Cyber AI Security for Microsoft Azure

Powered by self-learning Cyber AI, Darktrace brings real-time visibility and autonomous defense to your Azure cloud.

Key Benefits

- ✔ Learns 'on the job' to offer continuous, context-based defense
- ✔ Offers complete real-time visibility of your organization's Azure environment
- ✔ Autonomously neutralizes novel and advanced threats
- ✔ Cyber AI Analyst automates threat investigation, reducing time to triage by up to 92%

"Darktrace complements Microsoft's security products with AI and takes us to another level."

Global Head of Information Solutions, Mainstream Renewable Power

Cyber AI Defense for Dynamic Workforces and Workloads

The Darktrace Immune System provides a unified, AI-native platform for autonomous threat detection, investigation, and response in Azure and across the enterprise, ensuring your dynamic workforce is always protected.

With advanced Cyber AI, Darktrace builds a deep understanding of normal behavior in your Azure cloud environment to identify even the most subtle deviations from usual activity that point to a threat – no matter how sophisticated or novel.

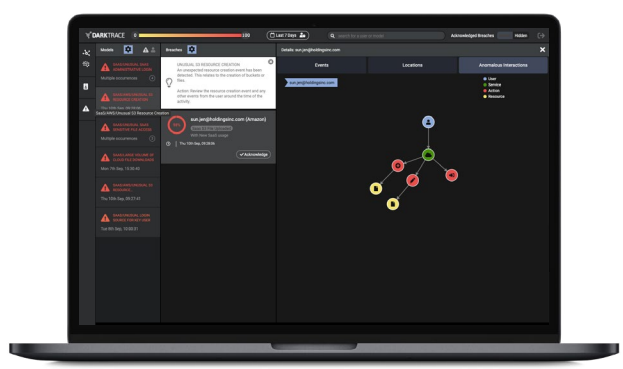


Figure 1: Darktrace's dedicated interface for cloud-based threats

Protecting Azure Cloud From Novel and Advanced Threats

Data Exfiltration and Destruction

- Detects anomalous device connections and user access, as well as unusual resource deletion, modification, and movement.

Critical Misconfigurations

- Identifies unusual permission changes and anomalous activity around compliance-related data and devices.

Compromised credentials

- Spots brute-force attempts, unusual login source or time, and unusual user behavior including rule changes and password resets.

Insider Threat and Admin Abuse

- Identifies the subtle signs of malicious insiders, including sensitive file access, resource modification, role changes, and adding/deleting users.

An AI-Native Solution for Azure Cloud Security

The Darktrace Immune System continuously monitors all Azure cloud traffic via Darktrace osSensors: lightweight, host-based server agents that allow Darktrace's Cyber AI to build rich behavioral models for workforce and workload activity.

Each osSensor feeds traffic to a local Darktrace vSensor, which then feeds the relevant metadata to a Darktrace master probe in the cloud or corporate network for analysis.

Darktrace's Security Module for Azure provides additional visibility, allowing for Cyber AI-powered monitoring of management activity, user access, and resource creation. Monitoring is achieved via HTTPS requests made with an authenticated token to the Microsoft Graph API.

With its bespoke, continuously evolving knowledge of how your business operates in the cloud, Darktrace's Cyber AI can put behavior in context and spot deviations from normal activity that point to an emerging threat.

This comprehensive view allows the Darktrace Immune System to deliver defense across all your Azure services, including:

- Azure DevOps
- Virtual Machines
- CosmosDB
- Azure Active Directory
- Azure Function
- Azure SQL
- Blob Storage
- Queue Storage
- File Storage
- Table Storage

> "Darktrace AI adapts while on the job, illuminating cloud infrastructure in real time and allowing us to defend the cloud with confidence."
>
> **Jason Barr, CISO, Aptean**

Figure 2: The Darktrace Immune System ensures your dynamic workforce is always protected.

Autonomous Defense: Darktrace Immune System

Detect

- With self-learning AI, the Darktrace Immune System can detect the sophisticated and novel threats that policy-based controls simply can't.

Respond

- Darktrace Antigena is the world's first Autonomous Response technology that can interrupt attacks on your behalf, at machine speed and with surgical precision.

Investigate

- Combining human security expertise with AI for the first time, Darktrace's Cyber AI Analyst automatically investigates every threat and reports on the full scope of incidents – reducing triage time by up to 92%.

Unified, Self-Learning Security Across the Enterprise

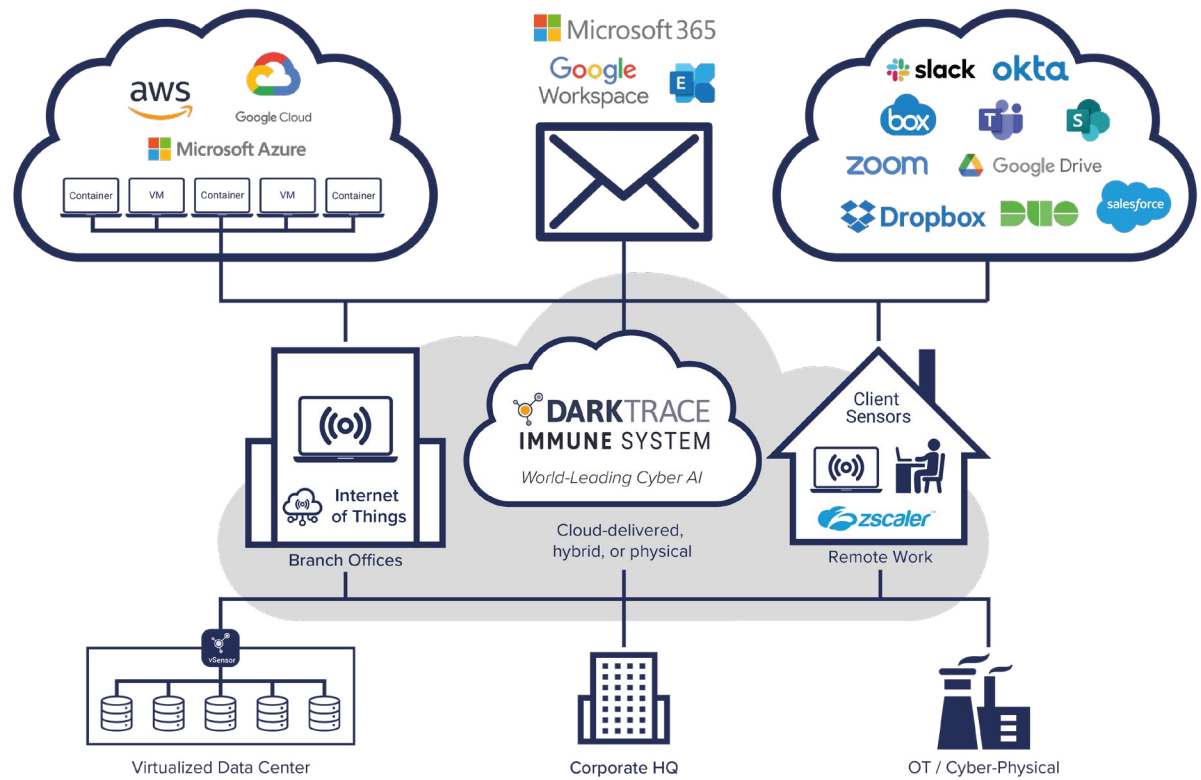
The Darktrace Immune System provides the industry's only self-learning platform that correlates information from across the organization and adapts in real time – improving productivity across the security team and letting you accelerate digital transformation and innovation.

Taking a fundamentally unique approach, the Darktrace Immune System can correlate behavior in Azure with activity across SaaS, email, remote endpoints, and any range of on- and off-premise infrastructure.

For customers who use Microsoft 365 workspace collaboration tools, Darktrace's Microsoft SaaS Module adds visibility and protection across Outlook, Microsoft Teams, SharePoint, and OneDrive, identifying account takeovers and misuse. With a dedicated SaaS console, Darktrace offers unprecedented visibility of workforce activity across these applications.

Moreover, Antigena Email constantly adapts and analyzes Microsoft 365 email communications in the context of 'normal' for the sender, recipient, and wider organization. This allows it to identify and respond to the full range of email attacks, from fraudulent payment requests to sophisticated spear phishing.

This is of critical benefit, as businesses and workforces today are increasingly complex and dynamic. With Darktrace's pervasive approach, Cyber AI can connect the dots between unusual behavior in disparate infrastructure areas and ensure cloud security is not siloed from the protection of the organization.

For More Information

- Book a free trial
- Read our Cloud Security White Paper
- Visit our YouTube channel