DARKTRACE

Darktrace / Adaptive Human Defense

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

INDUSTRY CHALLENGE

Traditional 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.

This puts humans at the frontline of attacks, absorbing more risk than ever before.

68% of breaches involve a human element, not because people are "the problem," but because exploiting people and identity is the easiest way for an attacker to achieve success. Identity is the number one threat, as observed in our Annual Threat Report – 70% of incidents Darktrace observed in the Americas last year originated from SaaS/Microsoft 365 compromise or phishing, making it the single most effective initial access vector.

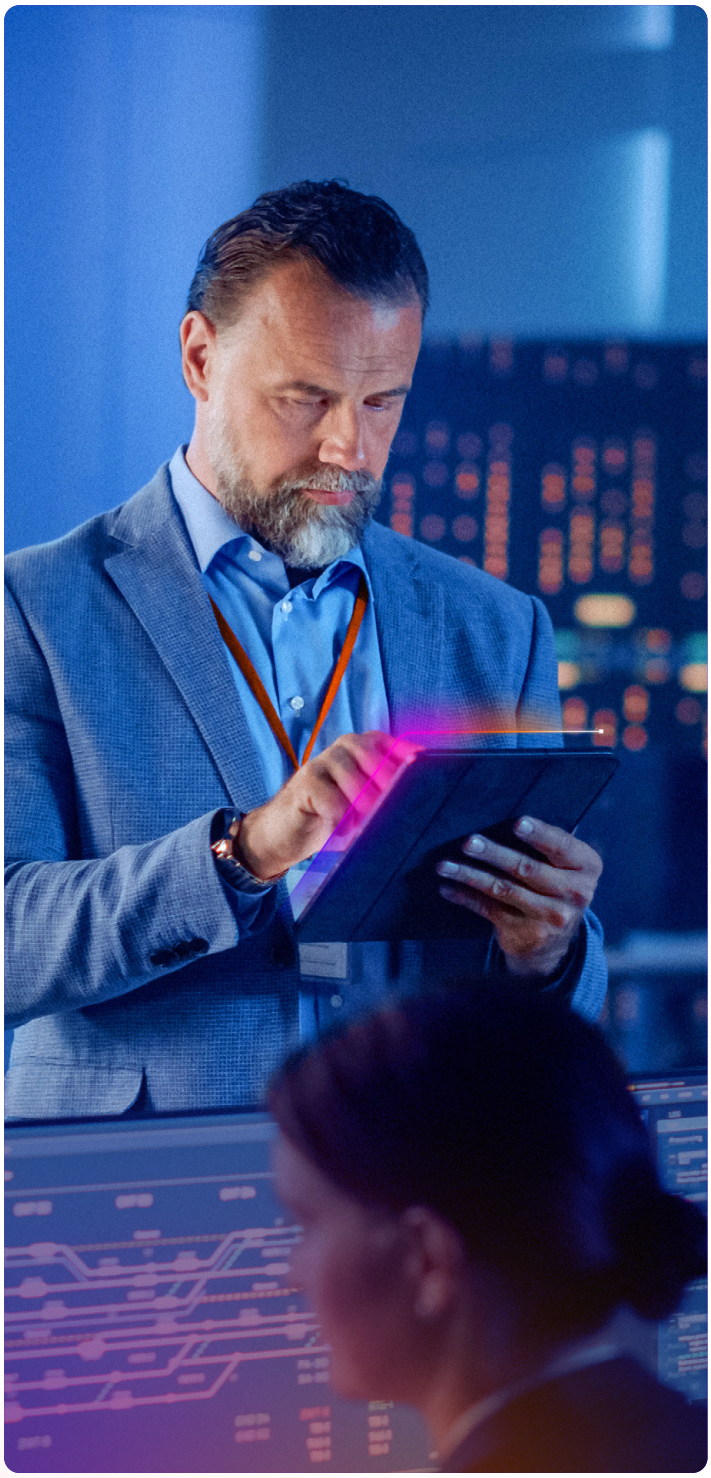
With humans on the front line, you'd assume that effective awareness training which improves decision-making and creates a positive security culture would be a pre-requisite. Unfortunately, security awareness training (SAT) has remained a compliance exercise for organizations, optimized for completion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

84% of organizations still **measure success through completion rates...**

<2% ...even though completion of standard training equates with **<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 security training system that identifies risky activity, delivers personalized and relevant coaching right at the moment of need, and continuously strengthens protection around every individual.

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 to close the gap between security training and email security – with a single, adaptive platform that strengthens both people and defenses.

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:

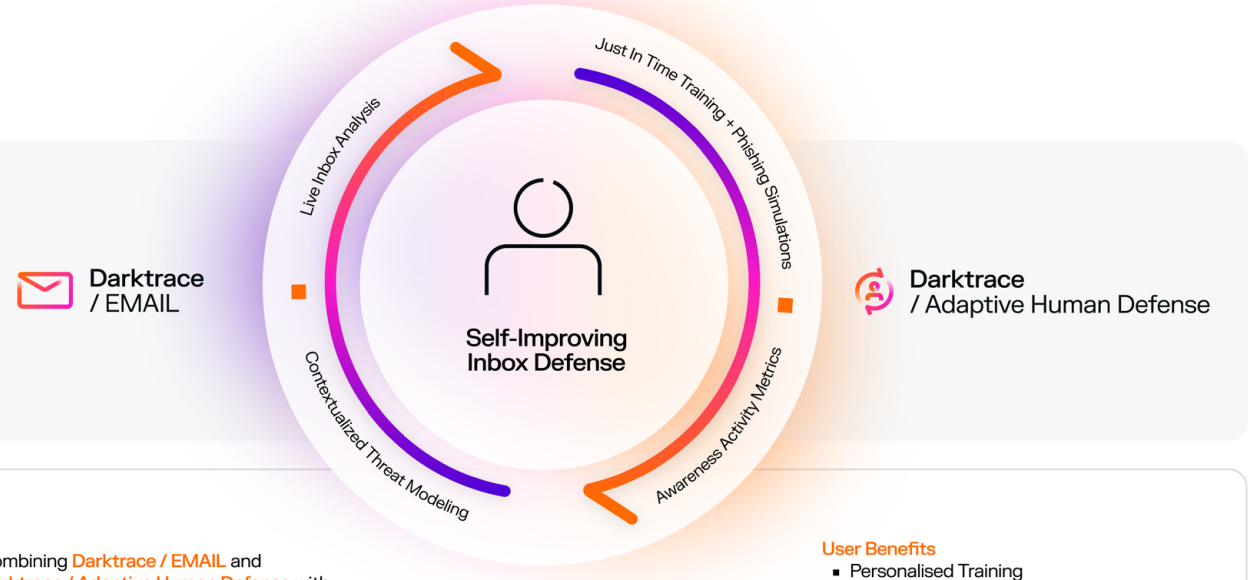
Fewer false alarms, reduced SOC workload:
Users learn to report phishing attempts more accurately, so your security team spends less time chasing false positives.

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.



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

Darktrace / Adaptive Human Defense offers:

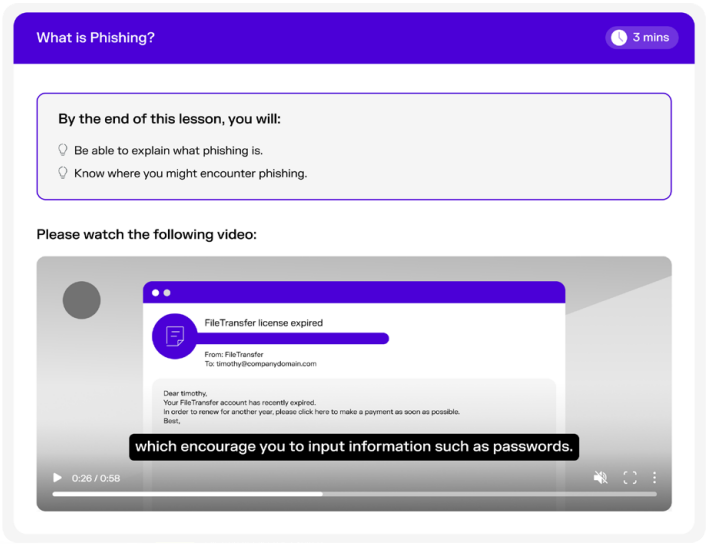
- **Contextual**, in-the-moment learning triggered by real risk
- **Personalized** simulations informed by live threat activity
- **Meaningful** metrics for measuring behavior change

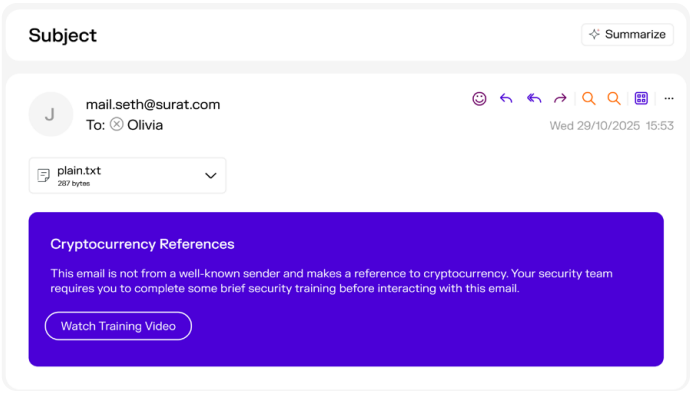
Contextual, in-the-moment learning triggered by **real risk**

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.

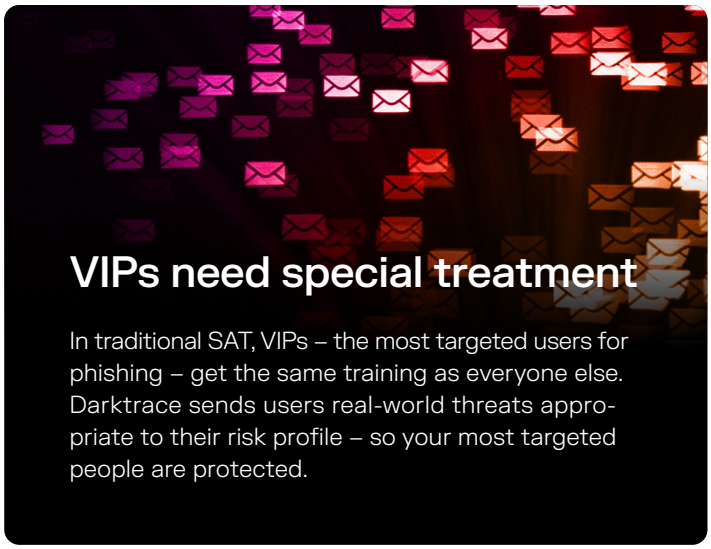




Just-in-time training doesn't need to be scheduled. The integration with Darktrace / EMAIL is leveraged to deliver micro-coaching just at the moment a user is about to take a risky action, managing risk in real time.

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.



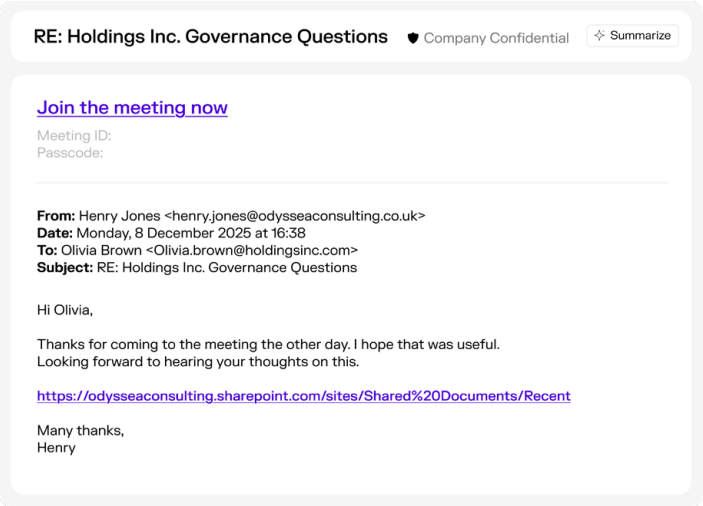
Personalized simulations informed by **live threat activity**

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

Adaptive phishing simulations adjust difficulty based on how each individual responds. Every user starts at a baseline, and the realism of simulations increases or decreases automatically based on their behavior. At the lower levels, phishing is more obvious, helping users build foundational skills.

As users demonstrate proficiency, simulations become progressively more realistic. This allows us to test real resilience — not just awareness — without overwhelming users or relying on one-size-fits-all campaigns.

At the highest level, simulations stop looking like training altogether. Level 5 mirrors the real inbox — impersonating known senders, matching the tone and context of existing conversations, and embedding directly into reply chains. This reflects the techniques used by sophisticated threat actors, including those leveraging AI to blend seamlessly into normal business communication.



When users make mistakes — which does happen — it becomes a learning opportunity. They're automatically guided to a relevant lesson that addresses the specific behavior that caught them out. This allows us to personalize training, reinforce the right habits, and test real resilience under realistic conditions.

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

Meaningful metrics for measuring behavior change

Darktrace Adaptive Human Defense goes beyond measuring training completion to give organizations a true picture of workforce resilience and risk posture.

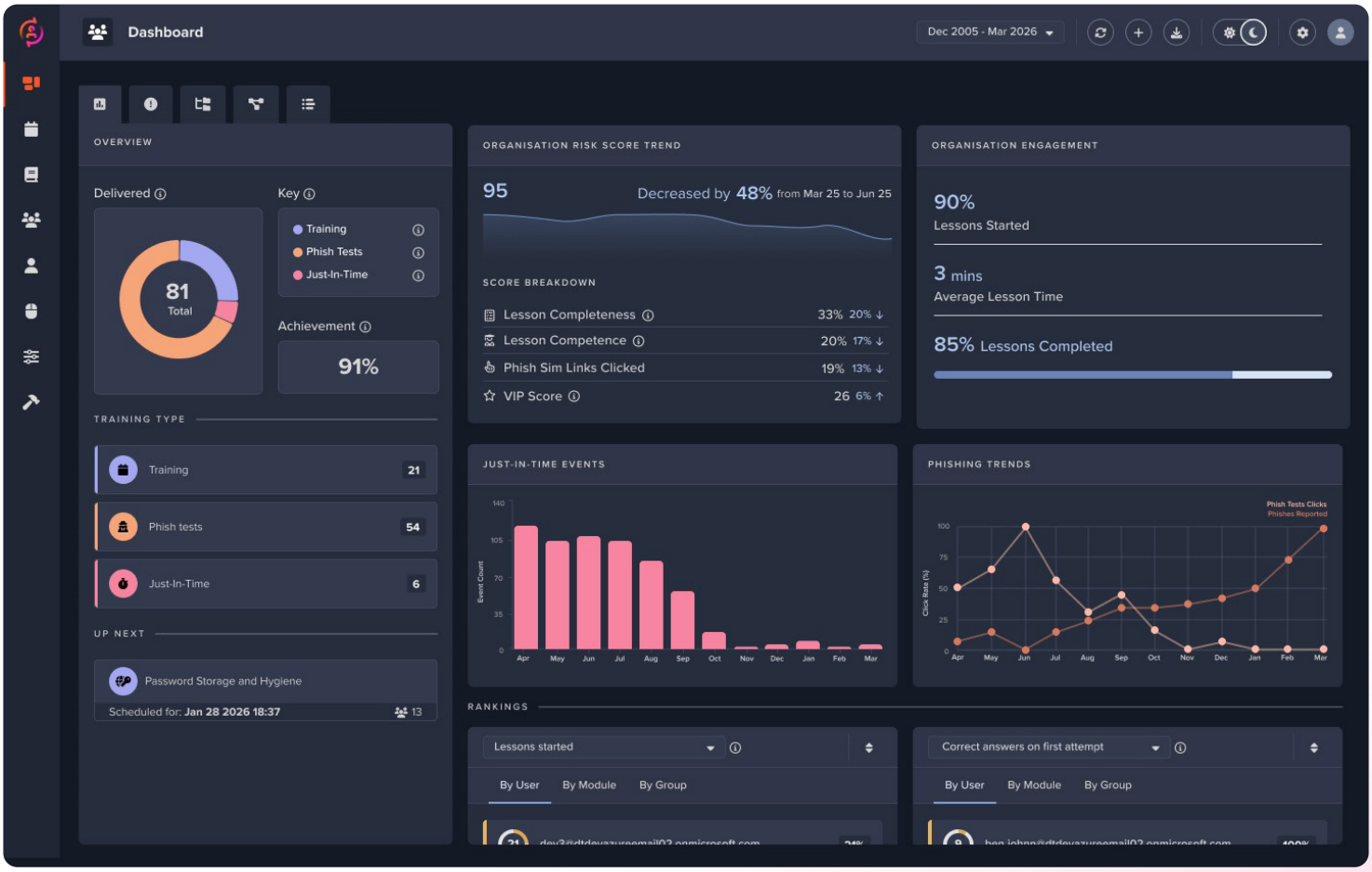
By continuously evaluating live email activity, the platform identifies which users are most exposed to threats, tracking patterns like targeting frequency, internal and external messaging volume, and potential exploitation points across the business.

This live threat exposure is combined with training performance, drawn from realistic simulations and context-aware coaching. Unlike generic phishing tests, the adaptive exercises measure how users actually respond to real-world phishing activity.

The result is a comprehensive user risk score that reflects:

- **Training completion** – did the user engage with the learning content?
- **Training performance** – how effectively does the user respond to simulated threats?
- **Email exposure** – how frequently and intensely is the user targeted in live email environments?

These scores feed directly into Darktrace / EMAIL, allowing detection and response workflows to adapt automatically as users improve. Administrators gain clear, actionable insights at the user, group, and organization level, with VIP context and board-ready reporting to demonstrate meaningful reductions in risk, not just course completions.



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