

# Secure your Cloud with Self-Learning AI

DARKTRACE

## / Dynamic infrastructure requires constantly adaptive learning

As organizations increasingly rely on the cloud to streamline operations and enable innovation, the challenge of securing critical data has taken on a new dimension. Developers can bypass the IT/security team and spin up instances with ease.

Although securing the cloud is often unfamiliar territory for traditional security teams, the shared responsibility model places the burden on their shoulders. Successful teams need technology which can handle the complexity of the cloud, and create meaningful outputs for the rest of the security ecosystem.

## / Darktrace learns every interaction in your cloud environment to ask:

### Is this normal?

Rather than aggregating historical attack data and collecting them in a centralized database, Darktrace's Self-Learning AI learns from your unique digital environment, understanding what's 'normal' and spotting the subtle deviations indicative of a cyber-threat.

### Combines network and service layer events

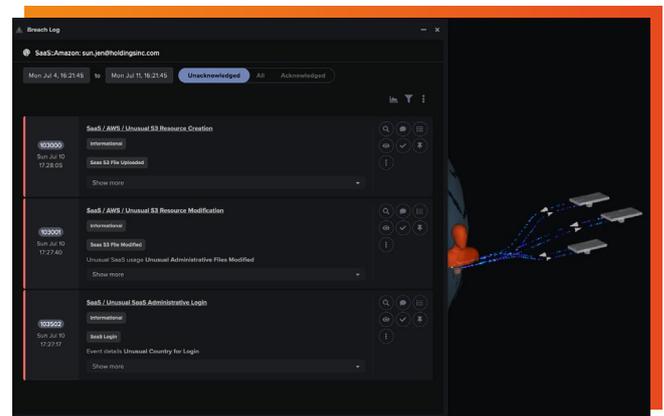
Analyzes network data in the cloud alongside control plane events, providing visibility and protection across every layer of the cloud.

### Responds autonomously

Uses its understanding of 'self' to take targeted, proportionate action to disarm cyber-attacks, neutralizing the threat without disrupting normal business.

### Reveals the full scope of the threat

Cyber AI Analyst applies an additional layer of AI to individual anomalies, connecting events to surface and prioritize wider security incidents.



### Challenge

Suspicious data flow in Kubernetes cluster?

VM instance to rare domain?

Suspicious connectivity?

Unusual resource creation?

### Darktrace/Cloud Solution

Contain it

Block the specific connections

Enforce normal behavior

Alert the security team

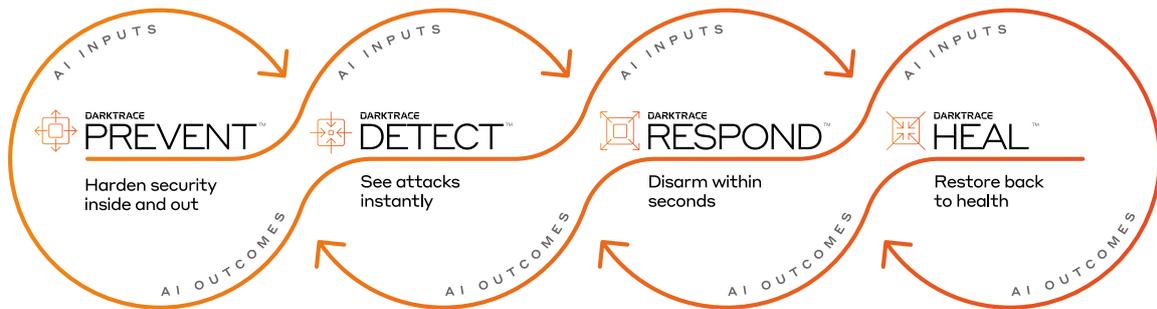
### Coverage:



And more

### Cyber AI Loop™

Darktrace is delivering the first ever always-on feedback system that creates a virtuous cycle in which each capability strengthens and hardens the entire security ecosystem.



Darktrace/Apps fits into the DETECT and RESPOND components of this ecosystem, sharing its insights with the rest of the security stack - and human teams through explainable AI.

### / Multi-platform coverage

Increasingly, threat actors are not limiting their attacks to one technology at a time. It no longer makes sense then, to handle security on a per-technology basis. Covering IaaS, PaaS, and SaaS with a single solution is crucial to regain control over single and multi-cloud infrastructure. Darktrace/Cloud investigates cloud data and activity with data from across the digital estate, enriching it's understanding with context from Darktrace/Network™, Darktrace/Email™, and Darktrace/Endpoint™.

### / Explainable AI augments your security team

The use of AI is crucial to handling the scale and complexity of real-world cloud environments without placing huge burdens onto humans. The Cyber AI Analyst keeps the human in the loop by connecting the dots between singular events to reveal the broader security incident and reducing time to meaning by 92% with automated as well as on-demand AI investigations.

#### Organizations using Darktrace to protect their cloud infrastructure

