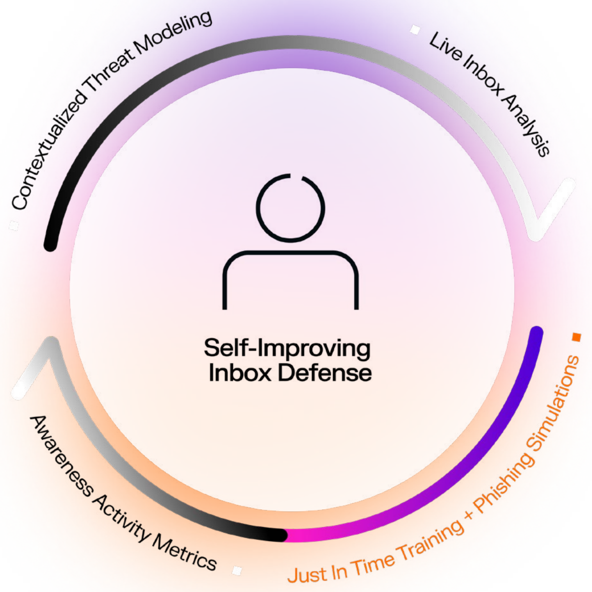
- Detects subtle, behavioral threats that signature-based systems miss
- Learns how your organization communicates and adapts automatically
- Identifies nuanced risks like tone shifts, unusual requests, or role-based anomalies
- Produces rich intelligence that enables personalized training and precise response

Stage 1: Live Email Analysis

The loop begins with Darktrace / EMAIL's deep analysis of every inbound, outbound, and internal message. Rather than relying on fixed rules, / EMAIL develops a behavioral understanding of how each individual and each relationship within the organization normally communicates. This includes tone, language patterns, cadence, roles, trust relationships, and typical communication styles. As the system observes real interactions over time, it constructs granular patterns of life that allow it to distinguish ordinary messages from highly subtle, human-targeted anomalies.

Every email is broken down into thousands of signals. These include routing and authentication markers, HTML and formatting structures, hidden content indicators, link and attachment characteristics, inducement language, tone and sentiment shifts, and topic changes. Behavioral and social-graph models work in parallel to identify unusual sender–recipient relationships, unexpected communication styles, or sudden shifts in behavior. Natural language processing uncovers financial requests, sensitive data, impersonation cues, and linguistic anomalies. All of these insights converge through multi-layered modeling to produce a set of characteristics and tags describing exactly which elements of the email may indicate risk.

These tags don't merely inform the final verdict – they are the raw intelligence that flows into the next stage of the loop. They become the basis for targeted user coaching and adaptive simulations, ensuring the training experience is driven by real threats and genuine user behaviors rather than generic templates.


Contextualized Threat Modeling
Live Inbox Analysis
Just In Time Training + Phishing Simulations
Awareness Activity Metrics
Self-Improving Inbox Defense

Value to customers

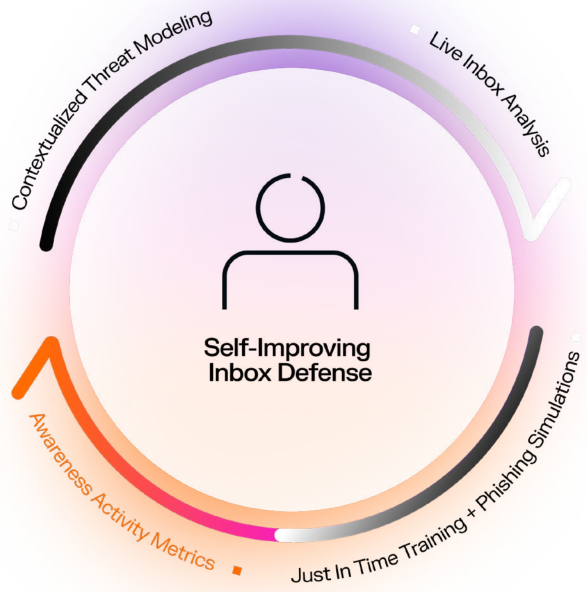
- Reinforces secure behavior in the moment of risk
- Simulations match each user's communication style and threat exposure
- Training intensity adapts to user performance and real-world danger
- High-risk users receive additional reinforcement while low-risk users avoid fatigue

Page 2: Just-in-Time Training + Adaptive Phishing Simulations

When Darktrace / EMAIL identifies suspicious characteristics in an email that is delivered to the user's inbox, those insights initiate contextual **Just-in-Time (JIT) training**. Instead of delivering training as a separate activity, Darktrace reinforces learning at exactly the moment a user is about to interact with a message that is potentially risky, but not risky enough to hold back entirely. When a user opens the relevant email, Darktrace injects micro-lessons via a banner in their inbox, relevant to the perceived characteristics within that email – for instance, references to bitcoin within the body of an email will trigger a micro lesson on cryptocurrency scams. This ensures the user learns from the exact scenario that prompted concern in the first place.

In parallel, EMAIL's intelligence shapes highly realistic and adaptive phishing simulations. These simulations evolve dynamically in difficulty and content based on the user's inbox behavior, communication patterns, and learning history. At higher difficulty tiers, simulations incorporate natural language analysis drawn from the user's real communication habits: preferred languages, writing styles, relationship contexts, and typical message formats. This makes advanced simulations feel authentic and relevant, mirroring the threats an attacker would realistically craft.

Timing and targeting are equally adaptive. Smart scheduling determines when to deliver training by analyzing each user's engagement with training, their risk exposure within the email environment, and their overall achievement scores across all training types. Users who struggle, who are more frequently targeted, or who exhibit high-risk behavior will naturally receive more tailored reinforcement. Users who perform well see training that is challenging but not burdensome.


Contextualized Threat Modeling
Live Inbox Analysis
Self-Improving Inbox Defense
Phishing Simulations
Just In Time Training +
Awareness Activity Metrics

Value to customers

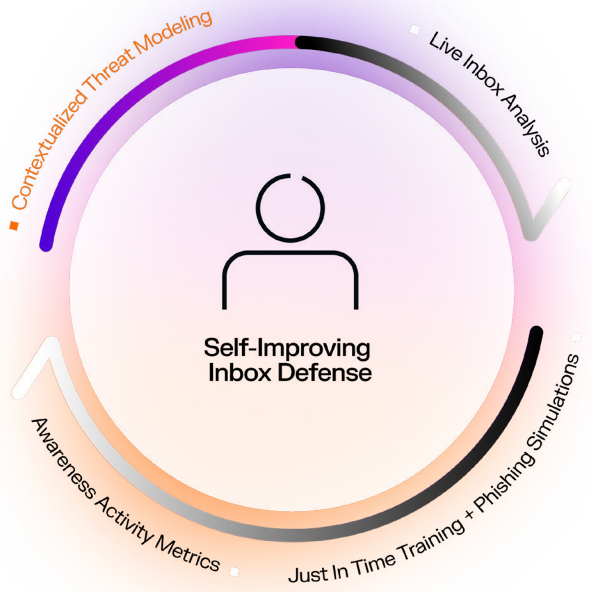
- Converts user behavior into measurable, actionable security intelligence
- Surfaces repeat offenders, high-risk users, and those needing intervention
- Shows true behavior change – not just module completion
- Builds a unified risk profile combining human and technical signals

Stage 3: Awareness Activity Metrics

Every interaction with Darktrace / Adaptive Human Defense – from JIT coaching to simulation responses to scheduled learning — produces a stream of behavioral signals that form each user's evolving risk profile. Instead of relying on completion rates as the only indicator of success, the solution evaluates learners across three dimensions: **Engagement, Risk, and Achievement**.

Engagement reflects how consistently and willingly a user participates in training, including whether they start lessons promptly, complete them fully, and engage with JIT modules when prompted. Risk captures how exposed a user is, taking into account EMAIL's ongoing analysis of targeting patterns, social-graph anomalies, and behavioral irregularities. Achievement represents whether the user actually understands what they have been trained on – measured through correctness rates, performance in simulations, difficulty levels reached, and improvements over time.

Together, these metrics provide a multidimensional understanding of human behavior that is far more meaningful than legacy SAT methods. Adaptive Human Defense transforms these findings into structured intelligence that is sent directly back into EMAIL's detection pipeline. Every piece of human-behavior data becomes part of the broader security model, helping EMAIL refine its understanding of both user-specific and organization-wide risk.


Contextualized Threat Modeling
Live Inbox Analysis
Just In Time Training + Phishing Simulations
Awareness Activity Metrics
Self-Improving Inbox Defense

Value to customers

- Intensified protection for high-risk users without burdening the entire organization
- Faster SOC response for trusted reporters
- Reduced false reports and operational fatigue
- Continuously improving detection driven by real user behavior

Stage 4: Contextualized Threat Modeling + Precision Inbox Actions

With human-behavior insights now incorporated, Darktrace / EMAIL recalibrates its detection and response models at the individual user level. EMAIL merges its original technical analysis with the human-learning profile generated by AHD to determine not only whether an email is risky, but how strongly to act on it, and for whom.

For users who demonstrate high risk —–whether because they are frequently targeted, struggle with specific threat types, or consistently make errors – EMAIL applies intensified protection. This may include stricter link locking, upgraded attachment handling, or boosted anomaly scoring for certain inducement categories. If a user repeatedly fails training on payment fraud scenarios, for example, EMAIL can automatically raise the severity applied to real payment-related anomalies in their inbox.

Conversely, users who show strong engagement, consistent accuracy, and reliable reporting can receive reduced friction and faster remediation pathways. If a trusted, low-risk user reports a suspicious email, EMAIL can treat it as a high-confidence indicator and initiate campaign remediation immediately. Likewise, overly cautious users who frequently misreport safe emails can have banner frequency reduced to prevent fatigue.

This dynamic adaptation not only tailors protection to each user but also improves SOC efficiency. By differentiating between risky behavior and reliable behavior, the system reduces noise, accelerates triage for credible reports, and improves overall detection accuracy.

To see the benefits of EMAIL + Adaptive Human Defense in your environment, click here to get a demo or speak to your account team.

Get a demo

Requirements & Deployment

Technical Requirements

- Darktrace / EMAIL deployment (Microsoft 365 or Google Workspace)
- Darktrace / Adaptive Human Defense cloud instance
- On-prem email environments are not supported

Deployment Overview

Adaptive Human Defense integrates natively with Darktrace / EMAIL. User and group data sync automatically from EMAIL, and JIT banners are applied directly through EMAIL's decision pipeline. No additional infrastructure is required. Once enabled, Adaptive Human Defense begins ingesting EMAIL's signals and generating adaptive simulations and behavioral metrics immediately. These metrics flow back into EMAIL to enhance modeling and autonomous actions.

About Darktrace

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,400+ employees who protect nearly 10,000 customers globally. To learn more, visit http://www.darktrace.com.

North America: +1 (415) 229 9100 | Europe: +44 (0) 1223 394 100 | Asia-Pacific: +65 6804 5010 | Latin America: +55 11 4949 7696