DARKTRACE

WHITE PAPER

A CISO's Guide to Email Security in 2023

CONTENTS

The Email Threat Landscape

In 2023, email is still the primary connective tissue for the majority of businesses. Nearly 350 billion emails are sent every day, many of them containing sensitive data, confidential plans, and financial transactions.

Considering this overwhelming reliance on email communication, it's a worrying fact that more than 90% of all successful cyber attacks start with a phishing email*.

Generative AI

With the help of tools like generative AI and ChatGPT, attackers are leveraging new technologies to impersonate trusted organizations and contacts with increasing sophistication – including damaging business email compromises, realistic spear phishing, spoofing and social engineering.

Darktrace researchers observed a 135% increase in 'novel social engineering attacks' across thousands of active Darktrace/Email customers from January to February 2023, corresponding with the widespread of ChatGPT**.

Targeting Supply Chains

On top of that, today's businesses rely on hundreds of interactions with suppliers and partners at every digital layer. Attackers are targeting the weakest links in supply chains to launch mass-scale fraud campaigns across multiple organizations:

62% of cyber attacks in 2021 exploited the trust of customers in their supplier***.

*Deloitte, 2020, "91% of all cyber attacks begin with a phishing email," https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

**Based on the average change in email attacks between January and February 2023 detected across Darktrace/Email deployments with control of outliers.

***ENISA Threat Landscape for Supply Chain Attacks, 2021, "62% of cyber attacks exploited trust in their supplier", https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

> Business Email Compromise cost over $2.7 billion in 2022
>
> **FBI**
> / FBI 2022 Internet Crime Report

Abusing Legitimate Infrastructure

Attackers are even moving away from creating their own attack infrastructure – instead they are increasingly relying on web-sites that pass reputational checks and legacy based systems to conceal their attacks. By piggybacking off legitimate cloud infrastructure like SharePoint or Google Drive, cyber criminals can evade the reputational checks of many security vendors, even those using AI.

Account Takeover

While many attacks enter via the inbox, it is rarely the final destination.

Account takeover is a major concern for businesses - once credentials are obtained via phishing, cyber criminals are using trusted accounts as a springboard to launch a further assault via ransomware or outbound supply chain attacks. In an era of escalating threats with email as the primary target, future-facing organizations are looking to embrace the new wave of email security.

Adopting technologies that can adapt to attackers' latest techniques and defend autonomously is likely to be critical to retaining cyber stability in an increasingly advanced and fast-changing landscape.

> When it comes to something like phishing emails, training on how to spot these is important but we simply cannot put the focus on humans to spot these well-researched, targeted email attacks.

CEO
/ Transport & Logistics

Figure 1: Current email tools don't protect against more sophisticated, research-based attacks

Looking to the Past: The Legacy Approach

Key Takeaways:

- Reliant on rules and deny lists
- Fails to catch novel or sophisticated threats
- False positives disrupt business
- Constant maintenance and policy up-keep required

> We're a global company but our security team also needs to sleep, so we needed something to monitor and respond in real time 24/7.

Global Head of Information Solutions,
/ Renewable Energy Generation

The majority of tools used by organizations today rely on using historical attack data to try and stop known threats from reentering the inbox. These tools rely on previous threat intelligence and on assembling 'deny-lists' of known bad elements of emails already identified as malicious. Every email is checked against these lists of 'bad' IPs, domains and file hashes, and if there is a match the email is held back.

In addition, security teams can create static policies to tailor these controls to their organization. This entails spending hours scrolling through Indicators of Compromise (IoCs) and updating their infrastructure with new rules to defend against the latest attacks. Because they are focused solely on the point of breach, these tools tend to take an oversensitive approach and surface plenty of false-positive emails, which the security team have to go through and release manually in the platform.

Such an approach invariably means that existing security tools are on the back foot, racing to update their protocols at the pace of innovation of the attackers. By the time an IoC has been created and a rule updated, the cyber-criminal has usually moved on. As attacks get more targeted, solutions that rely on reputations and historical attack data become more outdated and inadequate.

Some newer integrated cloud email security (ICES) vendors attempt to use AI to improve this flawed approach, looking not only for direct matches, but using "data augmentation" to try and find similar-looking emails. Despite leveraging new technology, this approach is still historically-focused and therefore blind to novel threats – it requires a Patient Zero to learn from in the first instance.

At the same time, attackers are innovating to bypass legacy tools – by abusing legitimate cloud infrastructure like SharePoint to direct users to malicious domains, or creating thousands of new domain names that don't yet have a reputation.

There is also a pressing risk from the supply chain, if a legitimate user's account is compromised and used to send out malicious phishing emails. Since these emails come from a trusted domain they are too often allowed through.

What's more, email security often focuses solely on the inbox, siloed from the rest of the organization. Consequently, once an attack does get through it becomes redundant.

For organizations using legacy email security systems, this all leads to a perfect storm of advancing threats, overstretched security teams and increasing time spent maintaining policies – leading to a growing risk of exposure to attack.

13 Days

Darktrace analysis reveals that other email security solutions, including native, cloud and 'static AI' tools, take an average of 13 days from an attack being launched on a victim to that attack being detected

> 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
/ Professor at Georgetown University and Former CIO/CTO

Email Security in 2023

There is a seismic shift underway in the industry, from "secure" email gateways to intelligent AI-driven thinking. Organizations are consequently re-evaluating what they need from their security infrastructure – 3,000 organizations are already relying on this approach.

In 2023, email security needs to fight AI with AI to match the advancing sophistication of cyber attacks. This entails moving beyond the 'allow-deny' philosophy of the past to evaluate context and behavior for sender and recipient – understanding the human behind every email. Security solutions can no longer rely on the assumption that the next attack will look like ones they have seen before.

What's more, email security today means more than just inbox protection. Account takeover, accidental data loss through misdirected recipients, malware and ransomware are all key concerns which can only be tackled by a more holistic view of a user across their account, network and apps.

Finally, the relationship between security teams and their email policies needs resetting – through tools that can act autonomously, solutions that adapt with the organization and accessible user interfaces.

Darktrace/Email™

Key Takeaways:

- Learns behavior patterns of email users to establish 'normal'
- Responds proportionately to the full range of email attacks
- Enhanced protection beyond the inbox
- Integrates with wider security ecosystem

Darktrace has developed a fundamentally different approach to email security, one that doesn't learn what's dangerous from historical data but from an in-depth understanding of each organization and its users.

Darktrace/Email focuses on individuals – how each person uses their inbox and what constitutes 'normal' for each user – in order to detect what's not normal. Self-Learning AI™ technology builds profiles for every email user, including their relationships, tone and sentiment, content and link sharing patterns, and thousands of other signals.

It makes use of context – how and when people communicate, and with who – to spot the unusual and to understand when something doesn't look quite right – and why.

Because Darktrace understands the human behind email communications – rather than knowledge of past attacks – it can stop the most sophisticated and evolving email security risks like generative AI attacks, BEC, account takeover, supply chain attacks, human error and ransomware.

By approaching email through the lenses of the security team, the employees, and integration with data sources across the digital estate, Darktrace/Email elevates its powerful capabilities into a comprehensive security strategy.

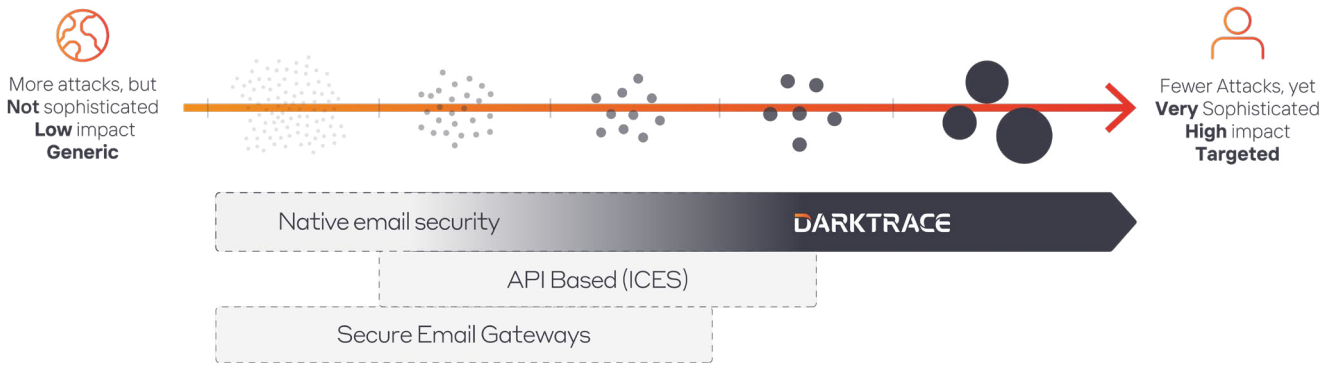


Figure 2: Combined with native email security, Darktrace catches the full spectrum of sophisticated threats

Precision Detection and Response

Darktrace AI builds behavioral profiles for every single person in an organization and continuously learns the relationships between senders and how they interact. When a new email arrives, regardless of its threat sophistication, Darktrace can determine in real time whether or not it belongs in a recipient's inbox and why.

This contextual understanding allows Darktrace to respond precisely according to the nature of each email. Rather than adhering strictly to a 'block' or 'allow' decision-making framework, an accurate sense of what makes an email suspicious means that it can take autonomous action according to the exact nature of the threat.

While emails with a high threat level will be withheld and escalated to the security team, there are plenty of emails that fall below that threshold. In these instances, Darktrace takes the least aggressive action necessary to remove only the riskiest parts of an email, rather than a broad blanket response. It can take a range of actions: leaving an email untouched, moving it to junk, rewriting links, remove attachments, or holding a message back entirely.

This approach neutralizes threats while repairing or allowing unusual but safe emails, in order to reduce risk without disrupting normal business operations. Precision detection and response frees up valuable decision-making time for security teams, who are no longer obliged to spend time releasing potentially safe emails which have been withheld out of caution.

> Darktrace/Email is so easy to set up and integrate, and it really turned the lights on in our email environment.

CISO
/ IT Services

> Darktrace/Email is as close to 'set it and forget it' as you can find in the email ecurity market. We've been using the product for a few months now and we have seen zero phishing attempts make it into our organization.

CIO
/ Transportation

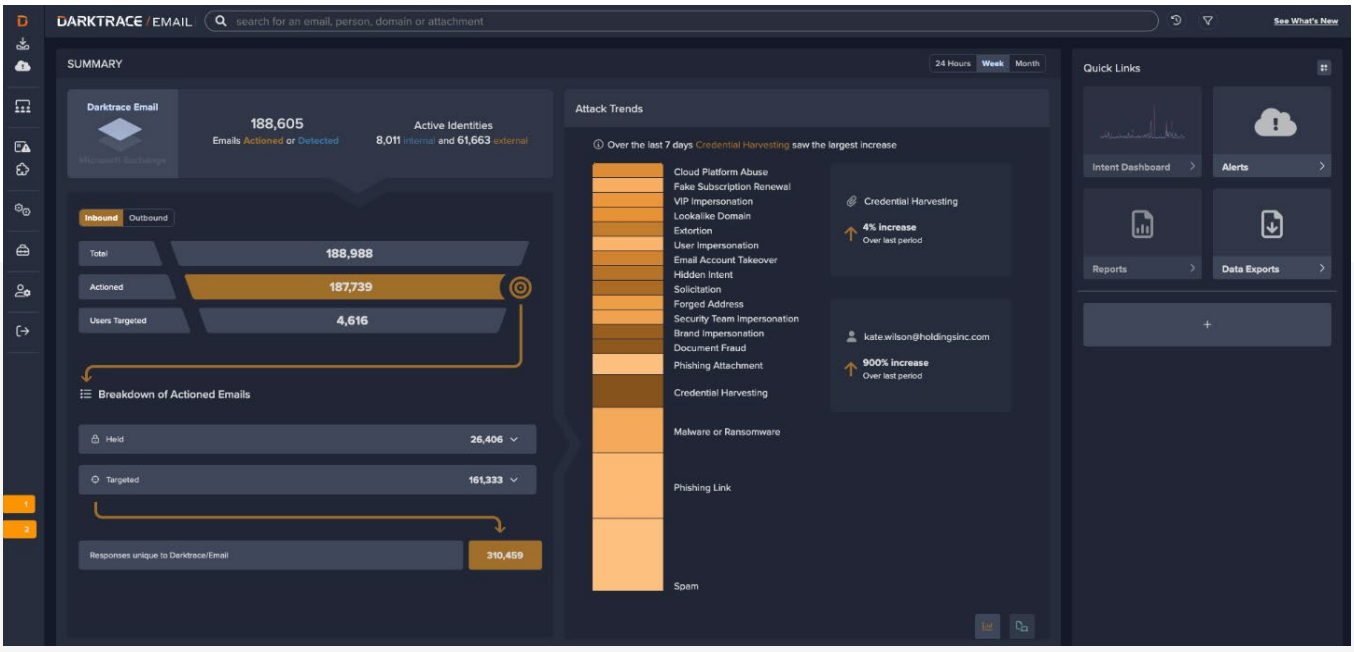


Figure 3: Current email tools don't protect against more sophisticated, research-based attacks

360-degree View of Every User

A user's activity isn't limited to Microsoft. Throughout their day they have many different touchpoints, which can all be compromised in an attack. Consequently, security teams need visibility not just over email breaches but of what happens once an attacker has control of an inbox. This means understanding a user's behavior in the inbox as well wider account activity in Microsoft 365 and beyond.

Such an understanding allows a system to understand when unusual login activity may point to an account takeover - especially when suspicious email activity is witnessed shortly afterwards.Instead of having multiple dashboards, the UI captures a user's activity across email and their Microsoft or Google account in a single pane of glass, for instant visibility.

With this 360° view of the user, subtle indicators of account compromise can be detected wherever they appear, and the attacker locked out across all accounts.

Darktrace/Email combines with Darktrace/Apps and Darktrace/Endpoint to offer complete protection against identity-based attacks, covering the full context of a user across apps like Sharepoint, Dropbox and Salesforce, as well as their device on the network.

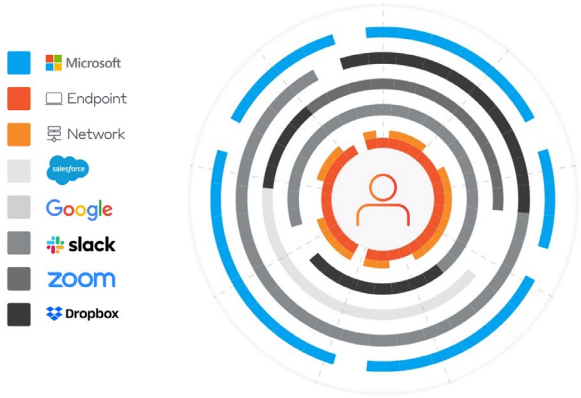


Figure 4: Darktrace looks beyond the inbox to cover the full scope of a user's account activity

Streamlined Workflows

Darktrace/Email considers the security team at every touchpoint, reducing time-to-access and time-to-meaning wherever possible. Precision detection and response dramatically reduces the time security teams need to spend in their tools – but when they do log in they can benefit from instant visibility and simplified workflows to access the information they need, quickly.

An optimized user interface doesn't just make team's lives easier – it supports organizations to advance their security posture. The UI provides a high-level view of the email environment of an organization, including a real-time snapshot of active user identities, targeted user and actioned emails, segmented by type of attack.

Admins also have the time-saving option of previewing links and emails within the UI, preventing the need to switch between windows.

Furthermore, Darktrace/Email has an open architecture that makes it immensely flexible. In addition to its mature integration with Microsoft, it is both API-driven and compatible with syslog, so it can integrate with any security tool or ticketing system and feed into any SIEM or SOAR.

This unlimited capacity for integration allows Darktrace to detect and respond to threats more precisely with access to more data, as well as reduce the security team's time-to-meaning by condensing all relevant information in a single UI.

Darktrace/Email can be accessed from Darktrace's Mobile App, so security teams can investigate, triage, and release emails at any time, even on the go. In this way, Darktrace not only fits into the greater security posture, but also with employees' day-to-day workflow.

Misdirected Email Protection

As cited by Gartner*, accidental data loss – often known as misdirected emails – is increasingly a concern for businesses. While the cause is often basic human error, implications could include a data leakage incurring GDPR or regulatory fines.

Because it understands normal for every user, Darktrace/Email can recognize cases of misdirected emails. It can catch the mistakes, typos and incorrect autocorrects that often result in sensitive data going outside of the business to the wrong address. If an action is highly unexpected, it will double-check with the user to ask: is this the intended recipient? – stopping them in their tracks before the email is sent.

*Gartner® 2023 Market Guide for Email Security

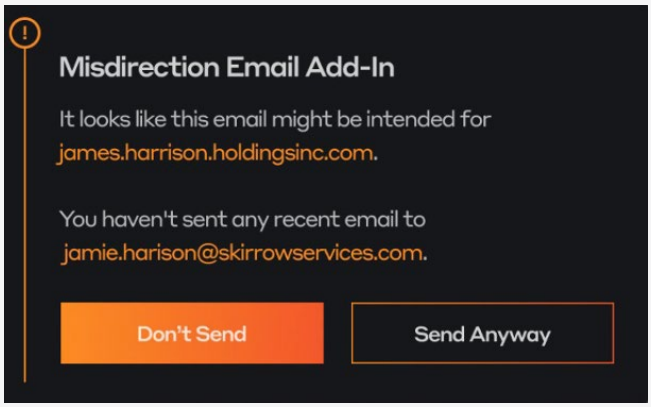


Figure 5: Through understanding users, Darktrace/Email identifies when an email is about to be sent to the wrong recipient

Enhanced Employee Experience

In the digital age, security is everyone's responsibility.

Email security today needs to educate and engage employees at the right level to arm them against attacks, as they are ultimately the last line of defense.

By empowering employees with information, while still leaving critical decisions to the security team, organizations can further strengthen their security posture.

Darktrace/Email encourages real-time security awareness by generating a digest in Explainable AI – natural language processing that translates millions of data points and micro-decisions into clear digests that explain what actions the AI has taken and why. Armed with context about why the AI found an email suspicious, employees can choose whether to release, bin, or report it to the security team.

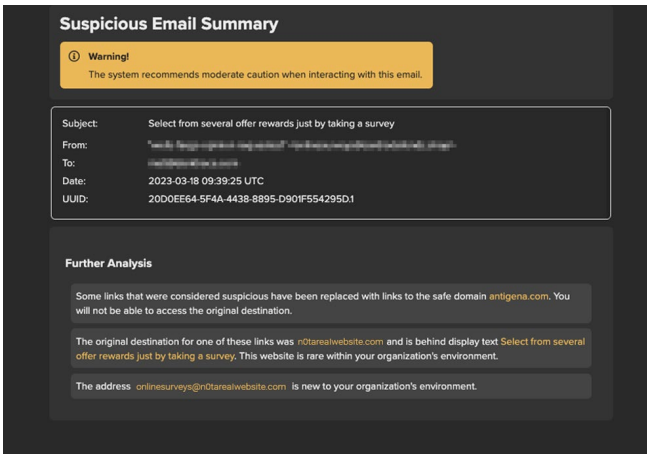


Figure 6: A high-level digest summarizing why an email has been deemed suspicious and what action the AI has taken

These actions feed back into the UI, which gradually improves its decision-making as a result. This Employee-AI feedback loop determines the appropriate level at which to engage users, while not relying on them for threat detection.

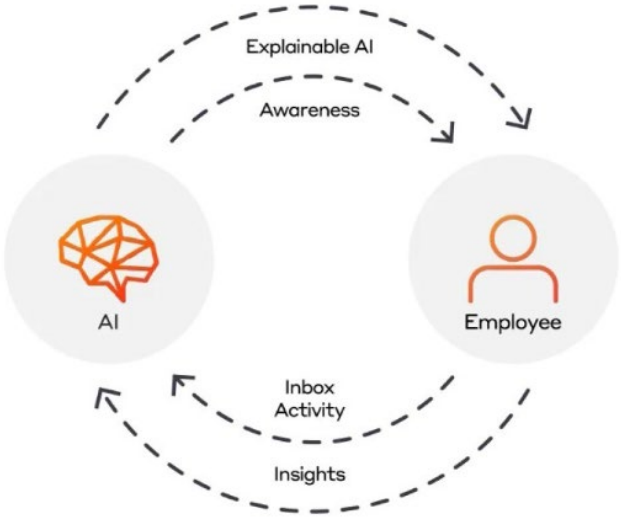


Figure 7: End users receive context of what action Darktrace/Email has taken and why – user input then feeds back to gradually improve AI decision making

At the same time, employees can feel the tangible benefits of Darktrace/Email on their productivity. The AI learns users' habits through their native inbox activity, such as which emails they consistently move to junk. Over time, it will remove unwanted mail, as well as non-productive spam.

Taking this admin out of employees' hands changes the narrative around security tools – bolstering productivity instead of hampering it and freeing up valuable time for useful work.

> Darktrace/Email only took ten or fifteen minutes to get going, and the value it would bring to the company hit home almost straightaway.

IT Director
/ Food and Beverage Manufacturing

Connecting Email Security with the Enterprise

Connecting email with the wider security ecosystem yields enormous benefits in the accuracy of decision-making and getting the full context of an attack.

Deploying AI to multiple data sources that can feed back and communicate allows for continuous improvement of an organization's defensive posture.

All Darktrace products make up a powerful Cyber AI Loop, four interconnected AI engines that allow defenders to simultaneously prevent, detect, respond, and ultimately heal from cyber attacks.

PREVENT Forewarns Darktrace/Email of Potential Spoof Domains

Connecting an email security tool with external insights from the attack surface yields further benefits. Proactively identifying potentially malicious domains spoofing your brand and then feeding this information back means the email security tool can be on high-alert should it see any activity from these domains.

For example, if PREVENT/ASM spots shadow domains being created that could be used to impersonate an organization, it informs Darktrace/Email so it can block any malicious messages being delivered if these spoof domains are activated.

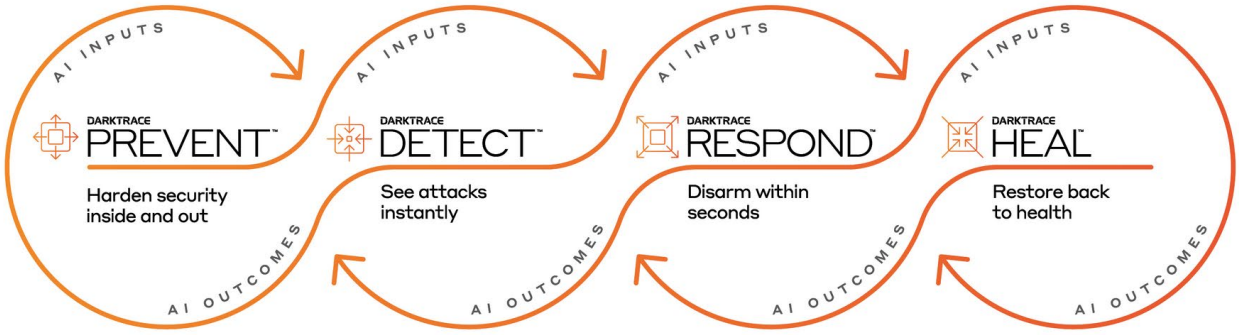


Figure 8: Darktrace/Email is a powerful tool on its own, but becomes stronger when part of the Cyber AI Loop

As email is so intertwined with the rest of the digital estate, it no longer makes sense for email security to exist in a silo. Connecting Darktrace/Email with the wider security ecosystem streamlines workflows, enhances AI decision-making and further reduces risk. Darktrace/Email connects to other Darktrace coverage areas, including:

/Apps /Endpoint /Network.

Darktrace/Apps brings in visibility across other applications like:

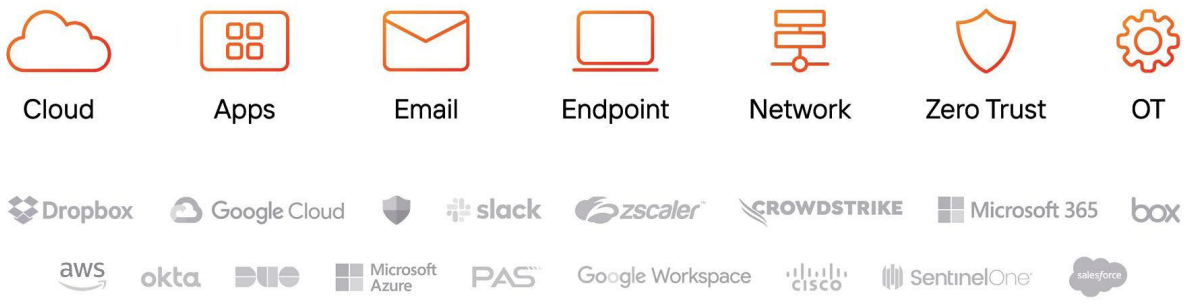
Zoom Slack SharePoint OneDrive

shining a light on activity like resource misuse, compliance issues and third party risks.

Darktrace/ Network offers full context so that /Email can see when a domain has never been seen or interacted with before, not just within an email environment, but across an entire whole organization.

Through integrating with the Cyber AI Analyst tool, email activity is brought into enterprise-wide investigations with cloud, apps, and network activity.

It uses data to build better context around security incidents, connecting the dots across the digital estate to trace how a wider problem may have originated in email and spread to apps, network or cloud – allowing the security team to communicate key takeaways generated by Darktrace/Email to anyone within the organization.



Real-World Threat Finds

Stolen Credentials and Account Takeover

Compromise Across Microsoft Outlook and Teams

Darktrace picked up on several anomalies at a public accounting firm, including a sudden surge in outbound email traffic, as well as an unusual login location: while the company was located in Wisconsin, an IP address located in Kansas was used to log in to both Outlook and Microsoft Teams accounts.

'Impossible travel' rules alone would have missed these anomalies, but an understanding of activity and behavior across different SaaS applications allowed Darktrace's AI to recognize these events as one systematic case of credential theft.

Five minutes later, the threat-actor tried to create a new email rule and send 220 outbound emails containing a generic subject line and an attached PDF. Darktrace/Email connected unusual login to the anomalous outbound email behavior and responded autonomously to neutralize each action and disable the compromised account, while offering security teams full visibility of the extent of the attack.

Figure 9: Darktrace detected a Microsoft Teams login from an 100% anomalous destination

> Our Office 365 environment, for every license and every mailbox across the enterprise, is a comprehensive footprint. Darktrace covers those critical areas where phishing risks and ransomware attacks typically are introduced into any organization.

CIO
/ Charity

> Darktrace /Email has the ability to suspend all activity it deems malicious.

General Manager
/ Transportation

Supply Chain Account Takeover

Phishing Attack Leads to Microsoft 365 Compromise

Darktrace/Email detected that a logistics company was under sustained attack. The cyber-criminal had already performed account hijacks on a number of their trusted suppliers and partners, and had sent out several tailored emails from these accounts which slipped through the gateway.

Darktrace/Email was being trialed in passive mode, so the attack was not shut down in its initial phases. Fifteen of these emails were opened, and one employee clicked on a malicious link, which led them to a fake Microsoft login page for credential harvesting. Three hours later, an anomalous SaaS login was detected from an IP address not seen across the business before. Shortly afterwards, Darktrace detected an anonymous sharing link being created for a password file.

The following day, the attacker sent out further malicious emails from this account to trusted business associates using the same methodology – sending fake and targeted RFPs in an attempt to compromise credentials.

Darktrace identified this anomalous behavior, graphically revealing that the attacker sent out over:

1,600 Tailored Emails in 25 Minutes

The Managed Security Service Provider (MSSP) running their cloud security was completely unaware of the account takeover.

With Darktrace/Email, Self-Learning AI autonomously stitched these disparate events together into a single incident and gave the security team full visibility of the account takeover.

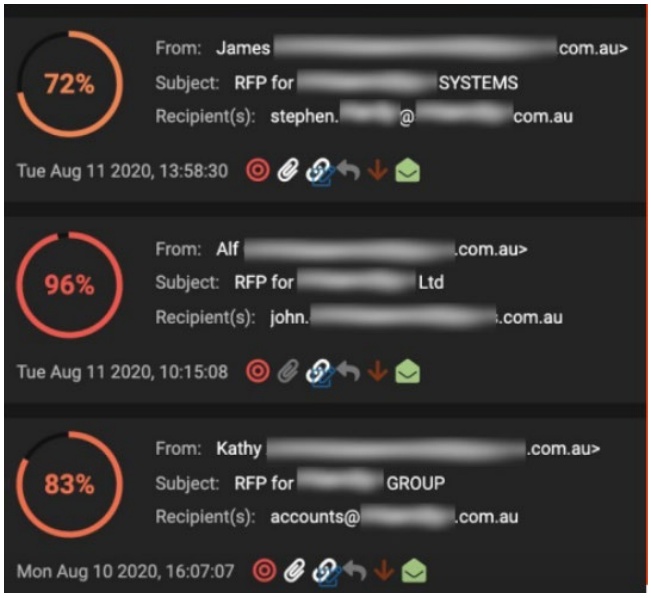


Figure 10: A sample of the malicious emails from the hijacked accounts; the red icon indicating that Darktrace/ Email would have actioned these emails

Social Engineering and Solicitation

Stopping a Targeted Credential-Grabbing Attack on McLaren

Darktrace/Email detected an email sent to one of McLaren's executives, prompting them to sign a financial document. The email appeared to come from DocuSign and contained a malicious link hidden behind the text 'Review Document'.

Had the executive clicked on the link and attempted to log in, they would unknowingly have sent their credentials to the attacker.

The malicious email was sent over the Imola GP race week-end, which was a high-pressure 48 hours for the McLaren team. Darktrace/Email recognized the sender as a new contact and deemed the link as suspicious.

As a result, it double locked the link and automatically moved the email to the executive's Junk folder, all without having to alert the on-call cyber security team over the weekend.

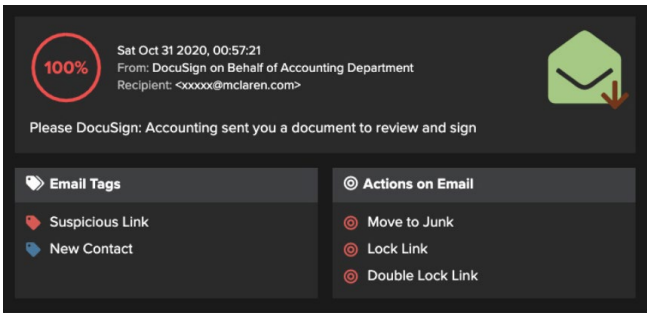


Figure 11: An interactive snapshot of Darktrace/Email's user interface surfacing the email

> Using AI, Darktrace can detect and respond to email-borne threats and cloud-based attacks that other tools miss
>
> **CIO**
> / Government Administration

'Piggybacking' off Legitimate Infrastructure

Attempted Credential Harvesting Using Sharepoint

Darktrace/Email detected a sophisticated attack in which a cyber-criminal used legitimate websites and links to conceal a credential phishing attempt.

The attacker was aiming to 'hitch a ride' off the back of known infrastructure – in this case SharePoint – to bypass the reputational checks that many historical-facing security vendors rely on. In this example, they used SharePoint to assign a task to an email user, which linked to a document within the platform.

Since both the notification email address

no-reply@sharepointonline.com

and the domain name

sharepoint.com

are both established and legitimate addresses, this email would have been allowed through by the majority of security tools.

If the user clicked on the link, it would have taken them to a document hosted in Word Online, another established 'safe' destination. A hyperlink within the document opened up a web resource hosted on app-building platform web.app: a known website, but one on which users can host anything they want.

In this case, the attacker had created a fake login page posting the inputted data to a bucket on the legitimate site liveformhq.com where they could harvest the credentials.

Darktrace/Email surfaced this email as anomalous due to the inducement to enter credentials, despite the established correspondent, domain and high communication history. It locked the link, moved the email to junk and added a contextual banner.

With this attack, the layers of legitimacy extended many layers deep. Only by judging every email in context of the organization and user was Darktrace able to neutralize this highly sophisticated threat.

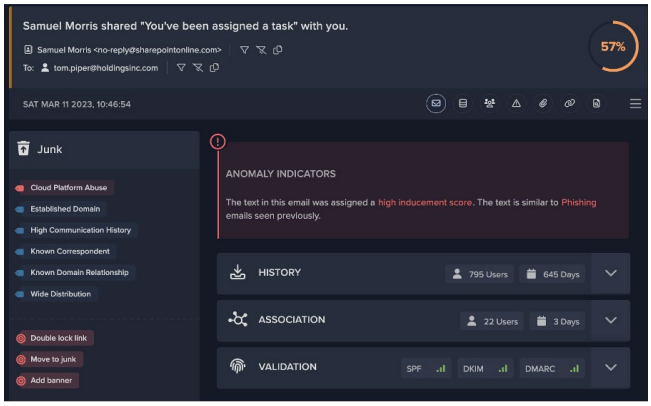


Figure 12: Digest explaining why Darktrace tagged the email as malicious and what action was taken

Deploying Darktrace/Email

The industry is shifting to vendors that install through API-only, allowing for faster and more seamless delivery of security solutions. However, Darktrace offers a range of options to balance speed of deployment with speed of operation.

Darktrace/Email can install via API only for a quick set up, **which gets the system up and running in seconds.**

Alternatively, customers can choose to enable journaling to reduce latency and ensure best in class detection speeds, **as much as 30 times faster than API-only.**

Once deployed there is minimal maintenance for the security team – Darktrace scales from just a handful of inboxes to tens of thousands, without any rerouting or additional configurations aside from accepting permissions.

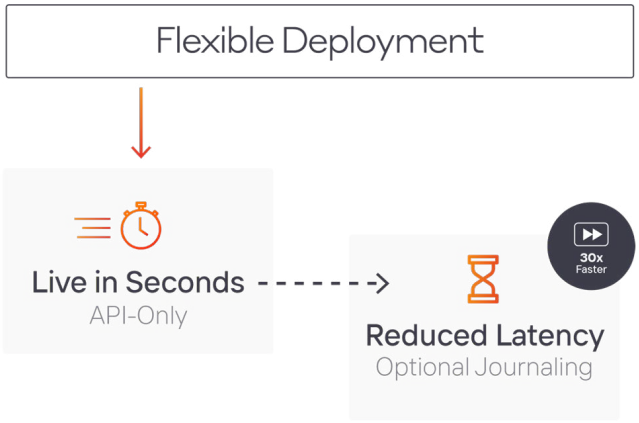


Figure 13: Darktrace offers API-only deployment with optional journaling for reduced latency

> Darktrace has greatly enhanced our ability to be proactive with email security. Darktrace's ease of use allows us to better train our team and there's no longer a huge learning curve to figuring out and digesting complex transport rules and other difficult ways of doing email security.

Senior Systems Engineer
/ Renewable Energy

> We quickly installed it to defend server and workstation subnets as well as company-wide email. After a month of self-learning, it learnt the normal behavior of my organization and got smarter and more meticulous with every passing minute. It gives us complete real-time visibility of systems and data.

CIO
/ Government Administration

Industry Recognition

2021 SC Europe Awards:

Winner – Best Security Company

UK IT Industry Awards

Winner — Security Innovation of the Year

Go:Tech Awards 2022

Winner – AI & Machine Learning Award

Cyber Defense Global InfoSec Awards 2022

Winner – Cutting Edge in Cybersecurity Artificial Intelligence

Winner – Market Leader in Enterprise Security

The American Business Awards (The Stevies®) 2021

Silver — Achievement in Product Innovation (Darktrace, Version 5)

Bronze — Company of the Year: Computer Software

Bronze — Artificial Intelligence/Machine Learning Solution (Darktrace/Email)

2021 Globee Awards

Gold — Customer Service and Support Team of the Year (Darktrace Customer Success)

Silver — Customer Service and Support Project of the Year (Darktrace PTN Initiative)

Marsh Cyber Catalyst Designated Solutions 2020: Cyber Catalyst Designation (Darktrace DETECT/Cloud +Network and Darktrace/Email)

Darktrace/Email has been designated as a Marsh Cyber Catalyst solution for 2020. Evaluated by leading cyber insurers, Marsh has recognized that Darktrace/Email plays crucial role in reducing cyber risk

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. It is delivering the first ever Cyber AI Loop, fueling a continuous end-to-end security capability that can autonomously prevent, detect, and respond to novel, in-progress threats in real time. Darktrace employs over 2,200 people around the world and protects over 8,100 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 97242 2011
info@darktrace.com
darktrace.com