

## Secure Your Cloud in Real Time

Business leaders continue to embrace the cloud to improve efficiency and flexibility. While the cloud enables scalable, highly-available, and fast-moving environments for businesses, cyber threat actors are presented new avenues for exploitation.

Security teams struggle to obtain real-time visibility, keep up with evolving threats, and handle the complexity that the cloud brings. **Darktrace Cloud Security uses Self-Learning AI to provide complete cyber resilience for multi-cloud environments.**



## Comprehensive Cloud Security

### Architectural Awareness

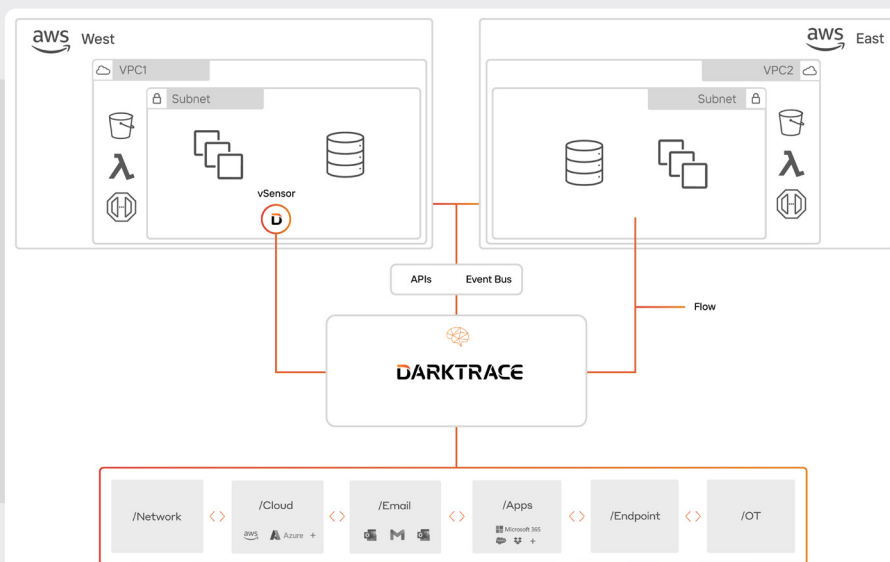
Gives users an understanding of their cloud footprint, including real-time visibility into cloud assets, architectures, users and permissions. Combines asset enumeration, modeled architectures, and flow log analysis. Cost insights give a better understanding of resource allocation, helping teams contextualize resources.

### Cloud-Native Detection & Response

AI understands 'normal' for your unique business and stops cyber-threats with autonomous response. Near-real-time response goes beyond simple email alerts or opening a ticket; and includes cloud-native actions like detaching EC2 instances and applying security groups to contain risky assets.

### Cloud Protection & Compliance

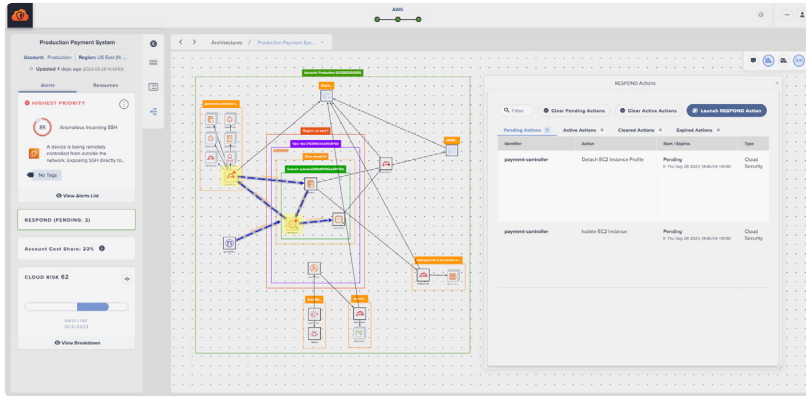
Identify compliance issues and potential misconfigurations, with attack path modeling and prioritized remediation steps. Darktrace's attack surface management (ASM) adds critical external view of your organization, highlighting vulnerabilities most impactful to your specific organization, and revealing shadow IT.



## Quick and Easy Install with Granularity Where You Need It

- Deploys from the cloud in minutes
- Data drawn either from lightweight host-based server agents or a combination of traffic mirroring and API logs
- Supports multi-tenant, hybrid, and serverless environments

Complete architectural visibility through an agentless deployment may reveal areas you want to deploy Darktrace agents for deeper analysis.



Darktrace models cloud architectures and highlights relevant risks

Gain an immediate understanding of your cloud footprint, including **real-time visibility** into cloud assets and architectures, as well as users and permissions.

Identify **misconfigurations, vulnerabilities & compliance issues** and prioritize your actions based on true cloud risk.

Identify critical avenues of attack with **attack surface management** and attack path modeling.

**Cost insights** give you a better understanding of resource allocation, helping teams contextualize resources.

## Self-Learning AI, Trained on Your Business Data

Core to Darktrace/Cloud is Self-Learning AI technology that learns from your unique business data to identify risks and real-time threats. Rather than learning from attack data across thousands of organizations, Darktrace leverages a dynamic understanding of your unique cloud footprint, **at the network, architectural, and management layer.**

This deep cloud behavioral monitoring enables real-time detection of threats across workloads and containerized environments such as Kubernetes. When a cyber-threat is detected, Darktrace will initiate an intelligent, targeted, autonomous response using platform-native controls (role/policy constraints and security groups) and interacting with the underlying network.



Cloud



Apps



Email



Endpoint



Network



Zero Trust



OT

### Consolidate your Point Solutions with a Platform Approach

Darktrace/Cloud combines with the rest of Darktrace's product suite, sharing insights across the digital estate to bring stronger, business-wide protection.



#### See Darktrace in action - and discover your cloud in a new light.

- Available on the AWS marketplace
- AI learns your environment within a week
- Agent or agentless delivery options
- 30-day no obligation free trial

