DARKTRACE

How Does Multi-Layered AI Work in Darktrace / EMAIL?

From data to decision — real AI, built for real email threats

Why multi-layered AI for email matters

Email is still the #1 attack vector – but attackers don't follow rules or signatures anymore.

Most email security tools:

- Bolt AI onto legacy SEGs
- Rely on static rules, past attacks, or single models
- Miss subtle, socially engineered threats like BEC and insider risk

Darktrace / EMAIL is different. It uses multi-layered AI that understands behavior, context, and intent — learning how your organization normally communicates, then spotting what doesn't belong.

Get the full guide to Darktrace AI

A full breakdown of how multi-layered AI powers threat detection and response across email, messaging, and account activity

The Darktrace / EMAIL AI Lifecycle

Let's break down how our multi-layered AI processes every incoming email, step by step.

01 DATA GATHERING

Emails and collaboration data (e.g. Teams, Slack, Zoom) are ingested and parsed in real time. Key attributes like headers, content, routing, and authentication signals are extracted to form the raw dataset for analysis.

02 SOCIAL GRAPHING

AI maps how users communicate across the organization. It builds dynamic peer groups based on real behavioural relationships, not static roles or assumptions – including identifying external facing mailboxes and VIP mailboxes (that will have different risk profiles).

03 METRIC CALCULATION

Thousands of behavioural and structural metrics are generated per email. These include signals like tone, exposure, spoof likelihood, PII presence, and shifts in user behavior.

04 EVALUATION MODELS & ACTIONS

Metrics are combined through decision models that assess intent and risk. This is where behavioral patterns are evaluated against users' normal activity for anomalies. Based on model outputs, the system takes actions such as holding emails, rewriting links, or adding warnings.

AI LAYERS ALGORITHMIC LAYERS (NON-AI)

The result:
An AI system built to understand your org

- Social graphing
- NLP
- Bayesian probability
- Meta-modelling
- Computer vision
- Autonomous response

All working together to:

- **Stop** BEC, phishing, insider threat, and data loss
- **Reduce** SOC workload
- **Protect** users without slowing the business

Why Darktrace?

AI-first since 2013 – not retrofitted

Trained on your organization, not yesterday's attacks

Recognized as a Leader in the 2025 Gartner® Magic Quadrant™ for Email Security Platforms

200+ registered patents

Responsible-AI certified by ISO 42001

05 META-MODELLING AND ACTIONS

A higher-level AI layer evaluates overall anomaly and risk. Each email is given an anomaly score, promoting visibility, transparency, and reducing alert fatigue in the SOC.

06 CAMPAIGN CLUSTERING

Adversaries are always changing their methods. Darktrace's campaign AI is able to cluster emails based on patterns traditional systems can't, allowing us to identify novel campaigns.

07 CYBER AI ANALYST

AI analysis investigates incidents autonomously, connecting email activity with broader security context in the business. It builds narratives that help SOC teams understand what's happening and why.

08 DATA PRESENTATION

Findings are surfaced to security teams through clear, actionable insights. These outputs also feed back into the system, continuously improving detection accuracy.