

DARKTRACE

Darktrace / CLOUD



Achieve cyber resilience with adaptive AI built to secure your multi-cloud environment in real time.

The cloud security landscape is rapidly **evolving**

As organizations transition more workloads and data to cloud environments, security teams often encounter challenges in detecting and responding to threats in real time, maintaining a clear view of all their assets and activities, and enforcing consistent security policies.

Many organizations struggle with inadequate visibility into their cloud architectures, making it difficult to track data and access across multi-cloud platforms. This lack of visibility can be attributed to the distributed nature of cloud services and the reliance on multiple platforms, which can obscure where data is stored and how it is being accessed.

Cloud environments also pose unique challenges for security teams particularly when responding to threats. The dynamic nature of cloud computing, where resources are constantly scaled up or down and configurations can change frequently, makes it difficult to detect and respond to threats in real time.

The combination of different cloud models (public, private, hybrid) and services (SaaS, PaaS, IaaS) results in a complex security landscape that is difficult to manage. This complexity not only makes it hard to enforce consistent security policies, but also increases the likelihood of configuration and permissions errors, which are a leading cause of cloud security incidents.

Existing solutions are siloed, creating **gaps in protection**

The dynamic nature and scale of cloud environments can overwhelm siloed security tools that are not designed to manage or integrate well across multiple cloud platforms and services. This complexity makes it difficult to detect and respond swiftly to threats, enforce unified security policies and identify misconfigurations promptly.

Securing both on-premises and cloud environments is crucial to ensure consistent protection and visibility across all parts of the infrastructure. Without complete visibility and a unified security strategy, gaps can emerge between on-premises and cloud infrastructure, providing opportunities for attackers to exploit these vulnerabilities and gain unauthorized access.

Current cloud security solutions often struggle to fully address the challenges of real-time detection and response, visibility and complexity, due to gaps in coverage and a siloed approach. Addressing these gaps requires a comprehensive cloud security strategy that includes real-time threat detection and response, contextual awareness, and proactive posture management. Unified multi-cloud security is essential for achieving robust protection against evolving cyber threats.

Discover real-time cloud security with Darktrace / CLOUD

Real-time detection & autonomous response

Detect and respond to known and novel threats across your entire cloud estate in real time with Self-Learning AI that understands what is normal for your organization. Leverage the power of Cyber AI Analyst to continually investigate and contextualize every alert in your cloud to simplify and accelerate the investigation process.

Dynamic cloud visibility & monitoring

Demystify your organization's complex cloud footprint and achieve real-time visibility into all cloud assets and architectures. Keep track of deployed cloud assets in real time and review automatically generated architecture diagrams to bring DevOps and Security together with shared context.

Proactive cloud protection & risk management

Shift security operations from reactive to proactive to stay ahead of attacks. Identify exposed assets and highlight internal attack paths to get a dynamic view of the riskiest paths across cloud environments.

Business benefits

Discover best-in-class cloud security

Industry leading real-time detection of unknown and novel cloud threats to gain a 60%¹ increase in the accurate detection of threats.

Respond with surgical accuracy in real time

The industry's only autonomous threat response with precision at machine speed to reduce time spent responding to detected threats by 90%².

Simplify and accelerate the investigation process

Automatically analyze and triage every alert transforming your security operations process for an 85%³ ROI improvement in prevented data breaches and reduced downtime.

Demystify your cloud infrastructure

With the industry's only dynamic real-time architecture modeling that delivers a clear picture of your infrastructure and 30%⁴ increase in visibility over cloud assets.

Proactively address cloud risk

Identify exposed assets and get a dynamic view of the riskiest paths across cloud environments.

Strengthen security posture and maintain compliance

Automated cloud posture management continuously evaluates cloud configurations, vulnerabilities and policy violations.

1 Based on increased threat detection from a Darktrace client in the manufacturing industry.

2 Based on time savings from a Darktrace client in the financial services industry.

3 Based on ROI improvement from a Darktrace client in the financial services industry.

4 Based on increased visibility from a Darktrace client in the real estate investment industry.

Key capabilities of Darktrace / CLOUD

Detect known and unknown threats across your on-premises and cloud environments

Get complete cloud coverage and uncover blind spots with precision threat detection.

Darktrace / CLOUD is an intelligent cloud security solution that uses Self-Learning AI to deliver complete cyber resilience for multi-cloud environments. It addresses modern cloud security challenges by giving you real-time detection and autonomous response in the cloud, continuous visibility and complete architectural awareness, and proactive cloud posture management in a unified solution.

Built on an industry leading AI platform that continuously learns from your day-to-day cloud operations, Darktrace / CLOUD applies this critical business context to visualize and monitor cloud assets, automate the investigation process, and disarm cloud-based threats in seconds. Darktrace / CLOUD supports multi-tenant, hybrid, and serverless environments, is agentless by default - with optional agents for enhanced real-time actioning and deep inspection- and deploys from the cloud in minutes. Unlike other cloud-native security vendors, Darktrace supports customers on their cloud migration journey by unifying visibility and security across on-premises and cloud workloads.

At a glance

-  Detect known and novel threats
-  Uncover anomalous activity in real time
-  Autonomous response at machine speed
-  Full cloud visibility and monitoring
-  Streamline SecOps with Self-Learning AI

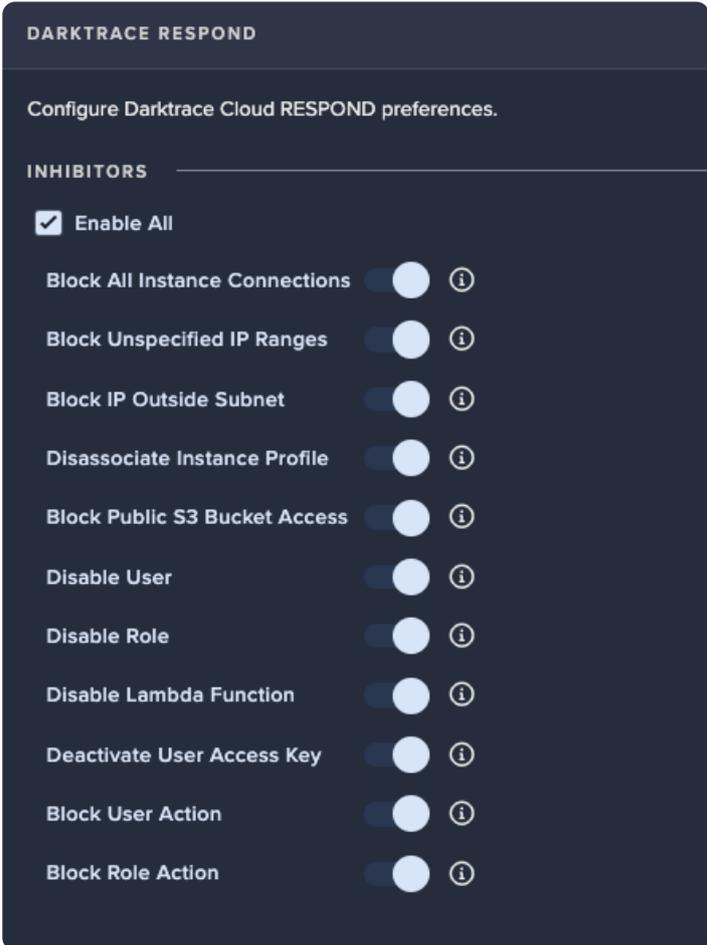


Figure 01: Darktrace / CLOUD autonomous response actions can be customized to your preferences and easily enabled or disabled as needed. (the image could be a little smaller to fit better on the page as well)

Real-time cloud detection & response

Disarm known, unknown, and novel cloud-based threats in seconds with autonomous real-time response in the cloud. Darktrace / CLOUD's Self-Learning AI continuously monitors and analyzes activity across cloud assets, containers, APIs, and users, using advanced identity and network context to rapidly detect and neutralize threats. Attack Path Modeling further enables security teams to identify attack paths as they happen.

Simplify and accelerate the investigation process with Cyber AI Analyst to ensure every alert is automatically analyzed and triaged, saving time and transforming your security operations. Cyber AI Analyst can make intelligent decisions based on thousands of data points correlated across network, identity, email, and cloud to save time and automatically investigate alerts.

Using platform-native Autonomous Response, AI-driven behavioral containment neutralizes malicious activity with surgical accuracy while preventing disruption to cloud infrastructure or services. As malicious behavior escalates, Darktrace Self-Learning AI correlates thousands of data points to identify and instantly respond to unusual activity by blocking specific connections and enforcing normal behavior.

Dynamic cloud visibility & monitoring

Gain real-time visibility into your entire cloud infrastructure, demystifying complex hybrid and multi-cloud cloud environments. Built from network, configuration and IAM connections, Cloud Asset Enumeration and Dynamic Architecture Modeling deliver a clear picture of your infrastructure that changes as your infrastructure evolves to display live detection information. With automatically generated architecture diagrams and continuous asset monitoring, DevOps and SecOps teams can collaborate effectively, ensuring a unified understanding and shared context for faster, more informed decisions.

Monitor and secure workloads at scale, including containerized environments like Kubernetes, with continuous network traffic analysis. Flexible and complimentary deployment options include agentless by default, with optional agents for deep packet inspection to ensure cyber resilience and seamless integration into existing workflows. Unite your teams with shared visibility to accelerate cloud migration and maintain security across on-premises and cloud environments.

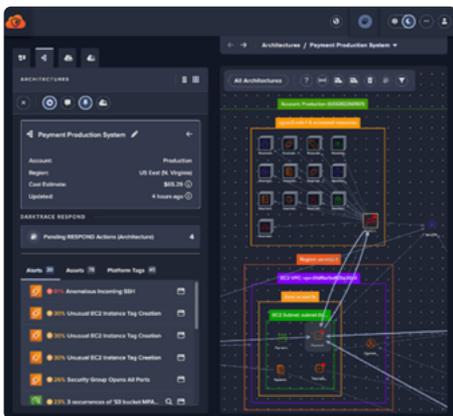


Figure 02: Dynamic Architecture Modelling provides continuous real-time monitoring.

Proactive cloud protection & risk management

Get ahead of attackers with Attack Path Modeling for the cloud. Identify exposed assets and highlight internal attack paths to get a dynamic view of the riskiest paths across cloud environments, network environments, and between – enabling security teams to prioritize based on your unique business risk, and address gaps to prevent future attacks.

Enhance your cloud security posture by prioritizing and addressing misconfigurations and risks based on your unique business context. Protect against insider threats and lateral movement by securing role permissions and access, shifting from reactive to proactive security operations to stay ahead of attacks. Automated cloud posture management continuously evaluates configurations against standards like CIS, identifying vulnerabilities and policy violations in real time.

Darktrace / CLOUD dynamically adjusts its focus based on evolving risks, analyzing misconfigurations and anomalous activity to prevent potential attacks. With Entitlement Enumeration, gain visibility into all identities, roles, and permissions, allowing dynamic adjustments to stop insider threats.

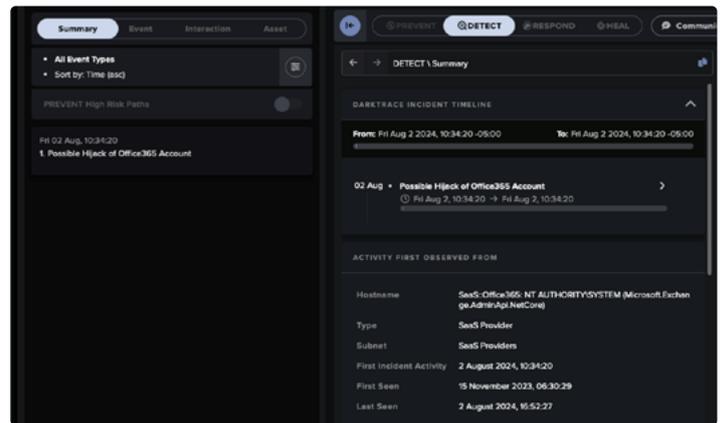


Figure 03: Gain visibility into all identities, roles and permissions to stop lateral attacks and insider threats in their tracks.

Investigate all alerts in your environment with the industry's first AI Analyst

Darktrace / CLOUD leverages the power of Cyber AI Analyst, bringing cognitive automation to your data and reducing triage times by 92%.⁵

Augment your SOC team capabilities

Unlike prompt-based LLMs that just create incident summaries or other vendors with basic AI investigation capabilities, Cyber AI Analyst is the only technology on the market that can truly operate like an experienced human analyst. It helps your SOC team automate the investigation of security incidents at machine speed and drastically reduce triage times.

Cyber AI Analyst continually analyzes and contextualizes every alert in your network with an understanding of what is normal behavior for your organization. It autonomously forms hypotheses and reaches conclusions just like a human analyst would, saving your team a significant amount of time and resources.

Uncover sophisticated threats with detailed investigations

Our Cyber AI Analyst intelligently investigates all alerts in your cloud, connecting seemingly benign events to uncover sophisticated threats and correlating related activities into a single incident. By piecing together anomalies which may appear

At a glance

- ✦ Harness the power of Cyber AI Analyst
- 🧠 Augment your SOC team
- ⚠️ Automate alert triage and investigation
- ☁️ Detailed cloud forensics
- 📄 Complete business context

harmless, Cyber AI Analyst autonomously identifies subtle malicious actions and uncovers advanced network threats, tracking them across the entire kill chain in real-time and at scale.

Get complete business context

Contextualize alerts from all areas of your environment in a single solution. Darktrace Cyber AI Analyst tracks connections and events across network, endpoint, cloud, identity, OT, email and remote devices, helping you detect and investigate modern threats that traverse your entire digital estate.

Add your existing EDR to Darktrace / NETWORK and Darktrace / CLOUD to create the foundation of an incredibly effective XDR solution in comparison to XDR vendors that lack native capabilities beyond their EDR origins. Security teams can leverage the Darktrace ActiveAI Security Platform to add proactive and recovery capabilities as well as covering email, identity and OT within a single connected solution.

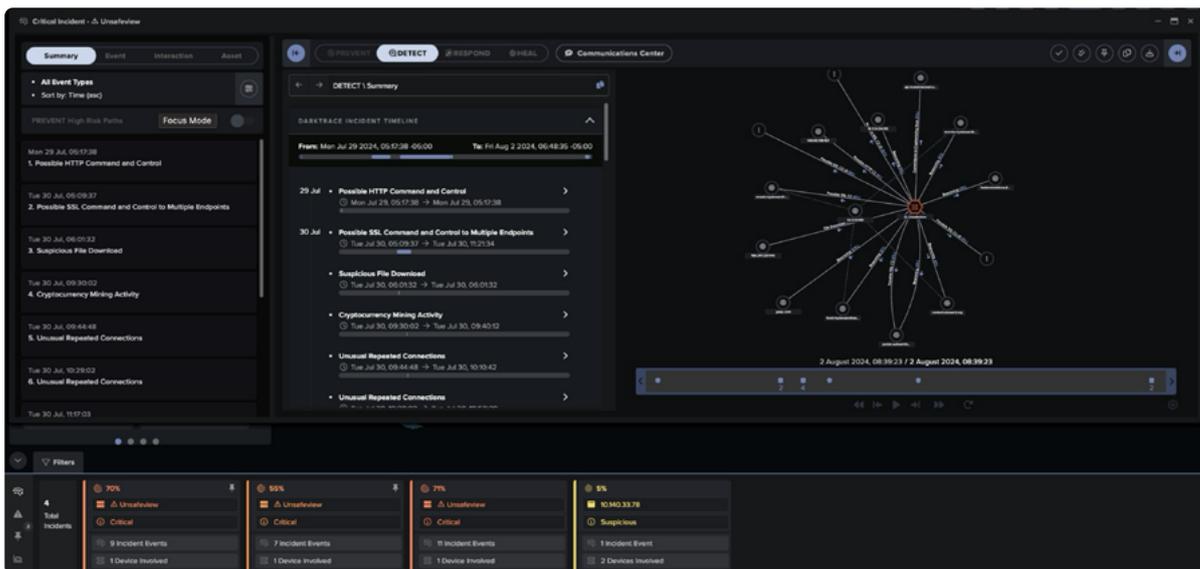


Figure 04: Cyber AI Analyst continually analyzes and contextualizes every alert in your cloud environment with an understanding of what is normal behavior for your organization. A detailed timeline of the incident and a full summary is provided to reduce time to meaning for your team.

⁵ Based on time savings from a Darktrace client in the manufacturing industry.

Neutralize cloud-based threats in seconds with autonomous response

Automatically contain and respond to attacks in real-time without disrupting business operations.

Autonomous threat response

Darktrace / CLOUD rapidly contains and disarms threats based on the overall context of the environment and a granular understanding of what is normal for a device or user - instead of relying on historical attack data. Darktrace / CLOUD is the only Cloud Detection and Response solution that can autonomously enforce a pattern of life based on what is normal for a standalone device or group of peers.

Darktrace / CLOUD autonomously takes precise response actions in real-time to contain threats without disrupting business operations - either natively or via third party integrations.

At a glance

- Autonomous response
- Pattern of life and behavioral context
- Targeted actions to avoid disruption
- Native response actions
- Fully customizable

Stay in full control

Darktrace / CLOUD autonomously takes the most effective response to cloud threats, so there's no need to spend time maintaining playbooks or manually tuning your deployment.

If you'd prefer to adjust response actions yourself, you can easily customize them with our intuitive model editor. Adjust every action and response logic in granular detail to fine-tune your deployment your way. Choose different response actions based on types of devices, IP ranges, office working hours and countless other parameters.

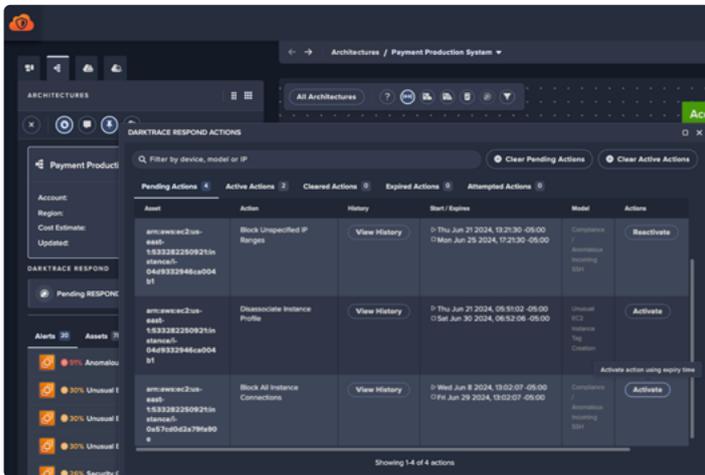


Figure 05: Get full visibility of the events leading up to an incident, including how our AI autonomously responds to protect your business.

Extend cloud visibility to the network and remote devices

Darktrace / ENDPOINT

Darktrace / NETWORK

Extend detection and response capabilities to your network and gain complete enterprise coverage with Darktrace / NETWORK. Disarm known and unknown novel network-based threats in seconds with platform-native autonomous response actions.

Darktrace / NETWORK

Darktrace / ENDPOINT

Darktrace / ENDPOINT enables you to maintain network visibility of remote devices and brings autonomous response capabilities to your endpoints, taking targeted response actions to restrict anomalous connectivity at the system level.

Deploying Darktrace / CLOUD

Darktrace / CLOUD deploys in minutes with flexible deployment options and supports multi-tenant, hybrid, and serverless environments. Darktrace / CLOUD is agentless by default, using combination of traffic mirroring and API logs, with optional lightweight host-based server agents for deep inspection.

Analysis

Darktrace can be deployed in a variety of ways to provide full visibility into your hybrid multi-cloud environments. Each deployment starts with the provision of a nominated 'master' instance of Darktrace, deployed as a virtual instance. Cloud and network data from across your environment is processed and analyzed by the Darktrace master instance, and the output is exposed in the Darktrace Threat Visualizer.

Darktrace provides fully virtualized deployments by hosting a cloud-based master instance within Darktrace cloud environments (AWS and Azure), which can address both virtual and physical locations. Where multiple masters are required, a 'Unified View' can be used to provide a single, consolidated user interface across all master instances. High Availability (HA) options are also available where required.

Collection

Darktrace master instances can process raw traffic themselves and collect network data from local 'probes' (virtualized or physical) across your cloud. In this topology, Darktrace probes perform Deep Packet Inspection (DPI) on ingested data, providing a continuous stream of data to the master appliance at a fraction of the bandwidth of the original traffic. Raw data, such as packet capture data, is kept on the probe and recalled on-demand from the master instance's Threat Visualizer web interface.

vSensors are lightweight virtual probes that can be deployed as a standalone virtual machine receiving packets from a virtual switch, in a public cloud VPC traffic mirroring, Microsoft virtual network flow logs, or by collecting packets from host-based osSensor agents deployed on VMs. Darktrace can also integrate with containerized environments such as Kubernetes.

Hardware probes can also be deployed to physical locations where required. A variety of hardware appliances are available depending on the volume of traffic and number of devices in your network.

Darktrace / CLOUD also collects data from host-based Client sensors, integrated third-party services (such as SaaS or cloud applications) or from connected Darktrace products.

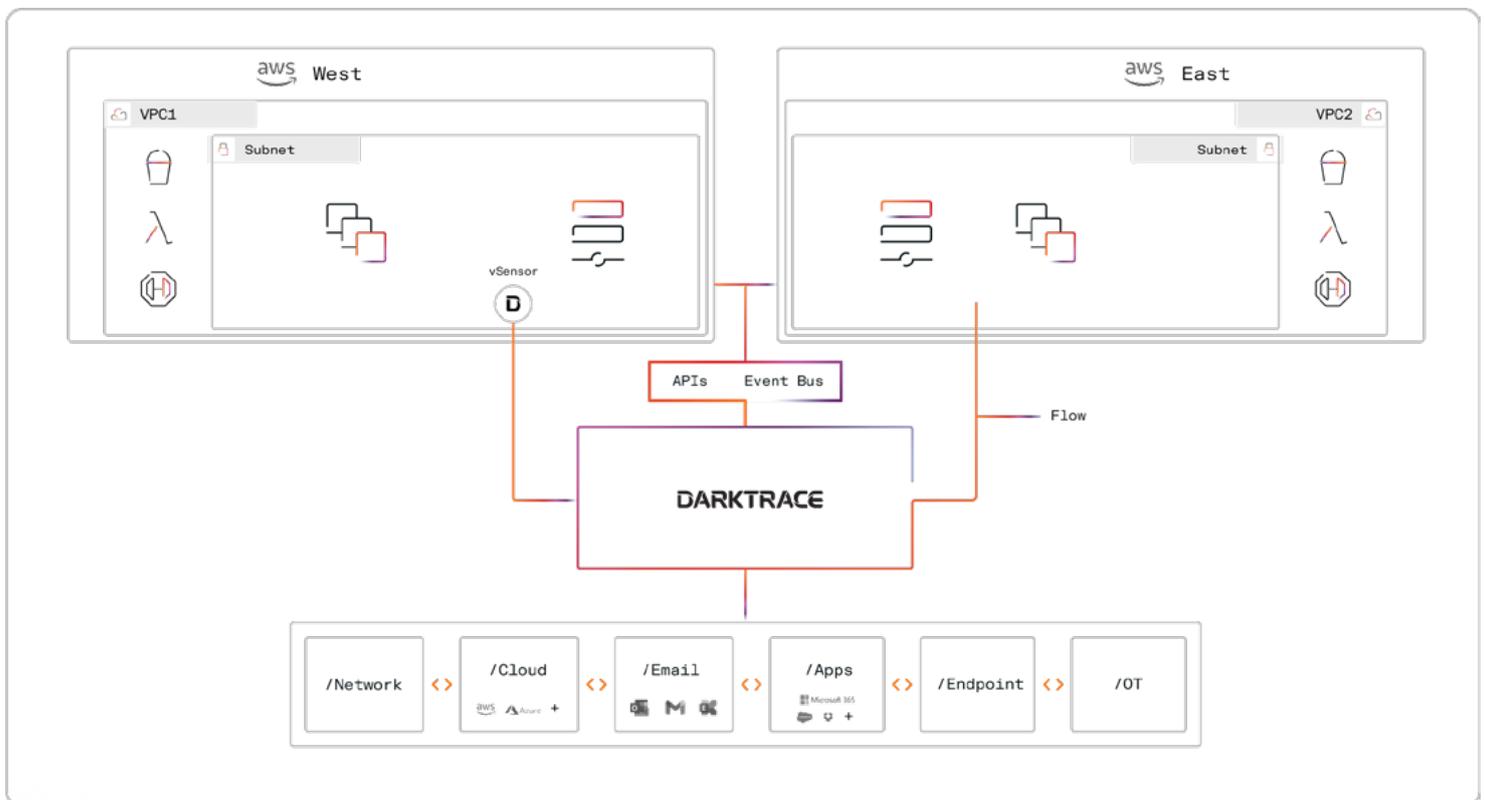


Figure 06: Darktrace / CLOUD deployment

Achieve cyber resilience with the Darktrace ActiveAI Security Platform

Darktrace / CLOUD is part of the Darktrace ActiveAI Security Platform, combining network security with the rest of your digital estate to enhance your security visibility and control across your cloud environments, endpoints, email, identities and OT devices.

Darktrace / CLOUD integrates with Darktrace / Attack Surface Management to deliver continuous, customized detection of externally exposed assets. When combined with Darktrace / Proactive Exposure Management, your organization can take pre-emptive actions to identify, analyze and mitigate internal and external security risks.

Darktrace / Incident Readiness & Recovery takes information from Darktrace / CLOUD and all other areas of the ActiveAI Security Platform to help you anticipate, detect, contain, recover and learn from any cyber incident. Tailored playbooks for effective recovery are based on a deep understanding of your network and wider threat landscape, helping you to maintain operational continuity against modern adversaries.

Darktrace ActiveAI Security Platform revolutionizes your cyber defenses by helping you proactively prevent cyberattacks, quickly recover from incidents and continually strengthen your security posture, all within a single platform.

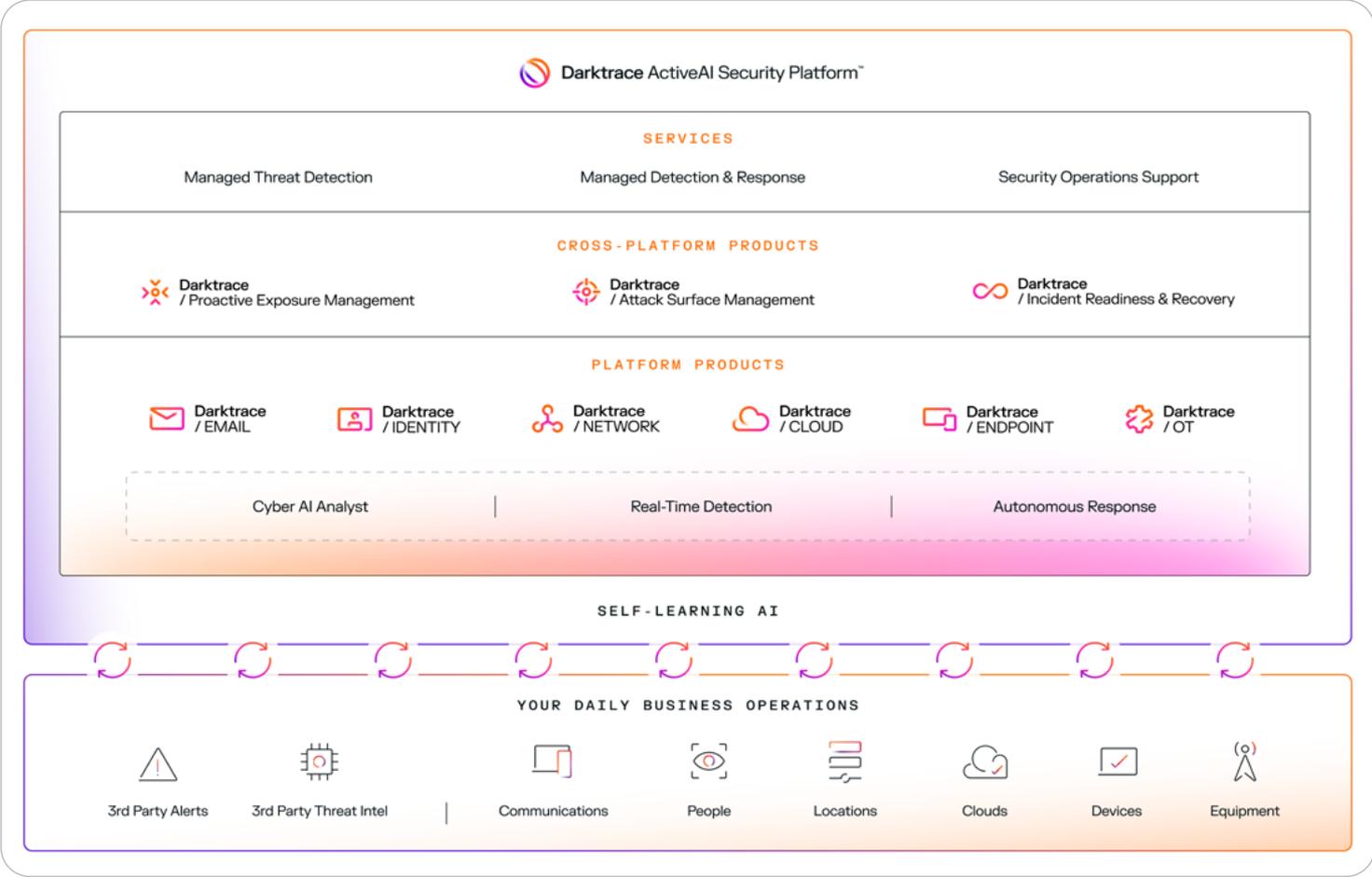


Figure 07: The Darktrace ActiveAI Security Platform

Operational Benefits

Increase operational efficiency

with Self-Learning AI that autonomously tunes itself to surface critical alerts to your attention and remove the hassle of manual tuning.

Reduce the pressure on security teams

by leveraging Cyber AI Analyst that operates just as a human analyst would, automating the investigation of security incidents and reducing triage times by 92%.⁵

Stay in full control

with advanced customization options and response actions based on device types, IP ranges, office working hours and countless other parameters.

“Darktrace / CLOUD is positioned to help security teams prioritize where to invest their valuable time and what to address based on the context into their environment and what’s really happening.”

■ CISO
Domino’s

“We can now identify problems in seconds and minutes as opposed to hours and days.”

■ Financial Services Company
US

Go beyond CDR (Cloud Detection & Response)

with advanced customization options and response actions based on device types, IP ranges, office working hours and countless other parameters.

Maximize your cyber defenses

with the Darktrace Managed Detection & Response service, helping you focus on security outcomes with support from a 24/7 SOC team.

“Darktrace allows us to apply the same security model to all traffic, whether it is on-premises or in the cloud.”

■ ICT Manager
Dreamworld

“Having a holistic, live view of our cloud environment enables us to work pragmatically and use AI to cut down management time so that we can address security risks and improve our resilience.”

■ Head of Cybersecurity
Sykes Cottages

▪ **About Darktrace**

Darktrace (DARK.L), a global leader in cybersecurity artificial intelligence, is on a mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to help transform security operations and improve cyber resilience. Breakthrough innovations from its R&D Centers have resulted in more than 200 patent applications filed. Darktrace employs 2,400 people around the world and protects over 9,700 organizations globally from known, unknown and novel cyber-threats.