DARKTRACE

Darktrace / EMAIL

Secure your entire messaging ecosystem with AI-driven email security that catches the threats other solutions miss

The communication attack surface is constantly expanding

The reality is that Generative AI has changed the game for communication-based attacks.

It has lowered the barrier to entry, allowing attackers to generate highly personalized, targeted threats at scale. Adversaries are leveraging it to craft convincing, multi-channel attacks – spanning chat, SMS, video, and collaboration tools. These advanced social engineering attacks often exploit trusted relationships or mimic legitimate business processes, making them harder to catch with traditional email security tools.

And threats are no longer confined to inbound email alone. In 2024, 40% of phishing activity extended into other platforms such as Microsoft Teams and social media[1], as attackers follow employees across the tools they use every day. It shows that attackers still see human psychology as an entry point that can be exploited – 60% of all incidents included a human element at the source of the breach.[2]

Security teams are facing an ever-increasing challenge as attackers employ these multi-vector, AI-driven techniques that penetrate every facet of organizational communication.

Of all the phishing attempts detected by Darktrace in 2024:

38%

were spear phishing attempts targeting high-value individuals.[3]

32%

used novel social engineering techniques, including AI-generated text with advanced linguistic complexity.[3]

1: Phishing Statistics 2025 (Deepstrike)
2: 2025 Verizon Data Breach Investigations Report
3: Darktrace Threat Report 2024

The limits of attack-centric security

Native email providers like Microsoft and Google have significantly strengthened their built-in security capabilities in recent years.

For most organizations, these native tools form a solid foundation that's deeply embedded in their workflows, but they don't address the full spectrum of threats. According to Forrester, most organizations adopt a layered approach of at least two solutions – the question, then, isn't whether to replace them, but how to best leverage that investment and complement it with deeper, more adaptive defenses.

Traditional Secure Email Gateways (SEGs) were designed with a similar, attack-centric philosophy — relying on signatures, threat intelligence, and rules derived from known threats. This often results in duplicated workflows and overlapping costs when combined with native tools. Even newer SEG alternatives that use APIs or pattern-based AI largely operate within the same reactive framework, detecting attacks only after they've surfaced.

In addition, many email-focused vendors lack visibility beyond the inbox. Their integrations with other systems are often superficial, rather than offering genuine intelligence sharing.

What's needed is a synergized platform that extends beyond email, using un-siloed AI to correlate behavior across the entire digital ecosystem — which can autonomously understand relationships between threats, coordinate responses across domains, and do so without relying on manual rule-creation in a SIEM.

Darktrace / EMAIL

The industry's most advanced cloud email security powered by Self-Learning AI

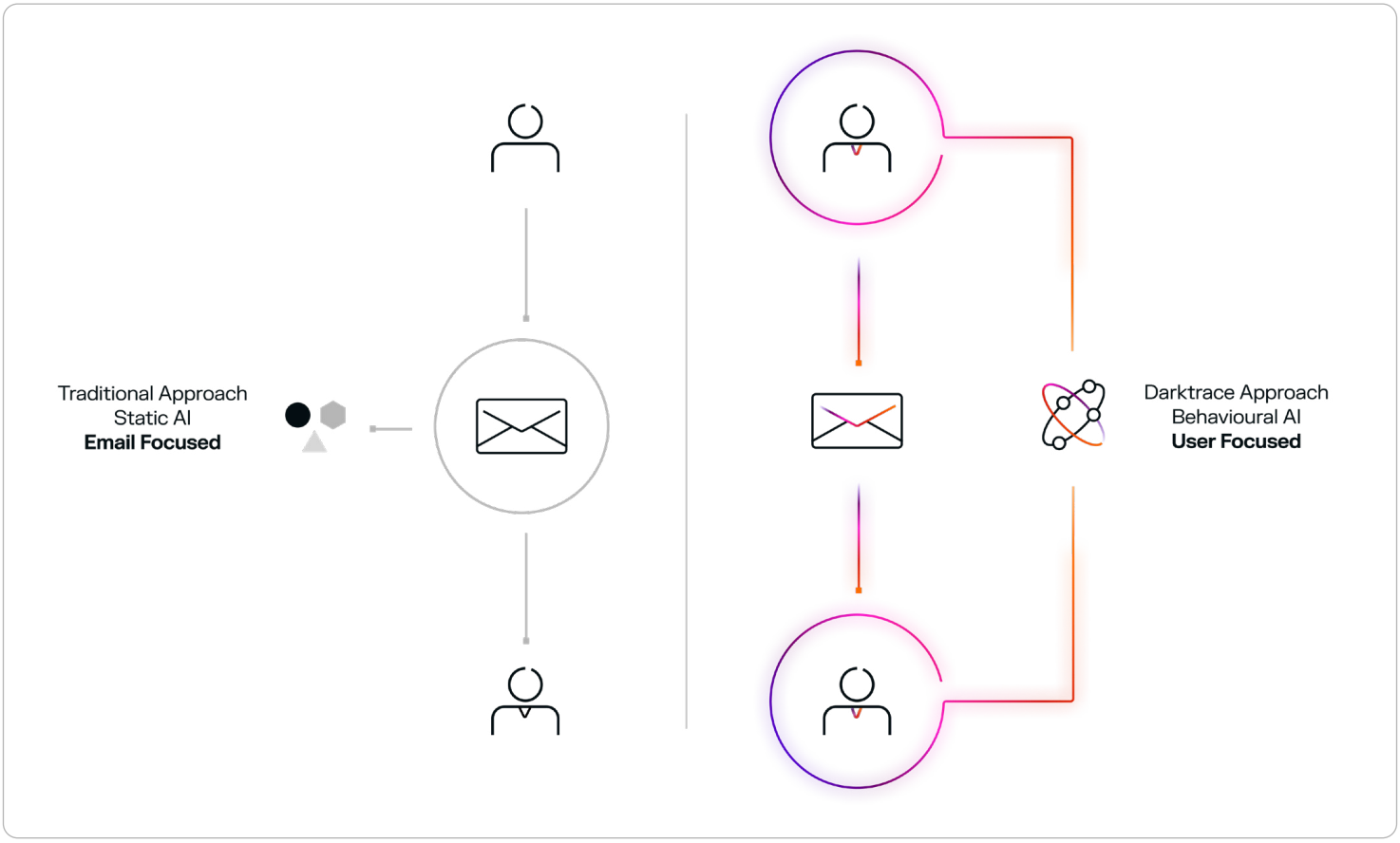
Darktrace / EMAIL enhances your native email security by leveraging business-centric behavioral anomaly detection across inbound, outbound, and lateral messages in both email and Microsoft Teams.

It's the first email security built on Self-Learning AI, which understands 'normal' for every organization and user account to quickly identify sophisticated threats like BEC, ransomware, phishing, and supply chain attacks – without duplicating existing capabilities or relying on traditional rules, signatures, and payload analysis.

Designed from the ground up to build on the benefits of your native email provider, it not only stops more threats than SEGs, but revolutionizes email security management to drastically decrease the load on security teams.

- **75% drop in suspicious emails**
  in the first month observed by one customer, saving 45 hours investigation time in the SOC.

(Global Technology Provider)



Darktrace takes a user-focused and business-centric approach to email security, in contrast to the attack-centric rules and signatures approach of secure email gateways

Business benefits

Complements your native email security
with behavioral anomaly detection, to stop the zero-day, advanced, and novel threats that evade other security layers

Avoid duplicate costs across your stack
by building on the capabilities of your native provider instead of deactivating or duplicating them

Gain maximum ROI
from advanced protection that enhances and builds on your native security workflows

Protect users' entire communication attack surface
for inbound, outbound and lateral mail plus Microsoft Teams and SaaS applications

Reduce phishing reports
by giving employees real-time feedback as they report, for fewer benign flagged emails

Decrease the load on security teams
with in-depth auto-triage for reported emails, to improve report-time analysis

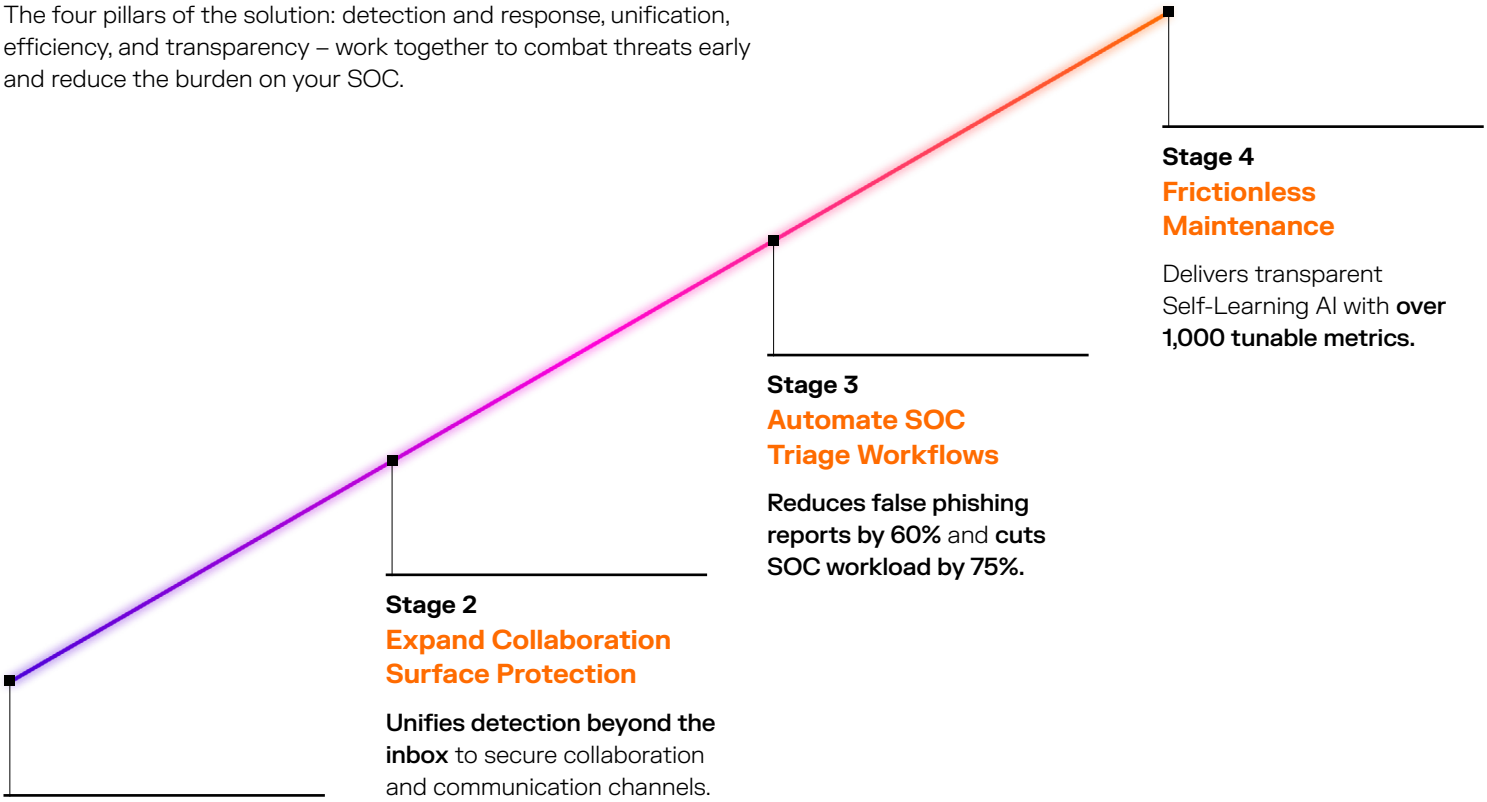
Easy investigation of multi-domain attacks
with greater visibility between email and the digital estate

Unify insights from email across your security surfaces
to improve the detection accuracy of each solution

Share insights across your security surfaces
to improve the detection accuracy of each solution

Darktrace / EMAIL is designed to help you build a resilient communication security operation.

The four pillars of the solution: detection and response, unification, efficiency, and transparency – work together to combat threats early and reduce the burden on your SOC.



Stage 1
Deploy Behavioral Threat Detection

Detect **55% more** threats across inbound, lateral, and outbound **13 days earlier** than native email providers.

Stage 2
Expand Collaboration Surface Protection

Unifies detection beyond the inbox to secure collaboration and communication channels.

Stage 3
Automate SOC Triage Workflows

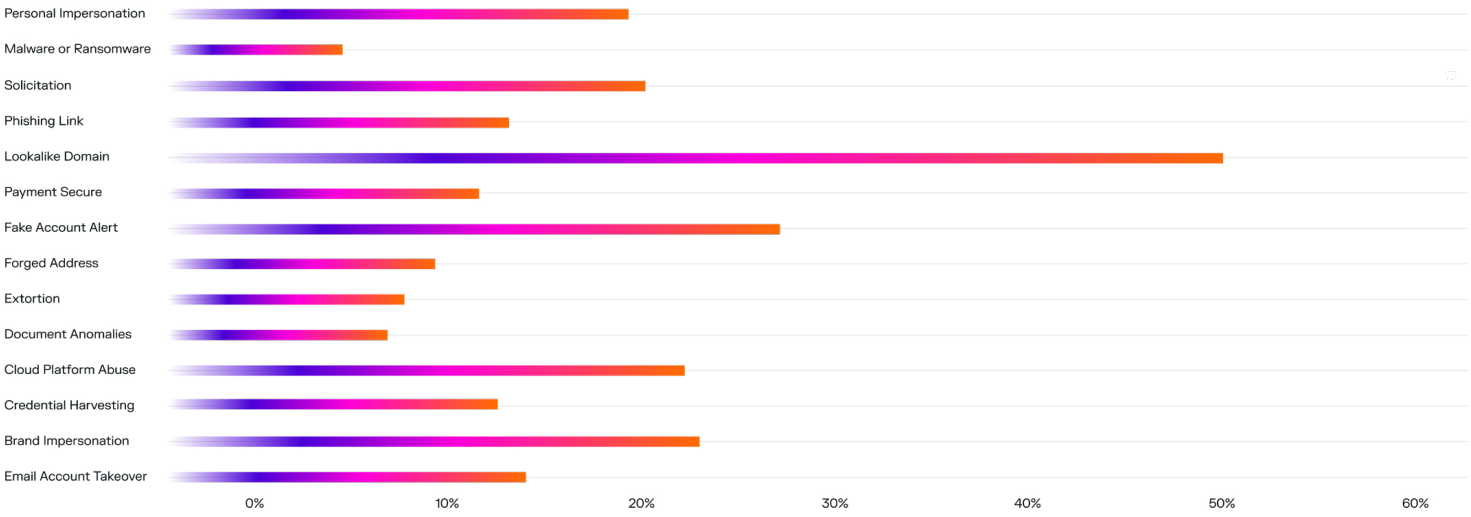
Reduces false phishing reports by 60% and **cuts SOC workload by 75%.**

Stage 4
Frictionless Maintenance

Delivers transparent Self-Learning AI with **over 1,000 tunable metrics.**

Behavioral threat detection and response

Detect 17% more threats than leading SEGs,
55% more than native providers



Darktrace catches more threats than SEGs across a range of attack vectors

Adaptive threat detection and response using business-centric techniques to catch novel and AI-generated threats.

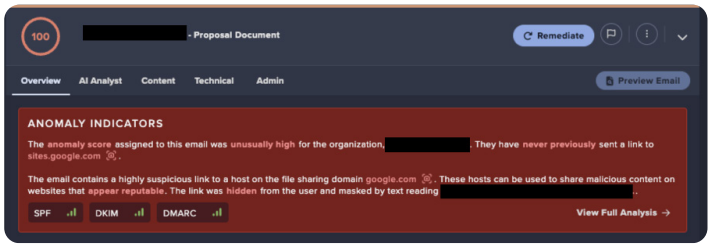
Darktrace AI learns what belongs for each user, rather than relying on payload analysis or threat intelligence. That's why it's better than attack-centric solutions at catching advanced threats like brand impersonation, lookalike domains, solicitation, phishing links, and zero-days.

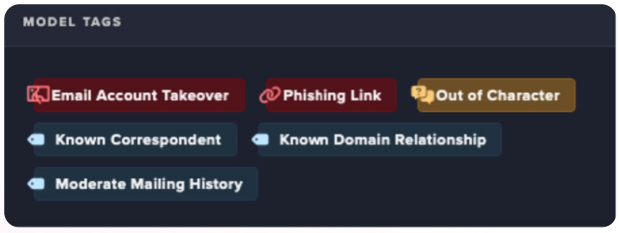
When a communication arrives, Darktrace analyzes thousands of data points: language, tone, sentiment, links, sender profile, and more. All this is compared to the normal communication history of sender and recipient.

The AI asks: "Does this message belong here?" This analysis happens in milliseconds. If the message is normal it flows through uninterrupted. If it's suspicious, Darktrace can take a range of autonomous actions, from tagging it to full quarantine.

Email threats demand more precision in response than other types of threats. Individual learning allows for individual responses tailored to each user, whether they are a VIP or have other responsibilities.

Precise response actions, including rewriting links, removing attachments, unspoofing the sender, or moving to junk, ensure that email security doesn't conflict with business continuity (see a complete list of actions in Appendix A).





Protection beyond the inbox

Secure your entire communication surface, to protect users wherever they share data

True defense-in-depth requires treating every interaction with the same scrutiny as inbound mail. Darktrace / EMAIL extends protection beyond the inbox to cover messaging and collaboration platforms, monitoring activity across email, chat, and productivity tools to catch account compromise, data loss, and lateral movement.

Unlike tools that focus only on payloads, Darktrace analyzes the intent, content, and context of communications across Teams, SharePoint, and M365. Every interaction, whether it's an email, a Teams message, or collaborating on a SharePoint file, is analyzed in context, feeding into Darktrace's Self-Learning AI to improve detection accuracy across domains. By correlating signals from email, identity, network, and cloud, Darktrace builds a complete picture of user behavior and the full attack chain.

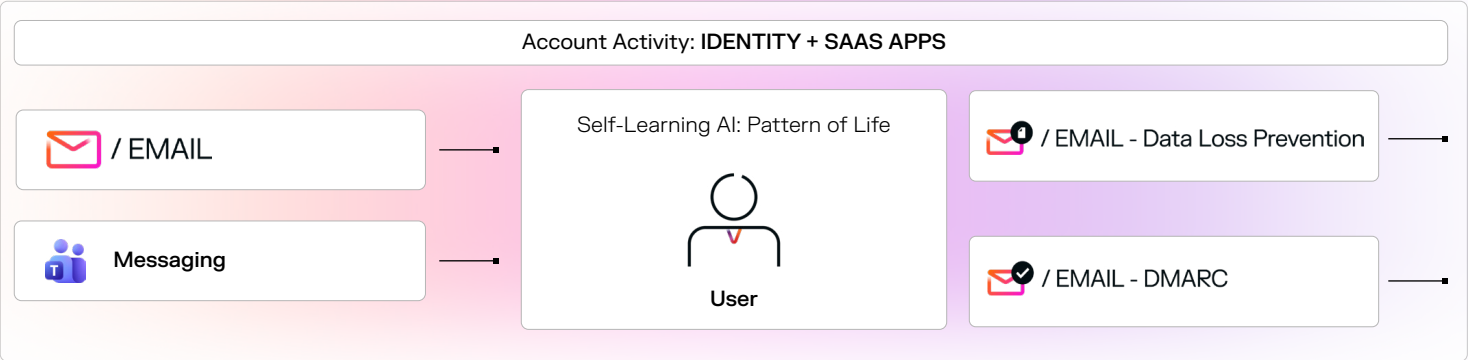
And protection doesn't stop there: securing outbound communications is just as critical. With advanced DLP and DMARC capabilities, Darktrace makes preventing data leaks and safeguarding brand reputation effortless and integrated.

55% of malicious emails blocked by Darktrace had **already evaded the native email provider**

17% Darktrace / EMAIL catches on average the **17% of threats that leading SEGs miss**

75% of Darktrace / EMAIL customers **don't use any email gateway**

50% of those customers, **50% initially deploy a SEG**, but **remove it by the end of their contract**



Darktrace / EMAIL protects the entire communication surface, from inbound mail to outbound and lateral mail, plus Teams messaging

Internal Darktrace research

Label-free behavioral DLP powered by a proprietary DSLM

Traditional DLP tools depend on static rules and manual labeling, creating overhead while failing to keep pace with modern threats.

Darktrace takes a different approach: autonomous, behavior-driven DLP that adapts to context and user behavior.

Darktrace / EMAIL-DLP combines behavioral content analysis with a domain-specific language model to prevent the loss of sensitive data on-send – including secrets, intellectual property, and personal identifiable information (PII). With enhanced PII detection, Darktrace automatically identifies over 35+ entity types spanning personal, financial, and health data, eliminating the need for manual classification.

Affordable DMARC with easy setup and management

Darktrace / EMAIL – DMARC brings enterprise-grade email authentication to organizations of all sizes, without the complexity or cost of traditional solutions.

It simplifies SPF/DKIM/DMARC deployment with responsive guidance, intelligent alerts, and continuous monitoring, helping teams stop spoofing, improve deliverability, and maintain compliance with evolving standards.

Unlike outsourced services, it keeps you in control, offering full visibility into your email infrastructure and third-party senders. It also supports BIMI logo verification, reinforcing sender authenticity to build trust in every communication.

46%

- **46% of breaches involved customer personal data**
  — the most commonly compromised asset.

IBM Cost of a Data Breach Report 2024

For a full view of the capabilities included in different Darktrace / EMAIL licenses, see Appendix B.

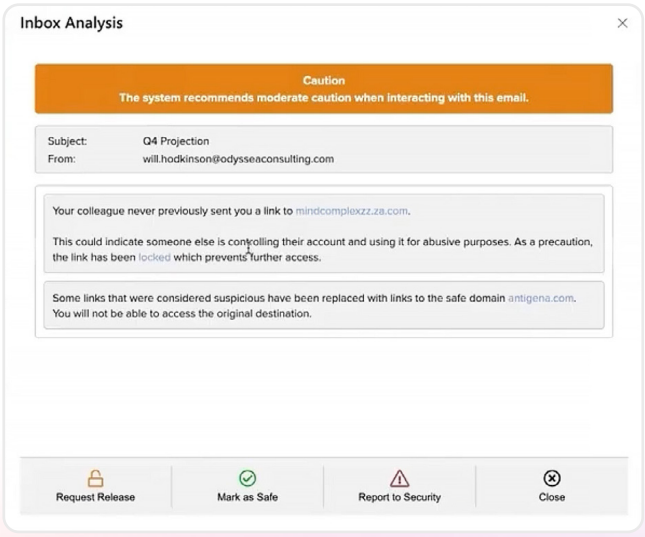
Seamless end-user and SOC workflows

Benefits your end-users

Darktrace / EMAIL transforms end-user reporting from a burden into a strength. Instead of dismissing user reports as low quality, Darktrace improves security awareness with contextual banners and Cyber AI Analyst narratives that explain why an email is suspicious. This empowers users to make informed decisions and reduces benign user reports by 60%.[4]

When a user clicks Analyze, they receive a clear narrative of the AI's decision. If they escalate the email, Cyber AI Analyst runs a deeper investigation (sandboxing links, correlating recent emails, and identifying campaigns) before handing only high-quality signals to the SOC.

[4]Internal Darktrace research



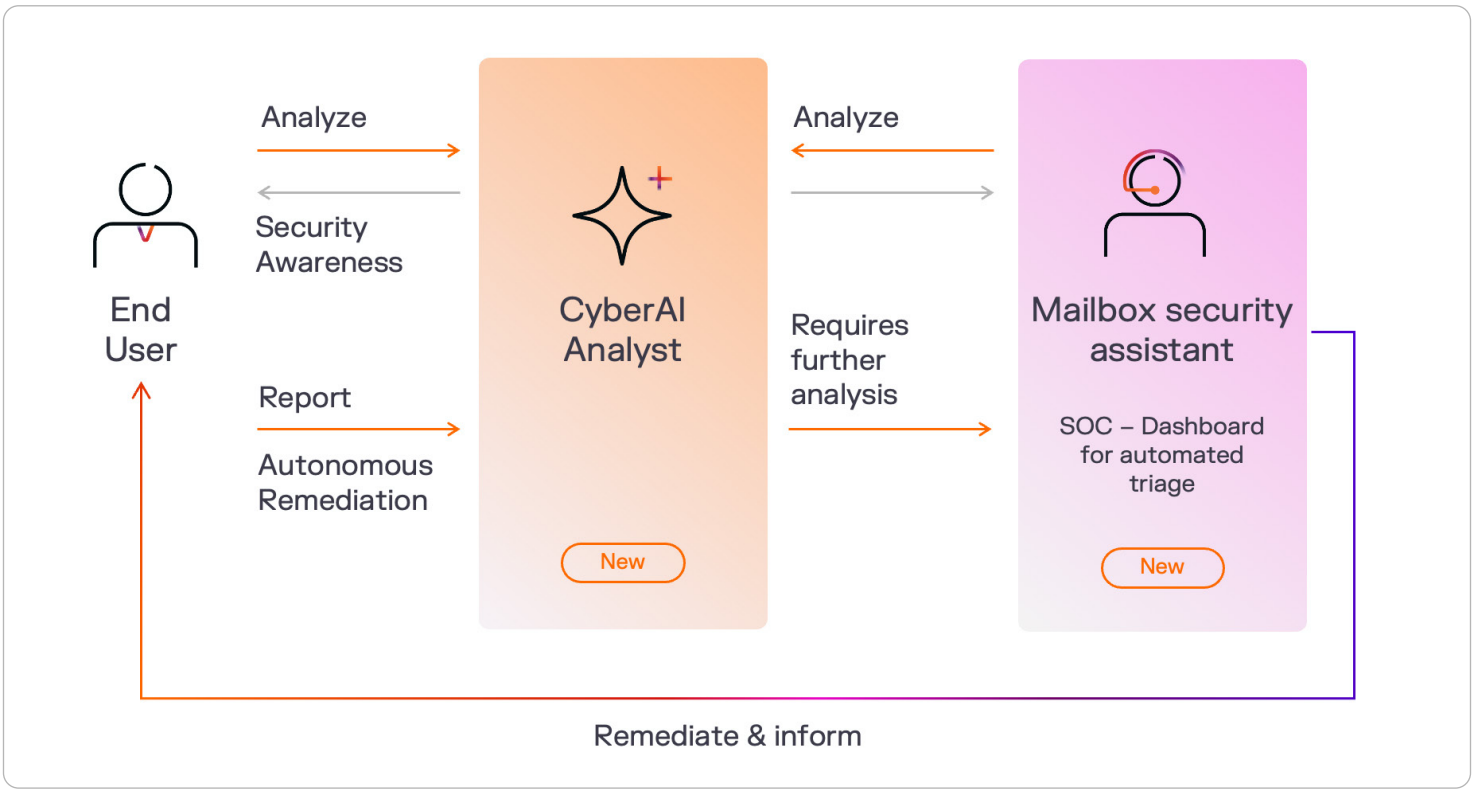
Elevates your SOC

Darktrace streamlines triage and investigations, ensuring that the SOC only deal with high-confidence threats supported by easy workflows. Cyber AI Analyst accelerates triage with rich context, link analysis, and campaign insights, while analysts remediate directly from the SOC dashboard – no ticketing delays, no wasted cycles.

Exclusive Microsoft integrations further elevate these workflows. Darktrace is the only solution with Microsoft-native quarantine and Copilot integration, streamlining investigations and surfacing threat insights in familiar tools. Automated JIRA ticketing speeds up response to user-reported messages, and sandbox integration provides deeper payload analysis for confident, efficient investigations.

486 **analyst hours saved** for one customer and their security team using Darktrace / EMAIL, Cyber AI Analyst on investigations within a 20-day period.

Global Telecom Provider



Darktrace uplifts the end user to drastically decrease the load on security teams, while centralizing and speeding analysis for initiated investigations

Fast, simple deployment

Deploy with ease, via API or API plus journaling – with no disruption to mailflow. With our unique deployment options, you can:

- **Eliminate maintenance**
  SEGs are a static collection of rules and detections that require time-intensive manual tuning to keep up with attackers. Darktrace AI adapts based on user behavior to stop threats without the need to update block lists.
- **Streamline deployment**
  Because Darktrace / EMAIL is built to co-exist with, rather than replace, native email security providers, it doesn't require rerouting MX records or turning off native security capabilities but builds seamlessly on your E3 or E5 security foundation.
- **Centralize costs and improve ROI**
  Eliminate the duplicate costs of operating a SEG alongside your native email provider and improve your return on investment with better protection supported by optimized workflows.

30x faster than API-only based security solutions

Darktrace / EMAIL Deployment Options

Delivery Model	M365 Deployments: A Microsoft 365 (formerly Office 365) Business Essentials license or above is required Hybrid Exchange Deployments: Exchange Server 2016 and above. On Premise Deployments: Exchange Server 2013 SP1, or Exchange Server 2016 / 2019 with NTLM(v2) configured. Google Deployment: Google Workspace Enterprise or Enterprise for Education License (or above).
Deployment Options	API-only or API+Journaling
Retention	Up to 90 days of log, 21 days on actioned mail, 7 days on non-actioned mail and 30 days on flagged mail

DARKTRACE | Microsoft

Better Together

The Darktrace–Microsoft partnership delivers complete, complementary protection for our customers. Built on Microsoft Azure and integrated with Microsoft 365 and Exchange, Darktrace / EMAIL enhances Microsoft's global attack intelligence with enterprise-specific behavioral AI.

This layered approach unites attack-centric and business-centric defense, improving detection, response, and remediation across the full email and collaboration ecosystem – without duplicating workflows or investments.

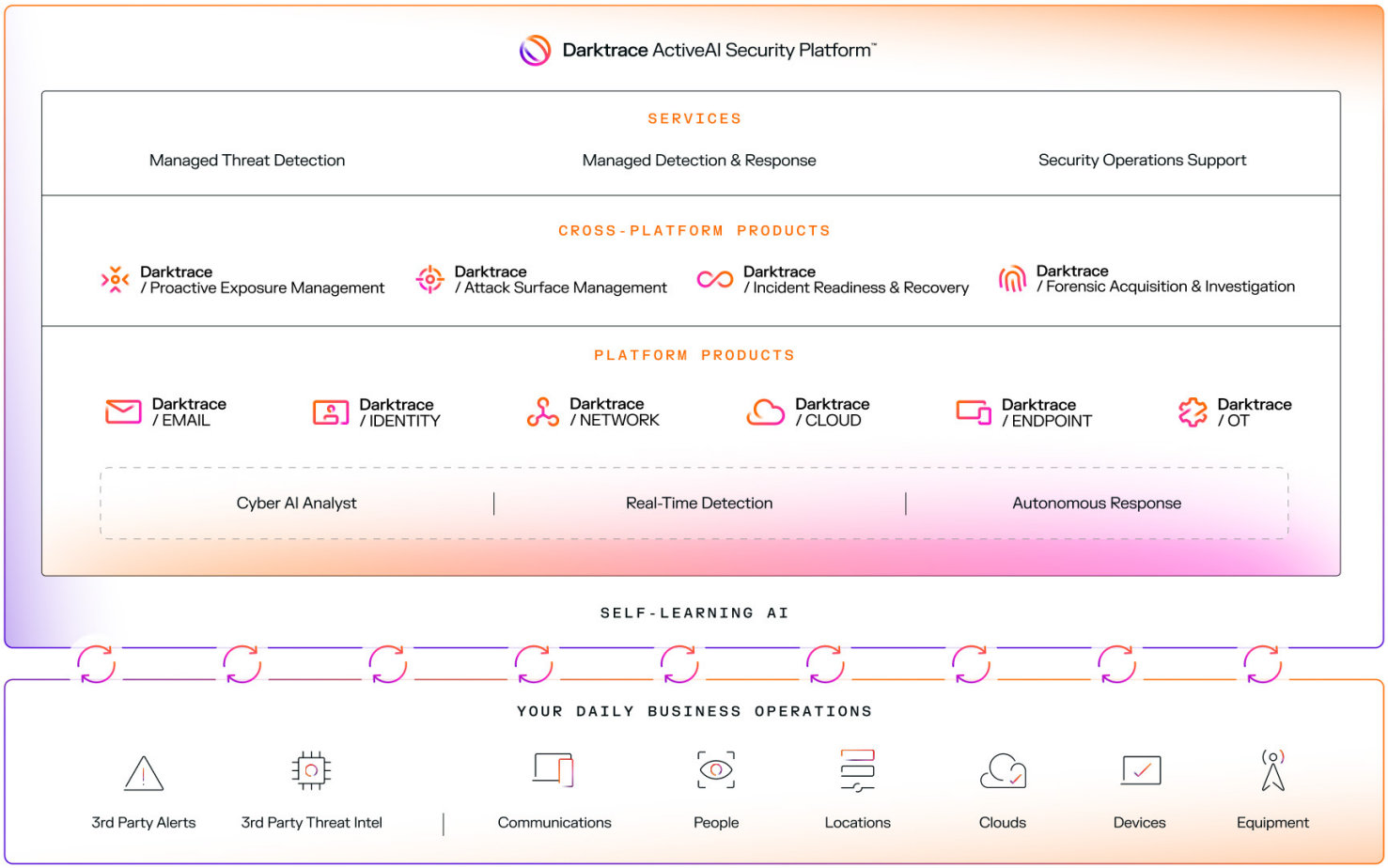
Darktrace ActiveAI Security Platform™

Darktrace / EMAIL is part of the Darktrace ActiveAI Security Platform, combining email security with the rest of the digital estate to enhance security visibility and control across your networks, clouds, endpoints, identities, and OT.

Powered, by Self-Learning AI, the platform correlates telemetry across domains to provide a unified view of risk and end-to-end coverage. Behavioral signals in one area, such as a suspicious email, immediately inform decisions in network and cloud, and vice versa.

This tight integration between areas of the digital estate enables faster threat detection, enriched and contextualized alerts, and smarter autonomous actions, without requiring human intervention or complex rule-based integrations.

The Darktrace ActiveAI Security platform provides **seamless, adaptive protection** that mirrors how real-world attacks unfold, giving defenders a consistent, unified advantage.



Appendix

■ Appendix A

Darktrace / EMAIL Actions

Targeted actions to reduce risk while maintaining the flow of business then the actions table.

Darktrace / EMAIL Actions

Delivery Actions: Hold Message or Move to Junk	Darktrace / EMAIL can hold or junk the message before delivery due to suspicious content or attachments. Held emails can be reprocessed and released by an operator after investigation.
Rewrite Links	URLs are rewritten to require user confirmation before proceeding, subjecting the destination to second-level checks. Suspicious links prompt a message indicating they are locked, preventing access while recording user intent. Once rewritten, suspicious links are analyzed to determine whether a user should be let through or blocked.
Attachment Actions: Convert or Strip Attachment	One or more attachments of these emails has been converted to a safe format, flattening the file typically by converting into a PDF through initial image conversion. This delivers the content of the attachment to the intended recipient, but with vastly reduced risk. Alternatively, either due to format or risk posed the attachment can be stripped entirely.
Unspoof	Reduces psychological impact of spoofing by removing the 'Spoofed' name from the visible address of the sender and replaces it with the genuine 'envelope sender' which is, under normal circumstances, hidden from the recipient.

Appendix B

Darktrace / EMAIL: Core capabilities & add-ons

Capabilities	Darktrace / EMAIL		Darktrace / IDENTITY	Darktrace / EMAIL - DMARC
	Darktrace / EMAIL - DLP	Darktrace / EMAIL - Teams		
Inbound Email Detection & Response	+	+	+	
Lateral Email Detection & Response	+	+	+	
Outbound Email Detection (Data loss, Misdirected Recipients, Insider Threats)	+	+	+	
Outbound Email Response (via “in-line action mailflow”)		+	+	
Account Compromise Detection	+	+	+	
Account Compromise Response				+
Expanded Account Activity Use Cases (Resource Management, Compliance..)				+
Non-Productive Mail	+	+	+	
Teams Threat Detection (does not include response)			+	
Cyber AI Analyst Narrative for Outlook Analysis Add-in and Mailbox Security Assistant	+	+	+	
Forensic Search	+	+	+	
AI Model Tuning and Learning Exceptions	+	+	+	
Analysis of inbound DMARC/SPF/ DKIM records for the purpose of threat analysis	+	+	+	
DMARC Authentication Enforcement and Monitoring of Customer’s Domain				+

About Darktrace

Darktrace (DARK.L), a global leader in cybersecurity artificial intelligence, is on a mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to help transform security operations and improve cyber resilience. Breakthrough innovations from its R&D Centers have resulted in more than 200 patent applications filed. Darktrace employs 2,400 people around the world and protects over 9,700 organizations globally from known, unknown and novel cyber-threats.

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