

THE DARKTRACE BEHAVIORAL DEFENSE PLATFORM

Secure AI, people, and infrastructure with unified visibility,
continuous behavioral monitoring, and autonomous response.

8 days

Before public disclosure

Average detection and
containment of novel threats.

10 times

Faster incident response

Enabled by Real-Time AI Analyst.

30 Analysts

Focus on what matters most

Provides the capacity of up to 30 additional
full-time analysts for level 2 investigation &
reporting annually

Security must adapt as fast as the enterprise

AI has moved from assistant to actor, changing how organizations operate, communicate, make decisions, and create value. At the same time, it's expanding the attack surface, introducing new systems, agents, identities, data flows, and autonomous actions. While businesses are becoming more connected, security tools still operate in silos. As a result, security teams switch between dashboards and spend hours manually connecting and investigating alerts without the business context needed to understand what matters.

Attacks now move laterally at machine speed across AI tools, email, and hybrid networks. To strengthen their defenses, security teams need a consolidated platform that understands their environment, connects activity across domains, surfaces threats with context, and automates investigation and response.

Accelerate innovation securely with Darktrace

**The Darktrace Behavioral Defense Platform
starts with the enterprise, not the attack.**

Powered by Adaptive AI, Darktrace continuously learns the behaviors, relationships, dependencies, and operational patterns unique to your organization. It uses this continuously updated behavioral model to detect anomalous activity, correlate signals across AI, people, and infrastructure, and autonomously contain threats before they disrupt operations.

As your environment changes, through new users, AI agents, applications, workloads, and operational assets, Darktrace adapts with it. This enables the platform to identify novel risk without waiting for a new rule, signature, or public disclosure.

Business benefits

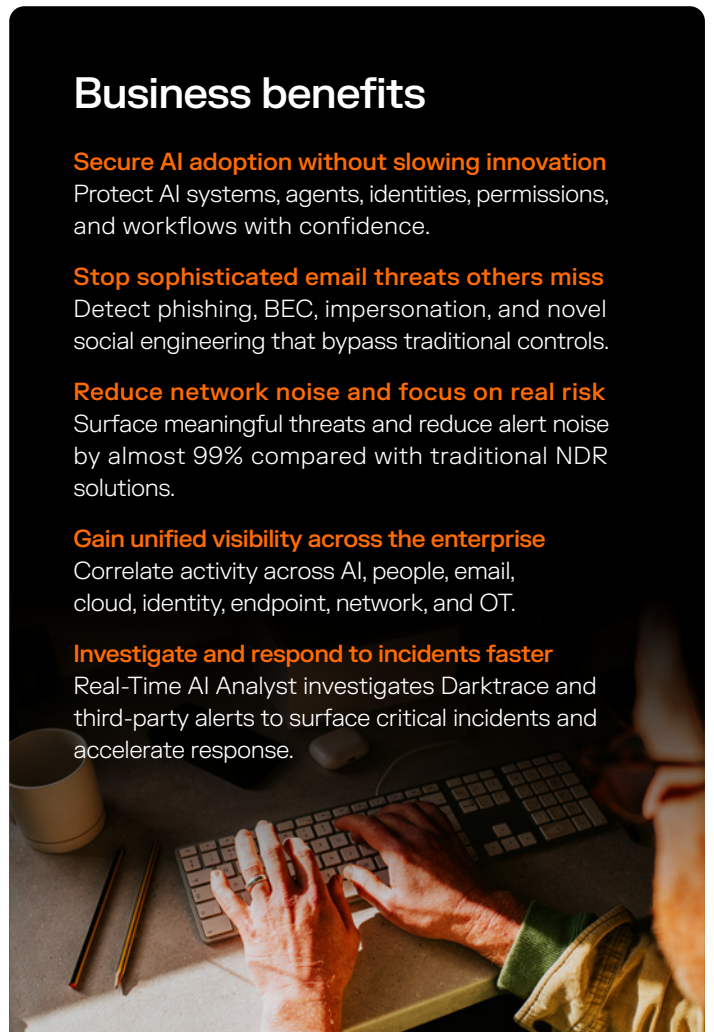
Secure AI adoption without slowing innovation
Protect AI systems, agents, identities, permissions, and workflows with confidence.

Stop sophisticated email threats others miss
Detect phishing, BEC, impersonation, and novel social engineering that bypass traditional controls.

Reduce network noise and focus on real risk
Surface meaningful threats and reduce alert noise by almost 99% compared with traditional NDR solutions.

Gain unified visibility across the enterprise
Correlate activity across AI, people, email, cloud, identity, endpoint, network, and OT.

Investigate and respond to incidents faster
Real-Time AI Analyst investigates Darktrace and third-party alerts to surface critical incidents and accelerate response.



Key differentiators

UNIQUE BEHAVIORAL PROFILE

Our intelligence layer

Darktrace builds an evolving representation of how your organization behaves, connects, and operates across AI, people, and infrastructure.

- Adaptive AI **continuously learns** the normal behavior of users, identities, AI systems, applications, devices, workloads, and operational technology.
- Identifies** subtle, novel, and fast-evolving threats that static rules, signatures, and generalized models can miss.

360° INSIGHTS

Our visibility layer

Darktrace brings together behavioral context from across the digital estate to provide a correlated, real-time understanding of risk.

- Connects** activity across AI, email, collaboration, SaaS, identity, endpoint, cloud, network, and OT.
- Reveals attacks that cross environments as one connected incident, not a collection of isolated alerts.

REAL-TIME AI ANALYST

Our autonomous layer

Darktrace applies its behavioral understanding to detect, investigate, prioritize, and respond to meaningful deviations as they happen.

- Automatically **gathers** evidence, **correlates** related activity, and **produces** a clear incident narrative.
- Supports** precise, autonomous responses to contain threats while allowing normal business operations to continue.



Together, these layers enable Darktrace to detect threats before they are defined, understand attacks across environments, and **respond at AI speed**.

DARKTRACE

Real-Time AI Analyst

360° Insights

AI

We secure deployment, management, and development across all your AI systems and agents.

People

We secure phishing, account takeover, data exfiltration, and human risk across email and every collaboration tool.

Infrastructure

We secure visibility, detection, and response across your network, cloud, and OT environments.

Unique Behavioral Profile

Adaptive AI

Our proprietary AI technology

Frontier AI, MCP, & SaaS Data



Email and Collaboration Data



Network, Endpoint, Cloud, and Identity Data



The Darktrace Behavioral Defense Platform

One platform protecting AI, people, and infrastructure

AI

DARKTRACE / SECURE AI

People

DARKTRACE / EMAIL

Infrastructure

DARKTRACE / HYBRID NETWORK

Protect the deployment, management, and development of enterprise AI systems and agents. Gain visibility into AI usage, prompts, data access, agent identities, permissions, tools, and downstream actions. Identify shadow AI, prompt manipulation, excessive privilege, abnormal data movement, and development risks across the AI lifecycle.	Protect the human layer across email and collaboration, where trust, identity, and intent are routinely exploited. Darktrace learns how each person communicates and collaborates to detect phishing, business email compromise, impersonation, account takeover, data exfiltration, and novel social engineering, even when an email appears technically legitimate.	Protect the systems that run the business across network, cloud, endpoint, identity, and OT. Darktrace learns how users, devices, workloads, applications, and operational systems interact to detect lateral movement, credential misuse, privilege escalation, ransomware, command-and-control activity, insider risk, and novel exploitation.
--	---	--

KEY USE CASES

AI prompt analysis and shadow AI management	Phishing, BEC, and impersonation defense	Known, unknown, and insider threat detection
AI agent identity, access, and action tracing	Account takeover and compromised identity detection	Lateral movement and cross-environment correlation
AI development and infrastructure risk management	Data loss and abnormal collaboration behavior	Precise autonomous containment across hybrid environments



The three solution areas share the same Adaptive AI, behavioral understanding, visibility, and autonomous capabilities. **Organizations gain one connected security platform, not another set of isolated products.**

Deploy anywhere. Connect to everything.

Deploy Darktrace across cloud, on-premises, and hybrid environments, with integrations across AI platforms, email and collaboration, cloud, identity, endpoint, SIEM, SOAR, ticketing systems, firewalls, and other enforcement technologies.

Organizations can start with the solution area that addresses their immediate priorities—AI, people, or infrastructure and choose from three progressive packaging tiers. Core provides the foundational package, Advanced builds on Core with additional capabilities, and Complete offers the fullest level of platform capability. **This gives customers a clear path to expand their Darktrace deployment as their environment and security needs evolve.**

