

Securing the AI Era with Behavioral Security

Award-winning partnership. Complementary technologies.

Microsoft helps organizations create, deploy and scale AI. Darktrace helps you operate AI securely.

As AI moves from assisting employees to taking action across identities, data, applications and infrastructure, security teams need to understand more than what is permitted. They need to know whether users, AI systems and agents are behaving as expected once they are operating inside the business.

Microsoft establishes the identity, governance, data protection, and security controls that define what users and AI are allowed to do. Darktrace adds behavioral context across AI, people and infrastructure, helping teams identify when activity no longer aligns with normal business behavior or intended purpose and responds before risk escalates.

How Darktrace extends Microsoft security



Strengthen existing Microsoft investments

Add behavioral context and autonomous response to complement Microsoft identity, governance, compliance and native security controls.



Understand activity with business context

Go beyond permissions and policy to understand how users, AI agents, applications and infrastructure actually behave.



Secure AI as adoption scales

Extend behavioral security across Microsoft 365 Copilot, Microsoft Agent 365 and broader enterprise AI as customers move from E5 to E7.



Investigate and respond faster across domains

Bring together activity across AI, email, identity, cloud, network, endpoint and OT, so attacks are understood as one incident, not isolated alerts.

Darktrace + Microsoft across AI, people & infrastructure

Microsoft provides the platforms and security controls, while Darktrace brings real-time behavioral context across your Microsoft environment. The tables below show how Darktrace complements Microsoft's capabilities across each domain.

/ SECURE AI + Microsoft

Secure AI adoption from use to runtime

Darktrace / SECURE AI extends Microsoft's AI, identity and governance capabilities with visibility into how AI is actually being used from prompts and users to agents, development activity and Shadow AI.

Microsoft Provides

Darktrace Adds

Microsoft 365 Copilot - Enterprise AI experiences across Microsoft 365.

Monitors supported prompts, sessions and responses to identify sensitive data exposure, jailbreak attempts and unexpected AI behavior.

Microsoft Copilot Studio - Tools to build, configure and deploy AI agents.

Connects agent development and configuration with runtime behavior to reveal misconfigurations, anomalous activity and drift from intended purpose.

Microsoft Entra + Agent 365 - Identity, permissions, lifecycle and governance for users and agents.

Provides visibility into agent identities, permissions and actions to identify excessive access, unexpected connections and risky behavior.

Microsoft Entra Global Secure Access - Secure access controls across users, devices and web activity.

Extends Shadow AI discovery through supported secure-web-gateway activity to uncover unsanctioned AI services and usage.

Microsoft Foundry + Defender for Cloud + Purview - AI development, security posture, governance and data-protection capabilities.

Identifies risky development activity, misconfigurations and over-entitlement while connecting build-time insights with runtime AI activity.

"Darktrace / SECURE AI has given us a clearer view of AI activity across the organization, including the tools employees are using and the types of data appearing in prompts."¹

■ Matthew Davis

Chief Information Security Officer,
ESL Federal Credit Union

¹darktrace.com/news/darktrace-extends-behavioral-security-with-general-availability-of-darktrace-secure-ai

Powered by Adaptive AI

Adaptive AI is Darktrace's proprietary AI technology, evolved over more than a decade to learn how each organization operates and apply the right AI technique to each security challenge.

Unique Behavioral Profile

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

360° Insights

A continuously evolving, correlated view of insights and threats across the digital estate.

Real-Time AI Analyst

Uses real-time behavioral understanding to detect, triage, investigate and respond at machine speed.

/ EMAIL + Microsoft

Protect communication in the context of how people actually work

Darktrace / EMAIL complements Microsoft's email, collaboration and data-protection capabilities by understanding communication in the context of how each business actually operates.

Microsoft Provides	Darktrace Adds
Defender for Office 365 - Native email and collaboration protection.	Behavioral context to help identify and detect sophisticated and novel attacks, with unified quarantine workflows that can streamline investigation and remediation.
Microsoft Teams - Enterprise communication and collaboration.	Detects social engineering and suspicious activity across supported Teams conversations.
Microsoft Purview - Data protection, governance and compliance controls.	Combines behavior, content and sensitivity labels to prevent email data loss.
Microsoft Security Copilot - AI-assisted security investigation and operational workflows.	Darktrace investigation findings and email-security context in the workflows security teams already use.

/ HYBRID NETWORK + Microsoft

Understand threats across the infrastructure AI and the business depend on

Darktrace / HYBRID NETWORK extends Microsoft security across the wider hybrid environment, using behavioral context to identify threats as they move across network, cloud, identity, endpoint and OT.

Microsoft Provides	Darktrace Adds
Microsoft Defender for Endpoint - Endpoint detection and protection.	Connects endpoint activity with network and infrastructure behavior to uncover threats that extend beyond individual devices.
Microsoft Sentinel - Security analytics, incident management and security operations workflows.	Brings Darktrace incidents and AI-driven investigation findings into Sentinel workflows, helping analysts prioritize threats and accelerate response.
Microsoft Azure - Cloud infrastructure and services.	Behavioral detection and response across Azure workloads and the wider hybrid estate.
Microsoft 365 + hybrid environments - Productivity, identity and enterprise services.	Cross-domain context across identity, network, cloud, endpoint and OT, so attacks can be understood as one evolving incident.

Better together for security teams

Less time stitching together alerts. More time acting on what matters.

Darktrace Real-Time AI Analyst uses the organization's behavioral understanding to detect, investigate, and prioritize emerging threats across the platform. In established Microsoft integrations, Darktrace's existing Cyber AI Analyst investigation capability can enrich Microsoft Sentinel and Security Copilot workflows, bringing Darktrace context into the tools analysts already use.

"Darktrace and Microsoft offer complementary approaches, giving our security team peace of mind. We know that if something slips through the net on one side, it will be picked up on the other."²

■ Mark Kane ,
Global Head of Information Solutions,
Mainstream Renewable Power

2: darktrace.com/ja/customers/mainstream-renewable-power