Darktrace / Adaptive Human Defense

Unified security awareness training and email protection delivering real-time, adaptive coaching

INDUSTRY CHALLENGE

Security training **isn't built** for modern attacks

Modern attackers no longer target just inboxes – they target humans and the productivity systems where work occurs.

When the workstream is the attack surface, humans are set up to fail. And the data shows that this vulnerability persists:

68% of all breaches involve a human element (Verizon DBIR 2025), and phishing remains the number one attack vector (IBM X Force 2025). Traditional programs were built for an era of generic, typo-ridden phishing emails – not highly personalized, context-aware, AI-generated attacks that are tailored to an individual's behavior.

With humans on the front line, you'd assume that effective awareness training which improves decision-making and creates a positive security culture would be a pre-requisite. Unfortunately, security awareness training (SAT) has remained a compliance exercise for organizations, optimized for completion rather than capability.

84% of organizations still measure success through completion rates, even though completion of standard training correlates with less than 2% real improvement in risky behavior.

(NIST; UC San Diego)

This compliance-first approach has left the workforce unprepared for the threats they actually face, with little to no thought for how SAT can improve defenses.

MARKET CHALLENGE

Why existing solutions don’t work

Security Awareness Training (SAT) tools have become a compliance staple, but the data shows they are not meaningfully changing individual or organizational behavior.

Most platforms rely on static learning modules and generic phishing simulations that are not tailored to individual risk profiles or real-world behavior patterns.

Effectiveness is typically measured by course completion rates rather than sustained behavior change, leaving organizations with little visibility into true risk reduction or return on investment. Critically, the insights gathered from simulations are rarely used to dynamically adapt training or strengthen controls, reducing SAT to a periodic, tick-box exercise.

While newer Human Risk Management (HRM) solutions incorporate live behavioral data, many still victim-blame, penalizing humans for mistakes rather than treating them as active contributors to strengthening organizational defenses.

Disadvantages of traditional SAT solutions:

Compliance-only mindset → Focused on ticking boxes, not driving real change.

One-size-fits-all training → Static modules that ignore user context.

Training fatigue → Overwhelming, repetitive content with low relevance.

Can’t keep up with threats → Static templates fail to reflect evolving attack techniques.

No support for good decision-making → Email environment doesn’t provide context to support learning.

Lack of behavior change → Users complete training but don’t alter risky habits.

High-risk user exposure → VIPs and sensitive roles treated the same as everyone else.

Backwards mindset → Employees are viewed negatively and punished for risky behavior.

Siloed from security stack → No connection to real threats or adaptive controls.

No clear ROI → Hard to measure cultural impact or risk reduction for leadership.

THE SOLUTION

Darktrace
/ Adaptive Human Defense

An **adaptive coaching platform** aligned to user behavior that delivers context-aware phishing simulations and native context signal sharing with email security.

SAT can't ignore compliance requirements (like content delivery and phishing tests), but compliance alone doesn't change behavior. Darktrace recognizes this, and is confronting the limitations of traditional SAT with an approach that combines compliance-ready training with continuous, behavior-led insights to help organizations move beyond box-ticking and toward measurable risk reduction and lasting security culture change.

/ Adaptive Human Defense

Darktrace / Adaptive Human Defense is the first AI-native unified engine that creates a closed loop between training behavior and email security.

When employees engage with realistic simulations, interact with coaching, or make decisions in real email scenarios, those signals become invaluable telemetry for the broader security ecosystem. Feeding this enablement data back into detection models continually sharpens an organization's defensive posture — adjusting policies, tightening responses, and improving threat interpretation automatically. Through this two-way flow of intelligence, employees don't just receive guidance; they strengthen the system with every decision they make.

HOW DOES IT WORK?

Traditional SAT components have been reimagined to deliver maximum learning potential for both the user and for the organization's understanding of risk. Instead of static modules or generic phishing templates, employees receive in-the-moment micro-guidance, context-responsive simulations, and short, engaging training aligned to real conditions, not theoretical ones.

This keeps people attentive, reduces training fatigue, and ensures compliance requirements are met without sacrificing relevance or engagement. The result is a security culture where the workforce stays informed about emerging threats, the defenses grow smarter through lived behavior, and both sides constantly reinforce one another in a continuous, dynamic cycle of protection.

Business benefits:

Fewer false alarms, reduced SOC workload:
Users learn to report phishing attempts more accurately, so your security team spends less time chasing false positives.

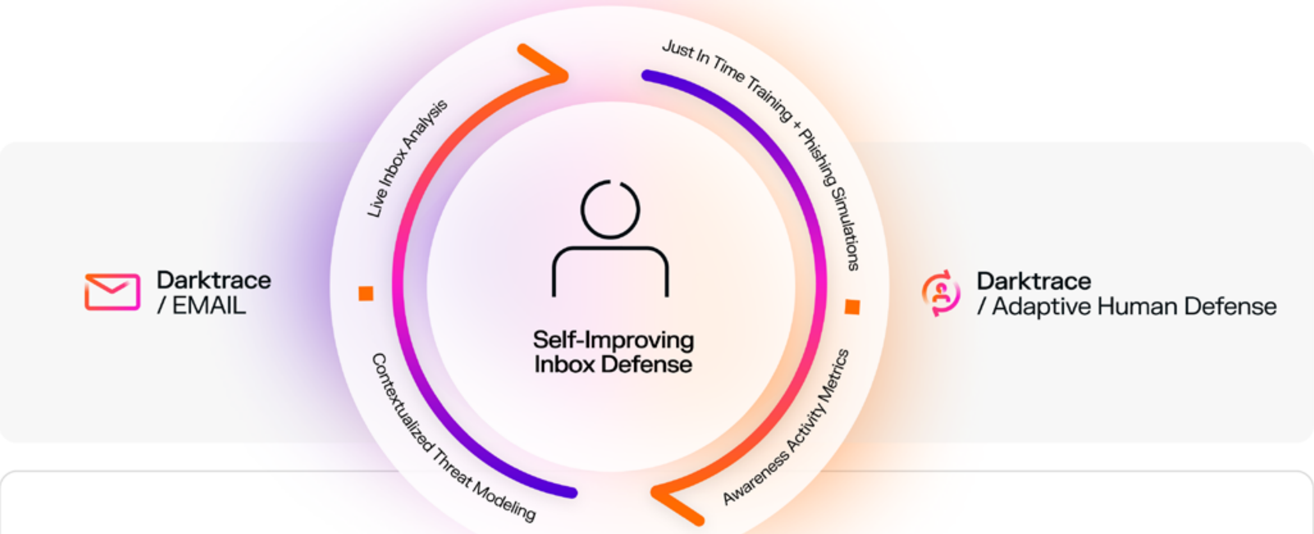
Risk reduction:
Email security adapts based on real user behavior, improving the precision of response actions where it actually matters.

Engaged employees, stronger security culture:
Personalized, dynamic learning motivates users and reinforces safe behavior across the organization.

Compliance that actually counts:
Helps meet regulatory requirements while delivering measurable risk reduction, not just a tick-box exercise.

Actionable insights and ROI:
Board-ready reporting shows real improvements in human risk, demonstrating the value of your investment.

Seamless security integration:
Works smoothly with your existing stack to reinforce defenses without disrupting operations.


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

Combining Darktrace / EMAIL and Darktrace / Adaptive Human Defense with a continous feedback loop that reinforces email security and awareness training

User Benefits

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

Key Capabilities

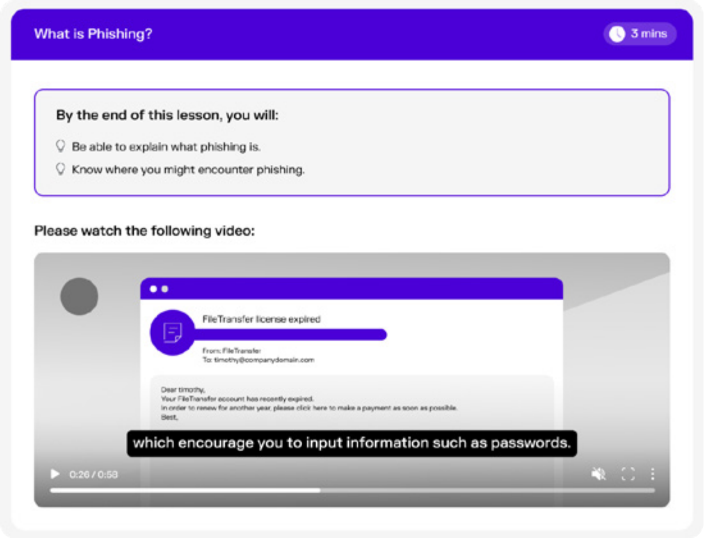
Contextual **human** enablement with personalized learning

Traditional SAT solutions lack dynamic learning, offering training that isn't personalized or contextual. The volume and time-suck of content creates training fatigue, as users are dealt repetitive content with low relevance. The result? Bloated one-size-fits-all modules that ignore user context and fail to deliver meaningful behavior change.

Darktrace / Adaptive Human Defense improves on the content, timing, and delivery of learning to turn it into true human enablement.

Scheduled learning looks more like traditional e-learning, delivered to users at a specified time and date. Admins can send content from the core library, which contains human-generated (non-AI), expertly curated, bitesize lessons on key cybersecurity topics.

They can also create custom training content for their organization, either by uploading SCORM content or using the course builder functionality to create bespoke lessons in-product.



What is Phishing?

3 mins

By the end of this lesson, you will:

- Be able to explain what phishing is.
- Know where you might encounter phishing.

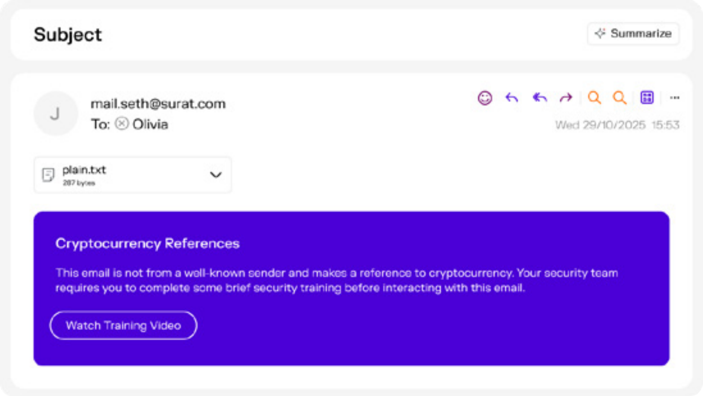
Please watch the following video:

FileTransfer license expired

From: FileTransfer
To: timothy@companydomain.com

Dear timothy,
Your FileTransfer account has recently expired.
In order to renew for another year, please click here to make a payment as soon as possible.
Best,

which encourage you to input information such as passwords.



Subject

mail.seth@surat.com
To: Olivia

Wed 29/10/2025 15:53

plain.txt
287 bytes

Cryptocurrency References

This email is not from a well-known sender and makes a reference to cryptocurrency. Your security team requires you to complete some brief security training before interacting with this email.

Just-in-time training doesn't need to be scheduled. The integration with Darktrace / EMAIL is leveraged to deliver micro-coaching just at the moment a user is about to take a risky action, managing risk in real time.

For instance, when an email is detected with anomalies which aren't strong enough to prevent delivery, a banner is added to the email describing its risky characteristics and providing a button to access relevant training.

These <1 min lessons cause minimum disruption to workflows while harnessing risky moments to deliver behavioral change and prevent compromise.

VIPs need special treatment

In traditional SAT, VIPs – the most targeted users for phishing – get the same training as everyone else. **Darktrace sends users real-world threats appropriate to their risk profile – so your most targeted people are protected.**

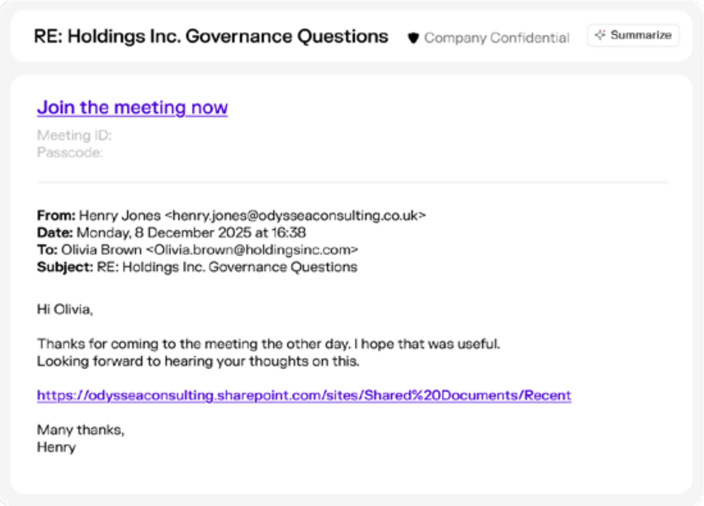
Adaptive phishing simulations for **real-world threats**

Most legacy programs use canned phishing lures and infrequent tests, don't meet the standards of real-world, evolving threats. The most sophisticated offering from the market uses defanged real threats to train employees, which don't progress and quickly become outdated – and they'll never appear in the inbox because they are known to email filters. In short, these phishing tests can't keep up with the pace of threats.

Darktrace uses AI to tailor intelligent phishing simulations that mimic evolving threats based on the context of each user and their role.

The difficulty of these attack scenarios adapts automatically based on user performance, allowing high performers to advance their skills and offering at-risk users targeted support. Upon a risky click, the user must complete a short e-learning module, turning that click into a learning moment.

The most advanced level simulations are crafted with AI based on analysis of recent phishing emails – integrating simulations directly into user conversations and creating a more immersive testing experience. Test campaigns can be fully automated or customized, allowing you to build tailored phishing templates to align with your unique organizational context if desired.



RE: Holdings Inc. Governance Questions

Join the meeting now

Meeting ID:
Passcode:

From: Henry Jones <henry.jones@odysseaconsulting.co.uk>
Date: Monday, 8 December 2025 at 16:38
To: Olivia Brown <Olivia.brown@holdingsinc.com>
Subject: RE: Holdings Inc. Governance Questions

Hi Olivia,

Thanks for coming to the meeting the other day. I hope that was useful.
Looking forward to hearing your thoughts on this.

https://odysseaconsulting.sharepoint.com/sites/Shared%20Documents/Recent

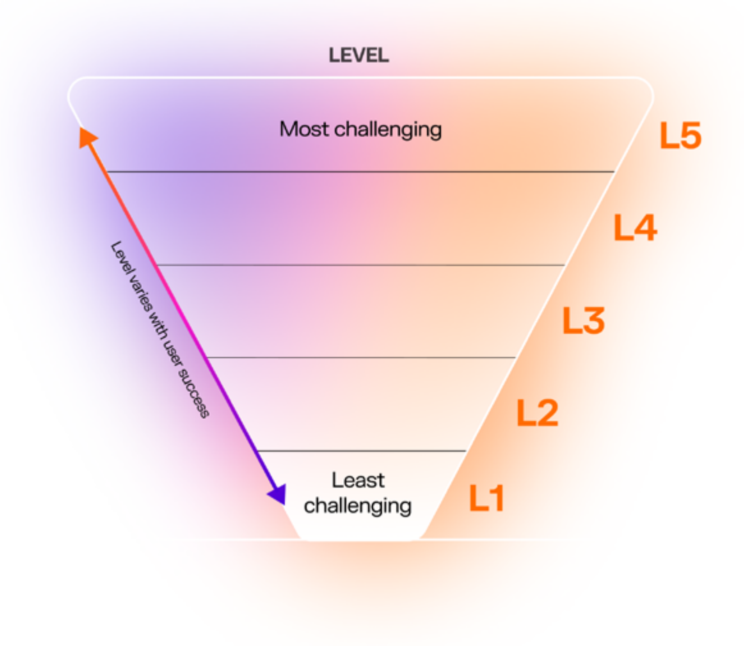
Many thanks,
Henry

While it's helpful for the user to learn from phishing simulations, the added benefit is what Darktrace / EMAIL learns from the employee interaction. **Every click provides feedback** that is used to strengthen the overall security posture.

In that sense, the phishing simulations contribute to refining the overall security culture – defenses can be adapted to cater to user behavior, rather than relying on users to spot phishing based on their training.

5 Level Phishing Simulations

Based on user responses to phishing simulations the system will increase or decrease their level to maintain engagement and skill progression



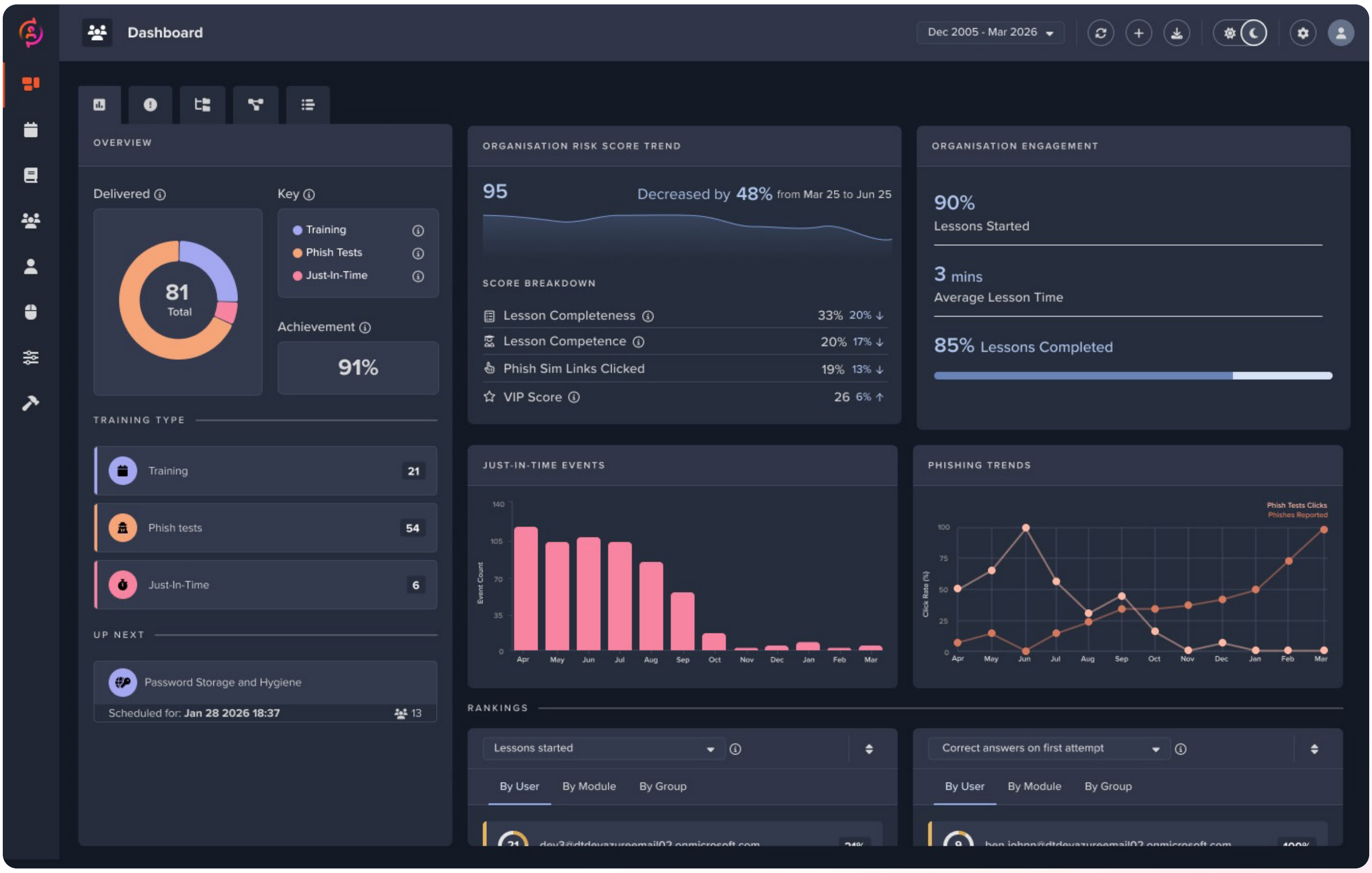
Integrated insights, **measurable outcomes**

Existing SAT solutions may have surface-level integrations with the rest of the security stack, but they fail to communicate proper intelligence or behaviors that determine actual user risk. This makes SAT outcomes impossible to measure.

Darktrace / Adaptive Human Defense integrates seamlessly with the security stack, enabling constant bidirectional feedback to fortify human decision-making and hardening systems in real-time.

This native email security integration breaks the awareness training silo: engagement, links clicked, and user risk scores flow back into your email security recipes and models, so detection and response adapt automatically as people learn. This enables a closed loop workflow to train, observe, and tighten controls at an email security and platform level.

Another critical element of SAT is visibility and measurement. Darktrace's risk scoring converts correctness, engagement, and event data into user, group, and org risk views with VIP context and board-ready metrics – admins can sort by user risk score to easily get visibility of their high-risk users. A user-facing API gives access to simple metrics across the solution, with board-ready PDF generation for quick insights. All allowing you to demonstrate the cultural impact and meaningful risk reduction of training to leadership, not just attendance.



Dashboard

Dec 2005 - Mar 2026

OVERVIEW

Delivered: 81 Total

Key: ● Training ● Phish Tests ● Just-In-Time

Achievement: 91%

TRAINING TYPE

Training	21
Phish tests	54
Just-In-Time	6

UP NEXT

Password Storage and Hygiene

Scheduled for: **Jan 28 2026 18:37** 13

ORGANISATION RISK SCORE TREND

95 Decreased by **48%** from Mar 25 to Jun 25

SCORE BREAKDOWN

Lesson Completeness	33%	20% ↓
Lesson Competence	20%	17% ↓
Phish Sim Links Clicked	19%	13% ↓
VIP Score	26	6% ↑

ORGANISATION ENGAGEMENT

90% Lessons Started

3 mins Average Lesson Time

85% Lessons Completed

JUST-IN-TIME EVENTS

PHISHING TRENDS

RANKINGS

Lessons started — By User | By Module | By Group

Correct answers on first attempt — By User | By Module | By Group

Inbox behavior and training insights are unified into a single view of workforce resilience across the organization, providing an integrated view of user and group exposure that isolate training tools cannot.

Darktrace ActiveAI Security Platform

Darktrace / Adaptive Human defense is fully integrated with Darktrace / EMAIL, delivering a powerful adaptive behavioral email security platform powered by Self-Learning AI.

Darktrace / EMAIL provides context-aware email defense for the entire messaging ecosystem, which unites with Darktrace / Adaptive Human Defense to create the first AI-native system that learns from authentic communication patterns, adapts security responses to each individual and their context, and unifies this behavioral intelligence so that organizations can strengthen people and defenses together.

The entire communication security stack is powered by one Self-Learning AI engine. This single behavioral model drives detection, training, investigation, and domain trust – eliminating blind spots, reducing operational overhead, and compounding **improvement over time.**

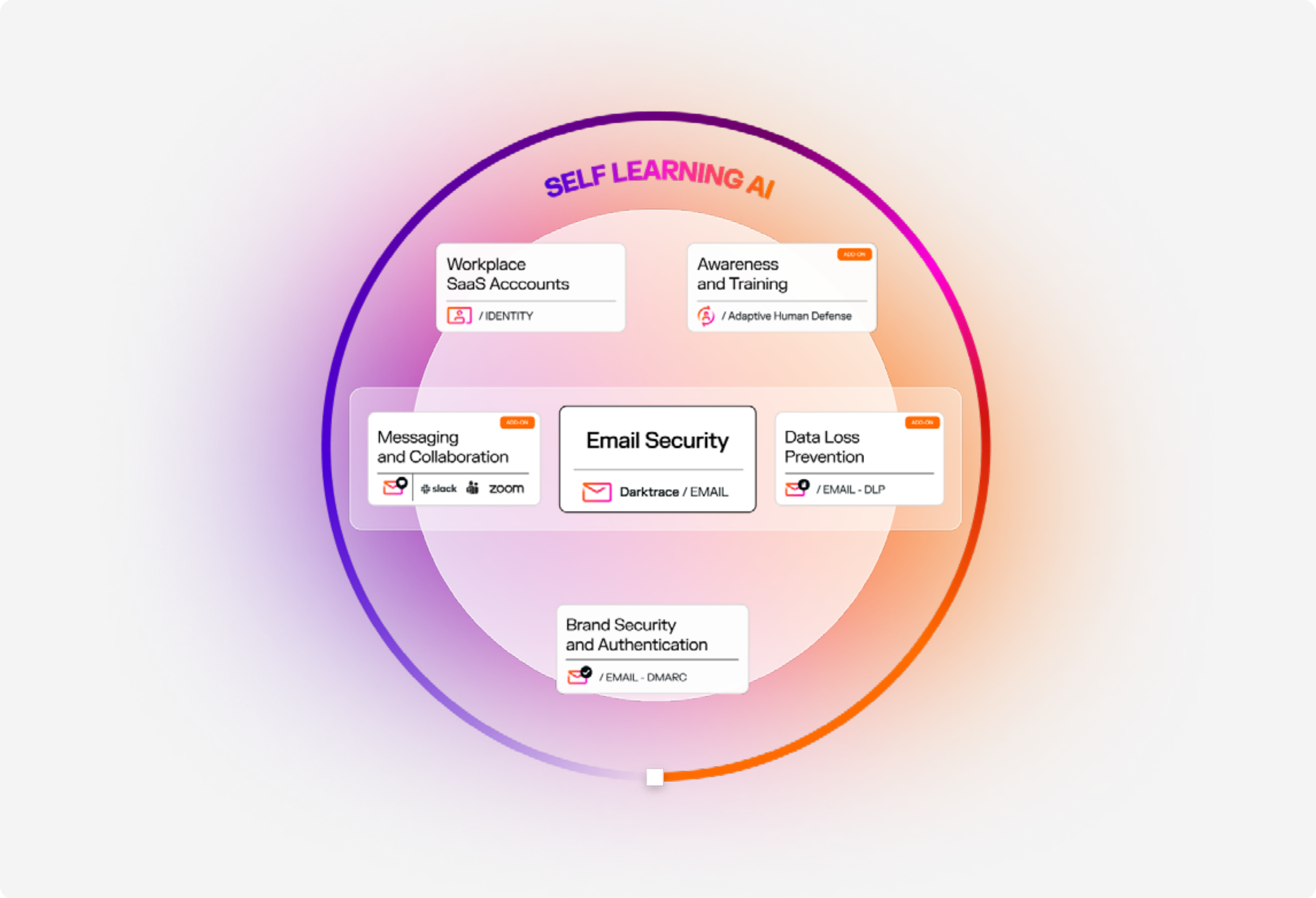
REQUIREMENTS

Darktrace / Adaptive Human Defense is currently aviaiable as an add-on to organizations with the following Darktrace products: **Darktrace / EMAIL.**

✓ **Compatible** with either Microsoft 365 or Google Workspace.

✗ On-premises **not supported.**

Darktrace / Adaptive Human Defense is part of the Darktrace / EMAIL platform, which is integrated into the wider ActiveAI Security Platform – all powered by Self-Learning AI.



■ **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 2,700+ employees who protect nearly 10,000 customers globally. To learn more, visit 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

darktrace.com | info@darktrace.com