

Building a modern security stack

Why Your NDR and Email Security Solutions Need to Work Together





Contents

02	Why unified security is no longer optional
03	Inside the attack: How threats move from inbox to internal compromise
04	Darktrace / NETWORK + / EMAIL: Two best-in-breed solutions, one AI approach
06	Benefits of a common approach
06	Technical edge
08	Operational advantage
08	Commercial value
09	Buying scenarios: Point solutions vs. Platform security
10	Taking the next step

Abstract

Though many cyber-attacks start in the inbox, it's rarely their final destination. Threat actors continue to launch AI-driven, multi-stage attacks that begin with email and quickly spread across networks and cloud environments. In this landscape, siloed security solutions struggle to piece together attacks, leaving critical blind spots that slow the pace of defense. The most effective defense against modern threats is a unified AI approach that deeply connects email and network security.

This white paper explores:

-  How AI is accelerating multi-stage, multi-domain attacks
-  Why siloed email and network solutions are failing to keep pace
-  How a unified, multi-layered AI approach improves threat detection and response
-  Security, operational, and commercial benefits of an integrated approach

Why unified security is no longer optional

Email attacks are getting stealthier with the help of AI

Email remains one of the most targeted and effective initial access points for cyber-criminals, and AI is rapidly making these threats more convincing and harder to detect. Threat actors use generative AI to craft highly personalized phishing emails at scale, while also exploiting emerging techniques like [QR code phishing](#).

According to Gartner, email continues to be a significant attack vector for malware and credential theft – with network compromise as the goal.



23%

- **23% of security leaders** cited social engineering as the root cause of a recent external attack on their organization, with **phishing close behind at 21%**

(Forrester Security Survey 2024).

...and so are network threats

Once inside an organization, attackers can use AI to accelerate and automate every phase of the attack life cycle.

This might include:

- Researching potential infrastructure and free hosting providers
- Faster reconnaissance on target organizations
- Adaptive malware behaviour
- Credential harvesting at scale
- Payload development
- Assistance with malicious scripting and evasion techniques

These advancements allow attackers to operate faster, with greater precision, and at much higher volumes than before. According to the [UK's National Cyber Security Centre \(NCSC\)](#), by 2027 AI will almost certainly enhance attackers' ability to exploit vulnerabilities, making it easier for both state and non-state actors to launch sophisticated intrusions.



74%

But already, **74% of security professionals say AI-driven attacks present a major challenge for their organizations** ([State of AI Cybersecurity 2025](#)).

Why siloed solutions fall short

In response to a complex threat landscape, many organizations have accumulated a patchwork of best-of-breed tools: one for email security, another for network monitoring, others for end-point or cloud defense. But these siloed solutions rarely operate in true symbiosis.

Most likely, they share data through a SIEM or SOAR platform, producing alerts that lack the necessary context to understand the full scope of an attack. This fragmented approach can create blind spots between different stages of the attack chain, forcing security teams to manually stitch together events from disconnected dashboards and logs. And as attackers move faster and more stealthily across environments, these delays in detection and investigation can prove catastrophic.

Even heavy investments in EDR and XDR solutions often leave gaps, particularly around network activity, creating false confidence in the SOC's visibility. Agents cannot be installed everywhere throughout a modern network, and traditional tools that simply focus on 'known bad' activity do not detect unknown, novel or insider threats.

The reality is clear:

only a truly integrated solution – one that seamlessly connects email and network telemetry – can deliver the speed, visibility, and fluidity required to detect and respond to today's AI-enhanced attacks.

Inside the attack: How threats move from inbox to internal compromise

Let's take a look at a recent attack Darktrace observed.

The customer in question had Darktrace configured in detect-only mode, without response being active, meaning the compromise was able to escalate until the security team acted on the alerts raised by Darktrace.

Had autonomous response been enabled, it would have applied swift actions to contain the attack. Nevertheless, Darktrace was able to provide visibility across different areas of the customer's digital estate and piece together the attack, allowing the customer to quickly enact remediation. The below diagram shows how the attack progressed through their environment.

This threat story highlights a common pattern in modern attacks:

they move fluidly across the entire digital estate, from email to network and beyond. If security operates in silos, defenders are left with a fragmented view, delaying detection, disrupting response, and ultimately giving attackers the upper hand.

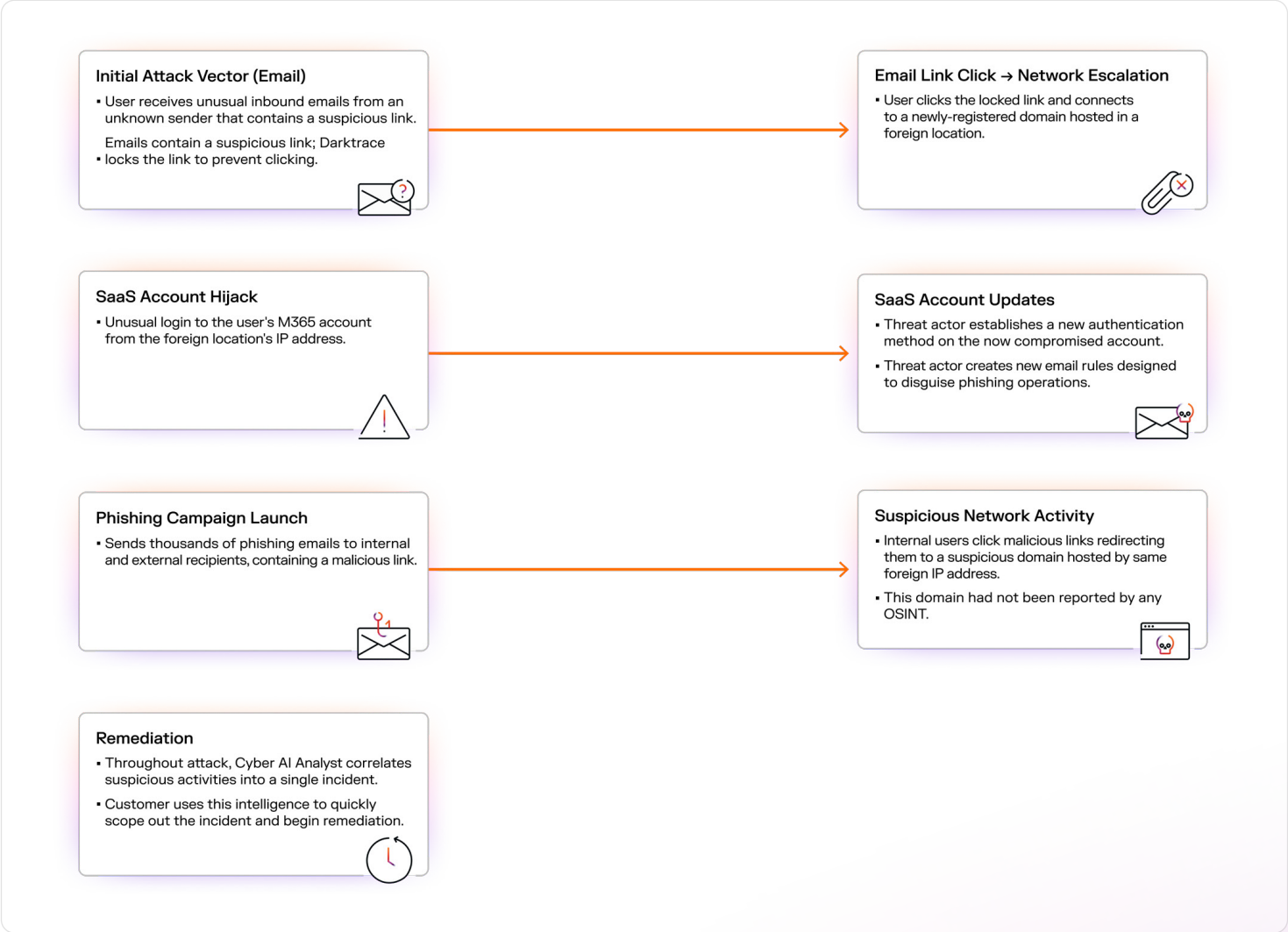


Figure 01: Diagram outlining an attack progressing from email to network and SaaS

Darktrace / NETWORK + / EMAIL

Two best-in-breed solutions, one multi-layered AI approach

Individually, Darktrace / NETWORK and Darktrace / EMAIL are powerful, industry-leading solutions.



Recognized as a Leader in the 2025 Gartner® Magic Quadrant™ for NDR, Darktrace / NETWORK brings its powerful, multi-layered AI to your modern network, neutralizing known and unknown threats in real time.

[Gartner Peer Insights](#): ★★★★★ 4.7* (465 ratings as of August 2025)



Darktrace / NETWORK has been shown to reduce alert noise by **almost 99% compared with an existing traditional NDR vendor**

(Darktrace customer in the energy sector)

08 Darktrace / NETWORK detects and contains zero-day vulnerabilities on average **8 days before public disclosure**

(Darktrace research)



Named a Customers' Choice in the 2025 Gartner® Peer Insights™ Voice of the Customer for Email Security, Darktrace / EMAIL brings industry-first AI innovation to the entire messaging ecosystem to stop novel and targeted attacks.

[Gartner Peer Insights](#): ★★★★★ 4.8* (323 ratings as of August 2025)



55% of threats detected by Darktrace / EMAIL passed through all existing security layers

(Annual Threat Report 2024)

13 Darktrace / EMAIL detects threats **13 days earlier than other solutions**

(Darktrace research)

A unique AI approach at its core

What makes Darktrace's network and email products **so powerful**?

The AI that underpins them.

Most cybersecurity vendors still rely on outdated detections based on rules and signatures. Even when AI is used, it's typically limited to supervised models trained on labelled attack data and threat intelligence. While effective at identifying known threats, these models require constant retraining and still struggle with novel or AI-driven attacks that don't match historical patterns. This results in unverifiable anomalies and a flood of low-confidence alerts, overwhelming security teams, contributing to alert fatigue, and resulting in heavy-handed or low-accuracy responses.

Darktrace's Self-Learning AI takes a fundamentally different approach to cybersecurity by **continuously learning** the unique digital environment of each organization. Using a multi-layered AI approach, it strategically integrates a range of AI techniques – including unsupervised machine learning, LLMs, GNNs, and NLP – both sequentially and hierarchically.

This enables it to **adapt to evolving threats** and build a dynamic understanding of normal behavior across users, devices, and systems. By combining these AI models, our Self-Learning AI can distinguish truly malicious activity from unfamiliar but benign events – without relying on signatures, rules, or manual tuning.

Our Self-Learning AI is the foundation of Darktrace's ActiveAI Security Platform, which correlates telemetry across domains for complete end-to-end coverage, including email and network. **This allows Darktrace to connect insights across environments, creating a unified view of risk.**

Behavioral signals from one area – such as a suspicious login detected on the network – can immediately inform decision-making in email, and vice versa. This tight integration enables faster threat detection, enriched and contextualized alerts, and smarter autonomous actions, without requiring human intervention or complex rule-based integrations.

With holistic AI-powered defense across network and email, you'll benefit from unified protection greater than the sum of its parts. It provides seamless, adaptive protection that mirrors how real-world attacks unfold, giving defenders a consistent, unified advantage.

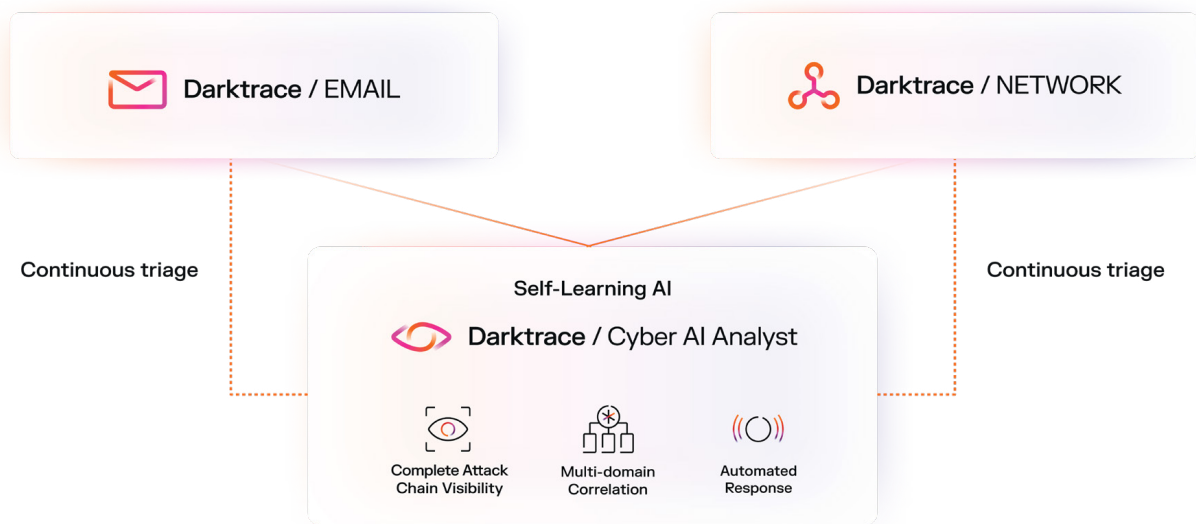


Figure 02: Together, Darktrace / NETWORK and / EMAIL combine proactive resilience and unified threat visibility and detection, helping you shift to an AI-led SOC

Your investigative companion: Cyber AI Analyst

If Self-Learning AI powers cross-domain threat detection and response, Cyber AI Analyst is your SOC's **tireless digital detective**.

It's an agentic AI system that autonomously investigates all relevant security alerts – from Darktrace as well as those from third party security tools (firewalls, EDR, SIEMs). Not just a Gen AI chatbot. Cyber AI Analyst uses multiple types of AI to mirror the human investigation process, including machine learning, models trained on expert analyst behavior, security-specific custom LLMs, and NLP.

It performs investigation and analysis equivalent to SOC Levels 1 & 2:

- forming and refining hypotheses
- querying and correlating information
- tracking complex attacks across multiple domains
- surfacing critical incidents for human review
- suggesting response actions based on pattern-of-life analysis

It typically reaches a conclusion within minutes and presents a clear, interactive incident summary – complete with linked alerts, contextual analysis, and graph-based interactive visualizations – making it easy to explore and understand even the most complex attacks.

By handling investigations and triage at a Level 2 SOC standard, Cyber AI Analyst frees up human analysts to focus on proactive threat hunting and deeper investigations.



x 10 acceleration in investigations provided by Cyber AI Analyst



Gain up to 50k analyst hours annually



The equivalent of adding up to 30 full time SOC analysts

■ Case study

In one month, Cyber AI Analyst saved one customer **1,104 hours of manual investigation** by automating the triage and investigation of 23 million alerts

(Customer case study, Aviso)

Benefits of a common approach

Bringing together network and email security delivers a range of quantitative and qualitative benefits to any organization, which can be broadly categorized into technical, operational and commercial advantages. **Let's take a look.**

Technical edge

On a technical level, the benefits can be divided into pre-alert intelligence and alert-related intelligence.

Pre-alert intelligence: Gathering data before the threat strikes

Many security tools only begin analysis once clear signs of compromise are present. Unlike other tools, our AI continuously ingests and analyzes data across both email and network – even in the absence of alerts. This ongoing analysis builds a rich behavioral understanding of every user, device, and domain interacting within the organization.

This means that by the time an email lands in a user's inbox, Darktrace already has context for the sender's domain based on its network visibility. Likewise, if a suspicious domain surfaces in an email, this information immediately informs how future network activity is interpreted. This shared understanding extends across the Darktrace ecosystem – whether the intelligence originates from email, network, endpoint, or external sources like threat intel feeds, it only needs to be ingested once. From there, it enriches detection and response across all products, ensuring consistent, context-aware decisions.

The result is a dynamic intelligence gathering and sharing process which builds knowledge within the tool – not of threats but of real-time behavioral baselines, which allows Darktrace to flag threats without requiring a compromise to occur.

Alert-related intelligence: Connecting the dots in real time

When a security alert is triggered, Cyber AI Analyst immediately begins investigating by forming hypotheses and analyzing real-time and historical data across domains. It autonomously connects related behaviors, such as linking a suspicious email to unusual network activity on the recipient's device, creating a single comprehensive incident for the SOC to review.

This process happens in minutes and at scale, dramatically reducing alert volume and manual triage.

Furthermore, this automatic correlation ensures that attack chains remain intact, offering continuous visibility from initial compromise to lateral movement or data exfiltration. This shared visibility informs the most targeted response, commensurate to the scale and scope of the attack.

Unlike point solutions or SIEM workflows, which often leave analysts to manually piece together fragmented alerts without full context, Darktrace provides unified, post-alert intelligence that's agnostic to where the threat first appeared.

Our approach not only speeds up investigations and improves the confidence behind response decisions, but supports a core tenet of Darktrace's security philosophy: defenders should never lose sight of the attacker after their initial entry point.



Though email may be the entry point,

the next move from attackers will typically target network infrastructure or cloud accounts, making it continuous, cross-environment correlation between email and network essential.

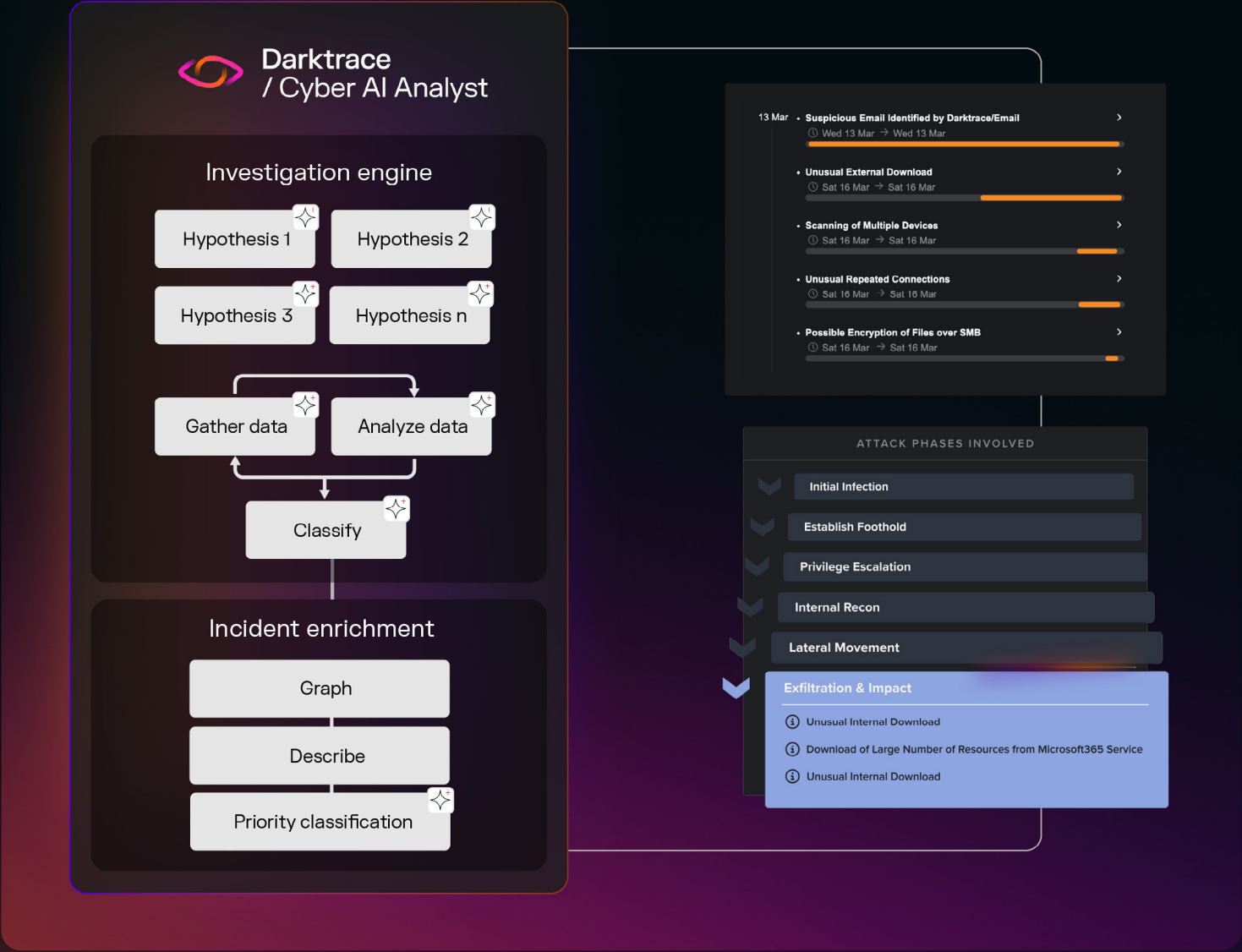


Figure 03: Stages of an attack originating in email and spreading to the network, with disparate stages of the attack chain correlated in Cyber AI Analyst

“Darktrace’s ability to distill vast amounts of data effectively eliminates the noise, allowing the team to focus on genuine risks without being overwhelmed by irrelevant information.”

■ CISO, Local government

Operational advantage

Streamlining SecOps across teams

In many organizations, email security and incident response are still managed by separate teams. Email often falls under IT operations, while network defense and incident response sit within the SOC. This separation creates operational friction, especially as email remains the most common entry point for cyber-attacks.

By deploying network and email security together – within a single platform and threat visualizer – critical email insights aren't confined to a separate console or team but are accessible directly within the SOC's core workflows.

This shared visibility gives the incident response team greater insight into email attack vectors without needing to escalate or outsource the request, and lays the path for greater collaboration between different areas of the security team.

Reducing time-to-meaning and enabling faster response

With network and email data unified in a single platform, security teams no longer need to jump between tools to correlate disparate alerts. As well as being manually seamless, the shared philosophy operating across network and email reduces time-to-meaning for users.

Equally, built-in threat correlation between email and network via the Cyber AI Analyst enables faster triage and more confident, coordinated responses across environments. Unlike traditional workflows that rely on SIEM correlation or SOAR playbooks, Darktrace connects the dots in real time and automates intelligent response actions.

Commercial value

Deploying network and email security together isn't just a technical and operational win, it also has commercial benefits.

With one vendor, organizations benefit from a single relationship, simplifying everything from procurement and negotiation to ongoing support. Instead of managing multiple contracts, customers gain one unified account team and a streamlined commercial process. The process of wrapping additional managed or professional services around both products is also simplified – giving you the ability to gain consistent expertise across the entire security environment.

Crucially, investing in a single AI-powered platform lays a strong foundation for future expansion.

With email and network under the same umbrella, adding new capabilities in the future – such as identity or cloud coverage – doesn't require rethinking your architecture, because the platform is designed to scale with your business.

While point solutions may appear flexible at the outset, they often lead to fragmented coverage, duplicative spending, and integration headaches. For organizations aiming to build a modern, AI-enabled SOC, buying best-of-suite, not best-of-breed, is not just simpler, but more strategic. **And with Darktrace, there is no sacrifice in quality while moving to a platform approach – every individual purchase strengthens the core platform, enhances shared intelligence, and delivers more value over time.**

Darktrace showed integrity, patience and a genuine investment in building a strong relationship with my team. That's why we're here today.

■ CISO, Global Technology Provider

Buying scenarios

Let's look at two buying scenarios, one for an organization implementing a point solutions strategy, one for an organization looking for a consolidated security stack.

Scenario 1: Point Solutions



Initial setup

An organization selects a standalone email security tool – perhaps chosen by the IT or messaging team – and later deploys a separate network detection and response (NDR) product via the security team. Or they might have no NDR tool at all, relying instead on an EDR or XDR. To connect insights, they lean on an existing SIEM or SOAR platform to correlate data and orchestrate response workflows.



Operational phase

While this approach offers flexibility and leverages existing tooling, it introduces complexity. The SOC must manage multiple dashboards and alerting systems. Investigation processes can be slower, as analysts manually connect events across different tools, each with its own data model and detection logic.



Scaling up

Expanding coverage into cloud, identity, or application layers involves sourcing additional point products, integrating them with the SIEM, and tuning rules or playbooks accordingly.

Over time, the burden on engineering and operations grows – with duplicated effort across tools, fragmented visibility, and inconsistent response coordination.

Scenario 2: Platform Security



Initial setup

An organization adopts email and network detection from the same vendor, delivered through a shared AI-powered platform and a single operational interface. Both surfaces feed into the same behavioral model, with intelligence and visibility seamlessly shared across the environment.



Operational phase

Security teams benefit from pre-integrated workflows, consistent alerting, and native incident correlation. When an email-based attack leads to suspicious internal activity, both are surfaced in a unified view – reducing investigation time and eliminating the need to manually bridge gaps between tools or teams. Optional services, such as MDR, can operate across both surfaces without duplication.



Scaling up

As the threat landscape evolves, expanding to other areas – such as cloud accounts, user identities, or endpoints – can be done incrementally without re-architecting the stack. Additional capabilities integrate into the same model, preserving context and enabling cohesive protection across the digital estate.

Take the next step

As attackers increasingly use AI to research, automate, and accelerate, defenders cannot afford to rely on superficially integrated tools or manual processes. Unifying network and email security isn't just about efficiency, it's about creating a security ecosystem that's bigger than the sum of its parts.

We've built the Darktrace ActiveAI Security Platform to deliver proactive, correlative security that thinks like an attacker – giving you the visibility and agility to defend against the targeted, multi-domain threats that evade siloed detection efforts.

Ready to take the next step?

Request a **tailored demo** to see unified protection in action

Get a demo



See how this customer **reduced MTTC by 80%** with Darktrace

Case study



Calculate **your ROI** with Darktrace / EMAIL

Get your ROI



■ 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.