DARKTRACE

DARKTRACE/EMAIL

Look Beyond Traditional Secure Email Gateways to a Market Leader in Cloud Email Security

Stop the 58% of Threats Other Solutions Miss[1]

The Email Threat Landscape is Constantly Evolving

While phishing is the initial access vector for almost a third of breaches recorded in 2023[2], adversaries are innovating to increase their success. Phishing specifically is leading the charge in offensive AI, as Large Language Models (LLMs) like ChatGPT have enabled the proliferation of sophisticated, targeted, phishing attacks at scale, with spear phishing now occupying 45% of all attempts[3].

Beyond phishing, other mail threats are advancing quickly, with cyber-criminals using multi-stage social engineering techniques that build trust prior to delivering or even altering traditional payloads like links and attachments – in particular, chat tool use has continued to increase[4] and the delivery of QR code payloads has increased by 59%[5]. The amount of cyber-attacks using stolen or compromised credentials increased by 71% in 2024[6], suggesting a rise in account-based threats including BEC and supply chain attacks. Security teams are facing an ever-increasing challenge as attackers employ multi-vector techniques that penetrate every facet of organizational communication.

Existing Solutions are Stuck Looking to the Past

Secure email gateways (SEGs) are adept at stopping low impact and generic attacks, but consistently lack the visibility to deal with advanced threats like Business Email Compromise (BEC). Recently, native email security providers like Microsoft and Google have made significant investments, leaving teams operating gateways with duplicate workflows and added expenses for similar capabilities. Newer API-based vendors that promise AI-driven detection still rely on data from recent attacks, making them unable to spot advanced or zero day threats.

In addition, they lack visibility across the digital estate, failing to correlate attacks between email and network, cloud, or endpoint, let alone allowing security teams to get ahead. Securing organizations in today's threat landscape and business environment necessitates a proactive approach that enhances the capabilities provided by native security vendors and provides granular analysis across the entire messaging attack surface, including inbound, outbound and lateral mail, and Microsoft Teams.

Business Benefits

Gain best-in-class email security
using behavioral anomaly detection to autonomously detect the 38% of advanced threats that evade all other email security solutions[7]

Avoid duplicate costs across your stack
by building on the capabilities of your native email security provider instead of replacing them

Gain maximum ROI from your email security
by implementing native and advanced email security that share workflows rather than duplicate costs and resources

Protect users' enterprise communications
to catch all threats – for inbound, outbound* and lateral mail plus Microsoft Teams and SaaS applications

Reduce successful phishing attempts against employees
by giving users real-time feedback when they report a phishing attempt, reducing benign user-reported emails by 60%[8].

Decrease the load on security teams
by automating mailbox remediation that stops 70% more malicious links[9] and leveraging the explainability of Cyber AI Analyst to reduce triage time by 90%[10].

Unify insights from email across your security surfaces
by correlating insights from across the entire Darktrace platform into a single triage and reporting engine

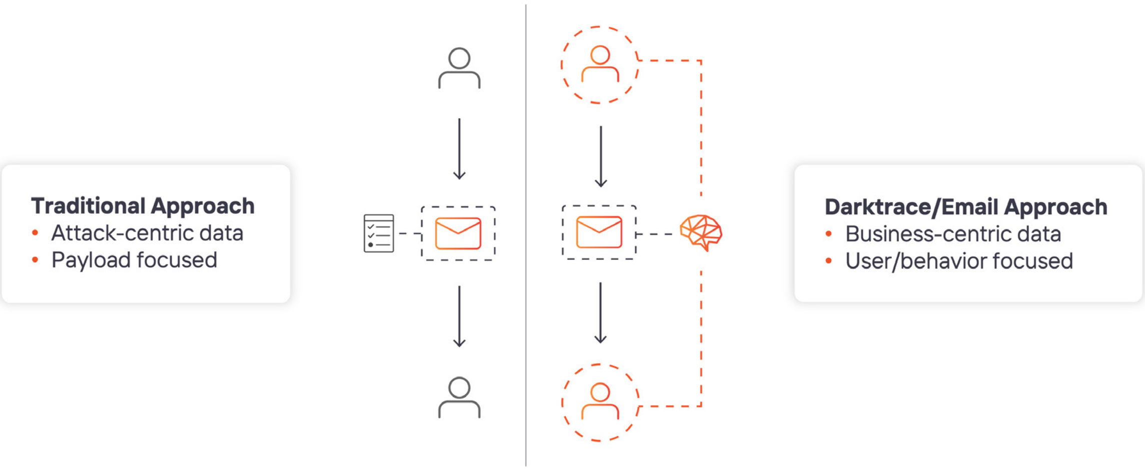
[1] Darktrace Threat Report 2023
[2] IBM Security X-Force Annual Threat Report 2023
[3] Darktrace Threat Report 2023
[4] Daily active users of Microsoft Teams increased by 270 million users in 2022 to 300 million in 2023, according to company data.
[5] Darktrace Threat Report 2023
[6] IBM X-Force Threat Intelligence Index 2024
[7] Darktrace Threat Report 2023
[8] Darktrace Internal Research
[9] Darktrace Internal Research
[10] Darktrace Press Release, 2019
* Outbound mail filtering capabilities are currently only available for Microsoft 365. Coverage for Google Suite is coming soon.

Darktrace/Email, The Industry's Largest and Most Advanced Cloud Email Security

Look beyond secure email gateways and point solutions to stop the 38% of threats that evade all other email security solutions. Darktrace/Email is the first email security built on Self-Learning AI – that analyzes content and context across your entire mail flow to protect your domain and brand while preventing phishing, novel social engineering, business email compromise, account takeover, and data loss.

Unlike other vendors that use previous attack data, rules, and signatures to try and catch future attacks, Darktrace uses a self-learning AI that understands 'normal' for every organization and user account, allowing accurate detection known and unknown threats – offering protection against zero-day and multi-vector attacks even if it has never been seen before. Designed from the ground up to build on the benefits of your native email provider – to not only stop more threats, but eliminate mail latency, ongoing configuration maintenance, and the need for duplicate costs across your IT estate.

Darktrace/Email revolutionizes email security management to drastically decrease the load on security teams. Contextual security awareness uplifts end-users to report fewer false positives than previously thought possible, while automating manual process like secondary analysis speeds up investigations. It delivers insights from your native email security and the rest of your security workflow as part of the Darktrace Active AI Security platform—including networks, endpoints, devices, identities, applications, and clouds. Only with Darktrace/Email can you stop threats 13 days earlier and gain the maximum ROI out of your existing native email provider and security resources.



Traditional Approach
- Attack-centric data
- Payload focused

Darktrace/Email Approach
- Business-centric data
- User/behavior focused

Figure 1: 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

Darktrace/Email revolutionizes email security management to drastically decrease the load on security teams. Contextual security awareness uplifts end-users to report fewer false positives than previously thought possible, while automating manual process like secondary analysis speeds up investigations. It delivers insights from your native email security and the rest of your security workflow as part of the Darktrace Active AI Security platform—including networks, endpoints, devices, identities, applications, and clouds.

Only with Darktrace/Email can you stop threats 13 days earlier[11] and gain the maximum ROI out of your existing native email provider and security resources.

[11] Darktrace Press Release, April 2023

DIGIMAX

Compared to its previous email security solution, Darktrace/Email successfully blocked 20-25% more suspicious emails.

Key Capabilities of Darktrace/Email

Leading Mail Protection

Stop the 38% of threats that evade all other email security solutions

Darktrace/Email combines behavioral and content analysis across inbound, outbound, and lateral mail, and Microsoft Teams messaging, to detect and stop the 38% of threats that other email security solutions – limited by the need for traditional rules, signatures, and payloads for detection – miss[12].

Darktrace/Email catches these sophisticated threats by understanding the normal email activity of your end-users. It analyzes thousands of data points for every message received – including language, tone, sentiment, links, sender profile, historical behavior of sender and recipient, and behavior of users across their entire digital activity.

Based on its analysis and a given anomaly score, a precise response is taken to either hold the email back entirely or neutralize the exact component of the email that makes it unusual – maintaining productivity while eliminating risk.

Darktrace/Email takes a range of autonomous targeted actions, including rewriting links, removing attachments, unspoofing the sender, or moving to junk. Where a campaign with similar malicious content is identified, Darktrace/Email can influence actions retrospectively to ensure full containment (see Table 2 for a complete list).

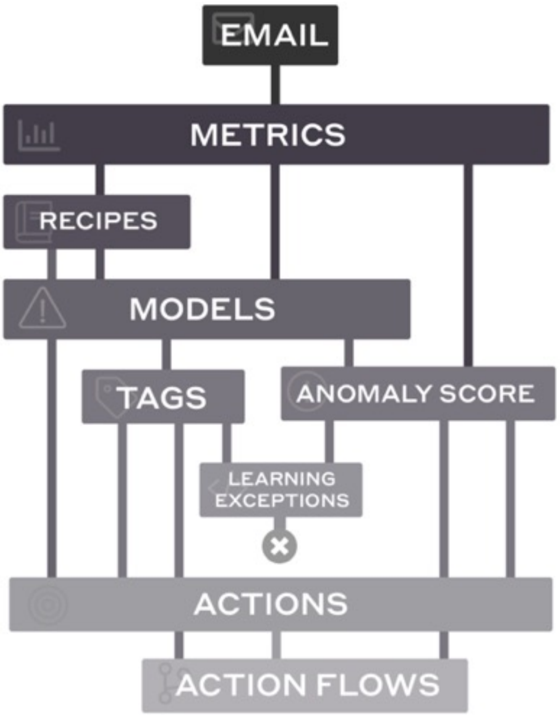


Figure 2: Darktrace/Email analyzes thousands of metrics for every message and assigns it a model and anomaly score to identify the specific risk of each communication

[12] Darktrace Threat Report 2023

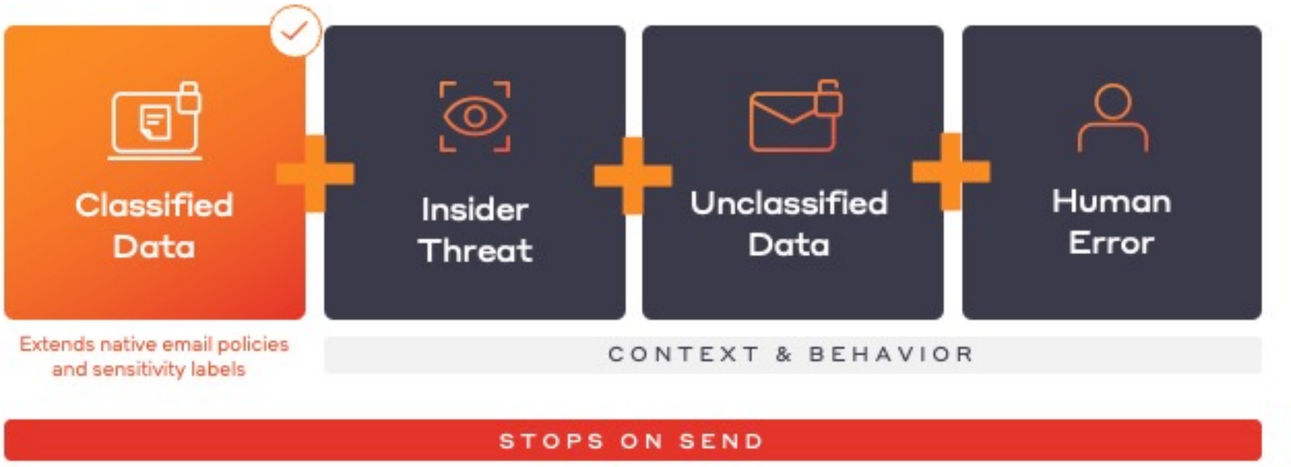
Data Loss Prevention (DLP)

Block the entire spectrum of outbound mail threats with advanced data loss prevention that builds on tags in native email to stop unknown, accidental, and malicious data loss

Through an understanding of normal at individual user, group and organization level with a proven AI that detects abnormal user behavior and dynamic content changes, Darktrace/Email actions outbound emails to stop unknown, accidental, and malicious data loss.

Traditional DLP solutions only take into account classified data, which relies on the manual input of labelling each data piece, or creating rules to catch pattern matches to try and stop data of certain types leaving the organization.

But in today's world of constantly changing data, regular expression and fingerprinting detection are no longer enough.



- **Insider threat**
  If a malicious actor has compromised an account, data exfiltration may still be attempted on encrypted, intellectual property, or other forms of unlabeled data to avoid detection. Darktrace analyzes user behavior to catch cases of unusual data exfiltration from individual accounts.
- **Unclassified data**
  Whereas traditional DLP solutions can only act on classified data through user defined labels, Darktrace extends analysis to the range of data that is either pending labels or can't be labeled, applying its understanding of the content and context of every email to detect data loss.
- **Human error**
  Because it understands normal for every user, Darktrace/Email can recognize cases of misdirected emails. Even if the data is correctly labelled or insensitive, Darktrace recognizes the context in which it is being sent could be a case of data loss and intervenes with a message to the user.

Classification efforts already in place are extended by Darktrace/Email, Microsoft Purview policies and sensitivity labels are used by the AI, avoiding duplicated workflows for the security team, combining the two approaches and ensuring organizations maintain control and visibility over their data.

Deploy DMARC quickly with AI

- Gain in-depth visibility and control of 3rd parties using your domain with an industry-first AI-assisted DMARC
- Stop spoofing and phishing from the enterprise domain, while automatically enhancing email security and reducing the attack surface
- Achieve easy compliance with requirements from Google and Yahoo
- Get visibility over shadow-IT and third-party vendors sending on behalf of an organization's brand
- Darktrace/DMARC integrates with the wider Darktrace product platform, sharing insights to help further secure your business

Account Takeover Protection

Significantly reduce the time it takes to detect a breached account from upwards of 200 days to the first day of suspicious activity[13].

Integrated seamlessly with Microsoft 365, Darktrace/Email provides the industry's most robust account takeover protection, taking a comprehensive view of potential threats directly within the interface. Every user is analyzed for various behavioral signals, such as authentication activities, resource usage, relationship history, and linguistic patterns.

This analysis creates an individual user account profile composed by signals from across the organization – including lateral mail analysis, DLP and Microsoft Teams – to understand what is normal for that employee and the wider organization. Unlike other solutions that rely solely on payload analysis for detection, Darktrace can spot the early symptoms of account takeover such as social engineering before a payload is delivered or exfiltration occurs. Early detection ensures that your reputation is protected by preventing your company or domain becoming an avenue for delivering business email compromise (BEC) or supply chain attacks.

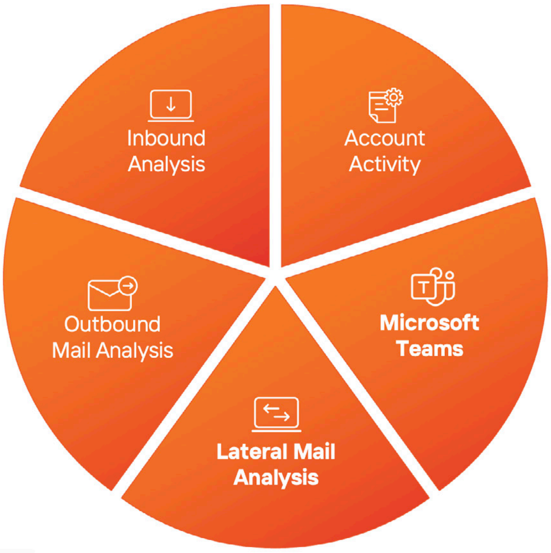


Figure 3: Darktrace integrates signals from across the entire mailflow and communication patterns to determine symptoms of account compromise

Operational Benefits

Up to 30x faster
Optional added Journaling reduces latency of API-only deployments

No mailflow disruption
Installation is not in-line, no need to redirect MX records

Flexible install in minutes
Via API-only or added Journaling

Reduce SOC operation efforts by 60%
Empower and educate end-user reporting of phishing attempts

Detect more advanced malicious URLs and web pages
Advanced behavioral web analysis that stops 70% more advanced threats than the leading cloud email security vendor

Contain investigations in one console
With full search, analysis, and reporting across email and messaging threats

[13] https://www.ibm.com/reports/data-breach: Compromised credentials

End-User and SOC Worfkflows

Achieve more than 60% improvement in the quality of end-user phishing reports and detection of sophisticated malicious weblinks

Darktrace/Email improves end-user reporting from the ground up to save security team resources. While other solutions assume that end-user reporting is of poor quality, Darktrace prioritizes improving users' security awareness to increase the quality of end-user reporting[14].

Users are empowered to assess and report suspicious activity with Cyber AI Analyst generated narratives and contextual banners on potentially suspicious emails, resulting in 60% fewer benign emails reported. While AI learns from the user to augment detection, the interactions of native users also inform how the AI learns what's normal, to improve its decision-making and overall accuracy. Over time, the AI starts to automate the organization of a user's non-productive mail, saving an average $5 per end user per month in regained productivity[15].

Once emails are reported, Darktrace/Email's Mailbox Security Assistant automates their triage with secondary analysis combining additional behavioral signals – using x20 more metrics than previously – with advanced link analysis to detect 70% more sophisticated malicious phishing links[16]. This directly alleviates the burden of manual triage for security analysts and reduces the amount of emails reaching the security team.

Darktrace/Email uses automation to reduce time spent investigating per incident. With live inbox view, security teams gain access to a centralized platform that combines intuitive search capabilities, Cyber AI Analyst reports, and mobile application access – eliminating console hopping and accelerating incident response.

> The fact that Darktrace detects new email attacks instantly, 13 days before anybody else does, is a game changer. For CIOs hours are important but two weeks is the difference between protection and devastation.

Gregory Smith,
/ Former CIO, WWF

Speed mean time to respond with **customizable AI investigations** and **automated remediation**

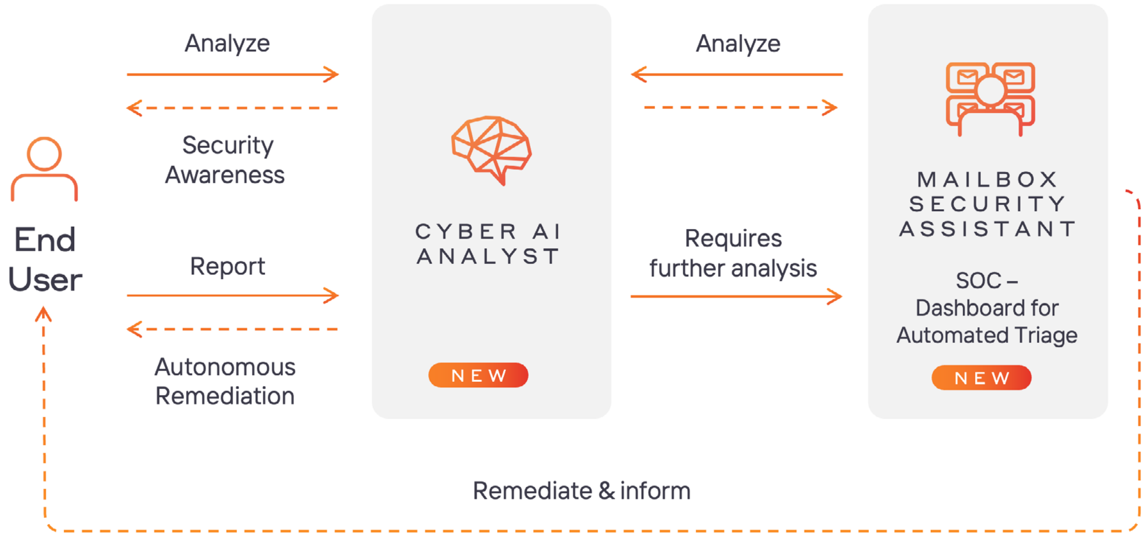


Figure 4: Darktrace uplifts the end user to drastically decrease the load on security teams, while centralizing and speeding analysis for initiated investigations

[14] Internal Darktrace research

[15] Internal Darktrace Research

[16] Internal Darktrace Research

Microsoft and Darktrace – Better Together

Microsoft

Darktrace/Email, hosted on Microsoft Azure, complements Microsoft security with Self-Learning AI to create a layered defense, uniting attack-centric and business-centric approaches to threat detection. Darktrace/Email was designed with Microsoft in mind to avoid duplicated workflows and capabilities, so purchasing and resource investments in Microsoft will be reflected in Darktrace.

Microsoft and Darktrace/Email together deliver the foundational components of email operations such as archiving, with leading known unknown threat detection, including early-stage pre-payload phishing attempts. Darktrace/Email integrates with both Microsoft 365 and Microsoft Exchange.

Deployment

Respond to threats 30x faster than traditional gateways and cloud email security providers [17]

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

TABLE 1: DARKTRACE/EMAIL DEPLOYMENT OPTIONS

Providing an advanced alternative to secure email gateways

- **Improve on performance:**
  Secure email gateways rely on centralized data, meaning they can only detect previously seen threats. Darktrace has unlimited visibility into all communications combined with behavioral anomaly detection to stop all known and unknown threats.
- **Eliminate maintenance:**
  Secure email gateways 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 like a secure email gateway – so native security efforts remain active and Darktrace provides additional security without overlap.
- **Centralize costs and improve ROI:**
  Eliminate the duplicate costs of operating a secure email gateway alongside your native email provider and improve your return on investment with better protection supported by optimized workflows.

[17] Internal Darktrace Research

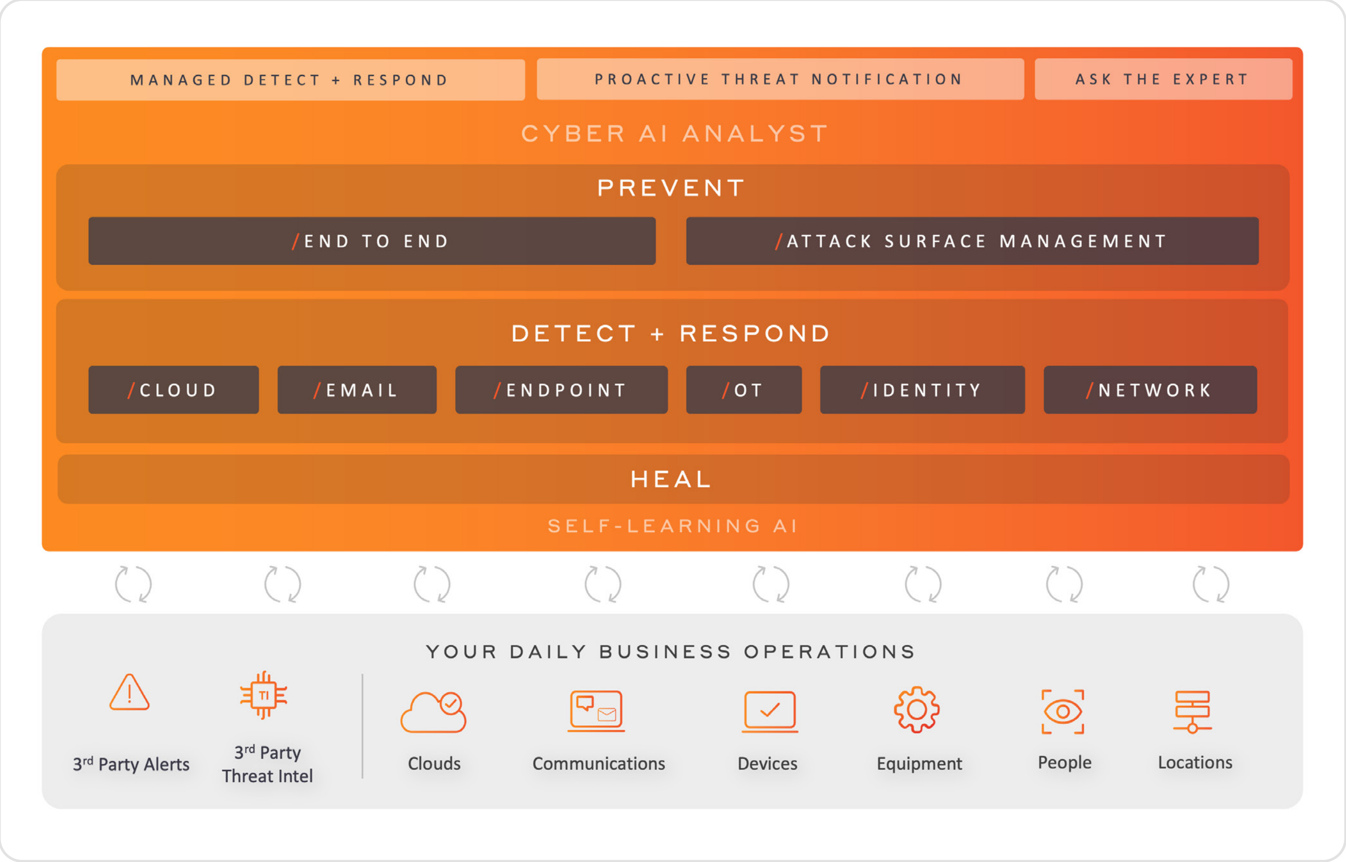
Darktrace ActiveAI Security Platform

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.

Darktrace PREVENT creates attack paths based on email as the most common attack vector while detections triggered by emails are used to better identify network or SaaS events that may have resulted from an email-borne attack. Cyber AI Analyst also incorporates email into the analysis of multi-domain attacks providing a complete investigation without the need for manual data pulls. Meanwhile, the overall attack surface for email is reduced via AI-assisted support for DMARC, stopping spoofing and phishing to preventatively harden defenses.

Darktrace is the first of its kind to provide proactive cyber defense in a single holistic platform. To achieve this, Darktrace pioneered the use of ActiveAI Security that continuously learns from your day-to-day business operations, applying context from your enterprise data ingested from internal native sources including email, cloud, operational technology, endpoints, identity, applications and networks, and external sources of third-party security tools and threat intelligence.

Through this approach, Darktrace provides the ability to visualize and correlate security incidents uninhibited by the siloed approach of individual point.



Darktrace/Email Actions

Targeted actions to reduce risk while maintaining the flow of business

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.
Add Banner	Adds a banner with custom text to the start of the actioned email which is visible to the end recipient. The color of the banner is defined by the severity selected when the action was configured. Multiple tags can be added to the same email to indicate the threat profile detected. Adding tags to emails can help educate the end user on the potential threats detected in the specific email

TABLE 2: DARKTRACE/EMAIL ACTIONS

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its 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 achieve an optimal state of cyber security. Breakthrough innovations from its R&D Centers have resulted more than 165 patent applications filed. Darktrace employs 2,300+ people around the world and protects over 9,200 organizations globally from advanced cyber-threats.

Scan to
LEARN MORE

DARKTRACE
Evolving threats call for evolved thinking™

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

darktrace.com