





KEY BENEFITS:

-  Offers complete, real-time visibility of workloads and admin activity in AWS and beyond
-  Self-learning AI detects, interprets, and responds to the advanced threats that get through policy-based defenses
-  Learns 'on the job' to evolve with your dynamic workforce and workloads
-  Cyber AI Analyst automates threat investigation at speed and scale, reducing time to triage by up to 92%

INTRODUCTION

With self-learning Cyber AI, Darktrace combines unprecedented real-time visibility and autonomous threat detection, response, and investigation in your AWS cloud.

Autonomously Defending the Dynamic Workforce

With the power of Darktrace, gain real-time visibility and defense against even the most stealthy and novel threats in AWS, from critical misconfigurations to insider threats.

Darktrace uses Cyber AI to learn normal 'patterns of life' for all users, technologies, and resources across the organization, enabling it to recognize the subtlest anomalies that point to an emerging threat.

Prior to deploying Darktrace, our AWS environment was a blind spot. Darktrace has armed us with Cyber AI technology that defends our entire distributed infrastructure in real time.

/ Innovating Capital

Protecting AWS 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 open S3 buckets, anomalous permission changes, and unusual activity around compliance-related data and devices.

/ Compromised Credentials

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

/ Insider Threats and Admin Abuse

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



Figure 1: Darktrace Illuminates AWS environments

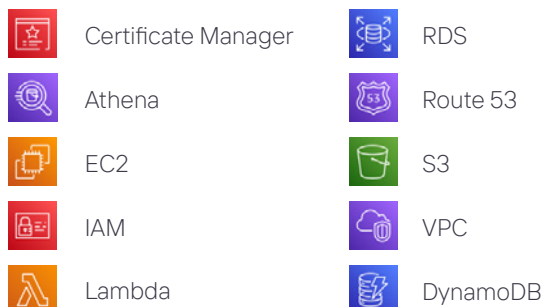
/ Leveraging VPC Traffic Mirroring for Enhanced Visibility

AWS VPC Traffic Mirroring gives our self-learning AI access to granular packet data, allowing Darktrace to extract hundreds of features from the raw data and build rich behavioral models for our customers' AWS cloud environments.

Real-time visibility of the underlying fabric of AWS environments, provided by VPC Traffic Mirroring, helps Darktrace's Cyber AI learn 'on the job,' continuously adapting as your business evolves. Darktrace provides the only security solution that learns in real time, a critical feature given the speed and scale of development in the cloud.

The Darktrace Security Module for AWS provides additional visibility, with AI-powered monitoring of management and administration activity via interaction with AWS CloudTrail.

With this deep knowledge of how your business operates in the cloud, Darktrace delivers total coverage across all your AWS services, including:



/ Unified AI-Driven Security Across the Enterprise

Darktrace/Cloud can be easily delivered via AWS or a hybrid deployment to provide coverage of customer cloud environments, as well as SaaS applications, email, corporate networks, industrial systems, and remote endpoints.

Taking a fundamentally unique approach, Darktrace/Cloud is the industry's only self-learning platform that correlates real-time information from across the organization.

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

/ Autonomous Cyber Defense

Prevent

Darktrace PREVENT continuously monitors your internal and external attack surface, including cloud environments, to reveal and prioritize threats and vulnerabilities before they are exploited.

Combining attack surface management with attack path modeling, security awareness training, and attack emulation, PREVENT offers an end-to-end solution that allows defenders to prioritize their time and resources, while autonomously hardening defenses.

Detect

With advanced self-learning AI, Darktrace/Cloud autonomously detects and correlates all the weak indicators of a threat – even if it's highly sophisticated or novel.

A real-time, contextual understanding of your AWS cloud environment and wider organizational activities grounds Darktrace/Cloud's ability to identify the threats that policy-based controls and other security solutions simply cannot.

Respond

The Darktrace RESPOND platform provides 24/7 active defense of your digital data and assets in AWS with autonomous response.

Darktrace RESPOND is the only technology on the market that can autonomously interrupt attacks on your behalf, at machine speed, and with surgical precision – providing advanced defense when your security team is overwhelmed or simply not around.

Investigate

Every threat is automatically investigated by Darktrace Cyber AI Analyst. An industry first, the technology autonomously triages, interprets, and reports on the full scope of security incidents.

Cyber AI Analyst Incident Reports include an executive-friendly summary of the event and response recommendations, as well as all the critical details needed for remediation. The AI-powered technology reduces triage time by up to 92%.

The majority of AI workloads nowadays are being done in the cloud. Because of this, we work closely with AWS both from an infrastructure perspective and in supporting our clients.

/ Mike Beck, Global CISO, Darktrace

