DARKTRACE

Darktrace / CLOUD

Real-Time Detection, Response, and Automated Investigation for the Cloud

The cloud security landscape is rapidly evolving

Cloud attacks are increasing in both speed and sophistication, with 82% of breaches now involving data stored in the cloud and 60% of organizations reporting delayed investigations due to missing evidence from short-lived assets.[1]

As cloud environments grow more dynamic, threats evolve faster than traditional tools can detect or contain. Security teams are under pressure to detect, investigate, and remediate incidents in real time, yet many lack the automation, visibility, and forensic depth to do so. The result is longer dwell times, higher costs, and increased compliance risk.

Cloud security remains dominated by legacy tools repurposed for the cloud that rely on agents, manual tuning, and siloed telemetry. These tools require privileged scanners for vulnerability management, manual processes for evidence gathering, and isolated dashboards that lack architectural context. Cloud assets can spin up and down in minutes, often disappearing before any evidence is collected. Without instant forensic capture or visibility into memory, disk, and logs, analysts are left reconstructing partial stories long after an attack has unfolded.

Security teams are overwhelmed, operating across fragmented tools and incomplete data. They need a unified solution that can detect and contain threats in real time, preserve forensic evidence instantly, and deliver live architectural context across workloads, storage, and users. By combining autonomous response with automated cloud investigations, organizations can finally close the gap between detection, investigation, and recovery and achieve true cyber resilience in the cloud.

Existing solutions are siloed, creating gaps in protection

The dynamic nature and scale of cloud environments continue to overwhelm traditional and siloed security tools. Many products were never built for cloud-native architectures and struggle to manage or integrate effectively across multiple platforms and services. This lack of unification makes it difficult to detect threats quickly, enforce consistent policies, and identify misconfigurations in real time.

Most cloud security tools today focus on a single aspect of the problem, leaving critical blind spots across detection, investigation, and response. CNAPP and CSPM tools surface risks but lack runtime visibility or forensic depth. XDR and SIEM platforms detect threats but rely on slow, manual investigations and often lose evidence when cloud assets terminate. Manual DFIR processes and external consultancies introduce additional delay and cost, preventing teams from achieving real-time incident understanding or response.

Organizations need an integrated approach that combines real-time threat detection and autonomous response with automated cloud investigations, dynamic visibility across cloud architectures and identities, and proactive posture management. A unified hybrid cloud security strategy is now essential to bridge the gap between detection and investigation, reduce mean time to respond, and deliver full architectural awareness across modern cloud ecosystems.

[1] IBM Cost of a Data Breach Report 2025;
2 ESG State of Cloud Security 2025

Key capabilities of Darktrace / CLOUD

Business benefits

Discover
best-in-class cloud security with up to a 60%[1] increase in accurate threat detection.

Respond
with precision in real time to reduce response times by 90%[2].

Accelerate
investigations with automated triage and analysis, delivering up to an 85%[3] ROI improvement in prevented breaches and reduced downtime.

Gain
complete visibility with dynamic, real-time architecture modeling for a 30%[4] increase in cloud asset awareness.

Strengthen
security posture and maintain compliance through continuous configuration and policy evaluation.

Reduce
mean time to respond (MTTR) with instant forensic acquisition and AI-driven investigations that eliminate evidence gaps.

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.

Detect and respond to known and unknown threats

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

Darktrace / CLOUD uses Self-Learning AI to deliver continuous detection and autonomous response across hybrid and multi-cloud environments. It learns what normal looks like for your unique business, detecting known, unknown, and novel threats across cloud assets, identities and networks.

Cyber AI Analyst automatically analyzes and correlates alerts to accelerate investigations, while Autonomous Response neutralizes malicious activity in seconds without disrupting business operations.

For organizations that require deeper analysis, Darktrace / CLOUD captures forensic evidence including disk, memory, and logs the moment suspicious activity is detected. This ensures visibility even into short-lived cloud assets, allowing security teams to investigate and respond with complete context. Together, these capabilities enable precision detection, instant containment, and faster resolution of threats across hybrid multi-cloud environments.

Real-time Cloud Detection & Response

Darktrace / CLOUD delivers precision detection and autonomous response in real time. Powered by Self-Learning AI, it continuously monitors workloads, containers, APIs, and users to identify known, unknown, and novel threats the moment they emerge.

Cyber AI Analyst automatically investigates every alert, correlating thousands of data points to accelerate triage and simplify the analyst workflow. Using Autonomous Response, Darktrace takes immediate, proportionate actions to contain malicious activity with surgical accuracy while maintaining uptime. Combined with Attack Path Modeling, teams can identify emerging attack routes as they happen and stop threats before they spread.

Automated Cloud Investigations & Root Cause Analysis

Darktrace / CLOUD automates the entire investigation process to reveal root cause in minutes. FAI instantly captures and preserves forensic evidence, including disk, memory, and log data, the moment a threat is detected, even for short-lived assets that traditional tools miss. It automatically correlates this evidence with additional context to automatically reconstruct the full attacker timeline, identify the entry point, and determine scope of impact. This enables security teams to reduce investigation time from days to minutes, eliminate data gaps, and respond confidence.

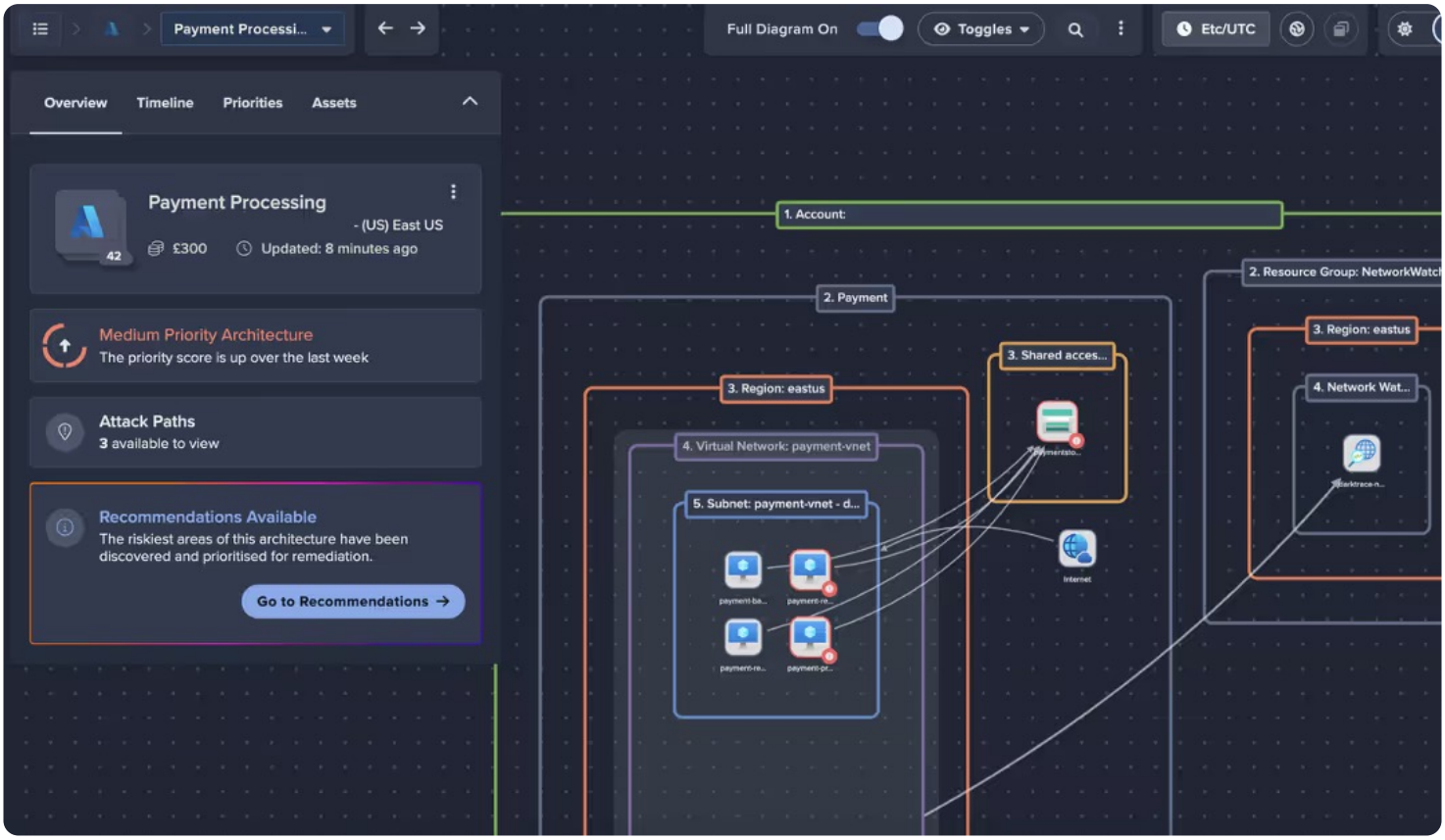


Figure 01: Live cloud topology maps unify visibility across architectures, identities, network connections and more.

Dynamic Cloud Visibility & Monitoring

Darktrace / CLOUD provides continuous visibility into your hybrid and multi-cloud environments with Dynamic Architecture Modeling and Cloud Asset Enumeration. These capabilities automatically map and visualize your infrastructure as it evolves, offering a real-time understanding of assets, users, and relationships across AWS, Azure, and GCP. Continuous monitoring across configuration, network, and IAM layers exposes misconfigurations, risky access paths, and lateral movement. Flexible deployment options include agentless coverage by default, with optional agents for Deep Packet Inspection to deliver additional depth where needed. With shared, real-time context, DevOps and SecOps teams can collaborate seamlessly and respond faster.

Proactive Cloud Protection & Risk Management

Darktrace / CLOUD transforms posture management into continuous risk prevention. Using Attack Path Modeling, it dynamically identifies exposed assets and high-risk pathways to prioritize remediation based on real business context. Continuous posture management automatically evaluates configurations, vulnerabilities, and policies against standards like CIS to maintain compliance and reduce exposure. Entitlement Enumeration provides full visibility into identities, roles, and permissions to prevent privilege misuse and insider threats. As environments evolve, Darktrace adapts focus to emerging risks, helping security teams stay proactive and resilient in the face of evolving threats.

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

92%

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

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 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.

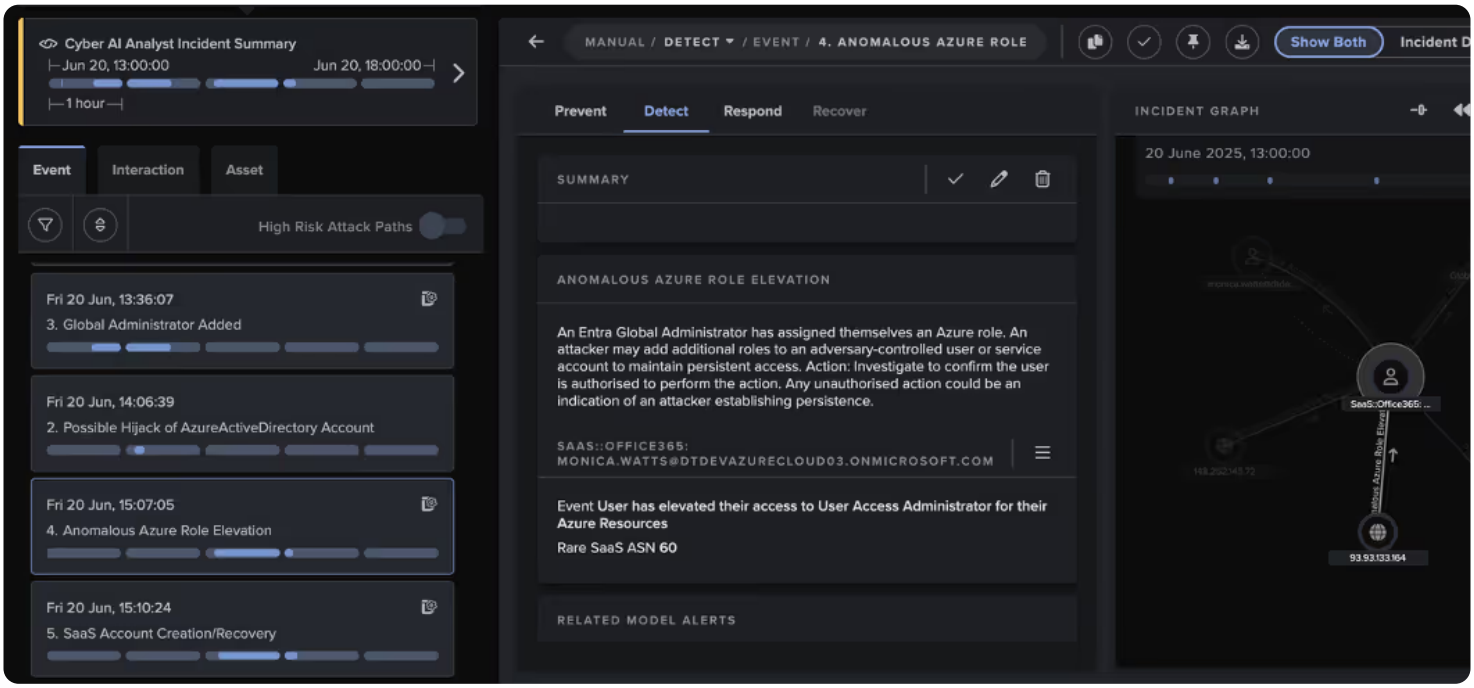


Figure 02: Cyber AI Analyst summary of anomalous behavior for privilege escalation and establishing persistence.

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.

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.

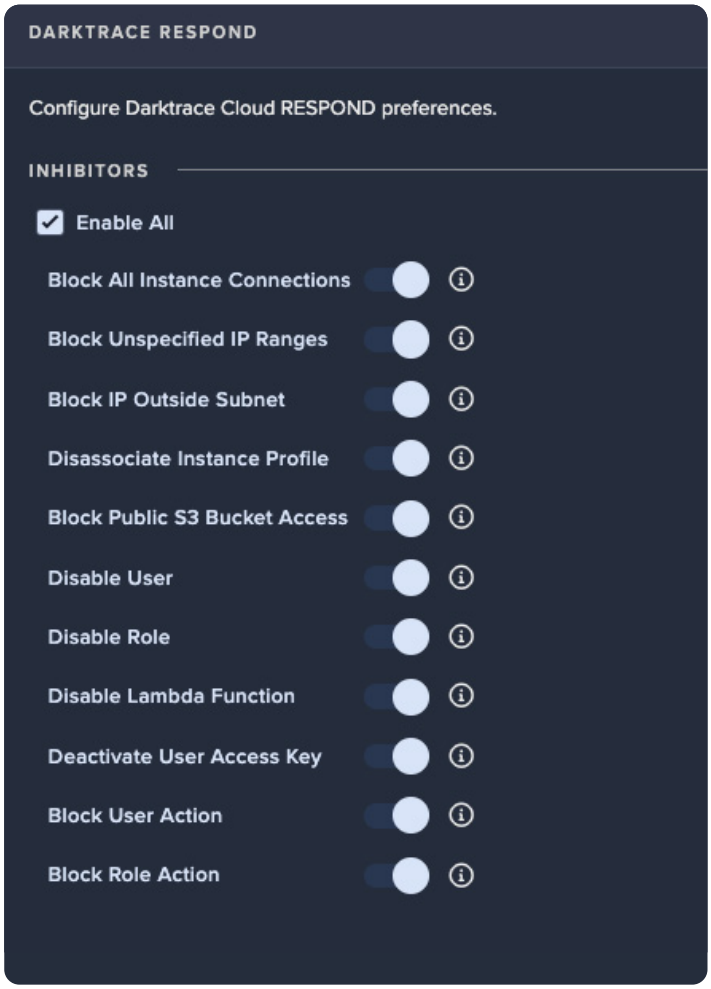


Figure 03: Darktrace / CLOUD autonomous response actions can be customized to your preferences and easily enabled or disabled as needed.

Deploying Darktrace / CLOUD

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

Deploys in minutes, not months

Darktrace / CLOUD deploys rapidly across multi-cloud, hybrid, and serverless environments with minimal configuration. Its agentless-by-default design connects directly through APIs and traffic mirroring to start learning your environment immediately. Most customers achieve full visibility within hours, not weeks, accelerating time to value.

Flexible, frictionless data collection

Choose the data collection approach that fits your environment — from API integrations and traffic mirroring to lightweight host-based agents for Deep Packet Inspection (DPI). This flexibility ensures the right level of depth for every workload without adding overhead or disrupting performance.

Unified visibility across any architecture

Whether your infrastructure spans multiple clouds or combines virtual and physical networks, Darktrace provides a single, consolidated view through the Darktrace Threat Visualizer. Its Unified View aggregates all environments, giving security teams consistent visibility and control across every deployment, region, and account.

Scales effortlessly with your cloud

Built to evolve with your environment, Darktrace / CLOUD supports multi-tenant and high-availability architectures to match your growth. Virtual sensors (vSensors) and optional probes can be deployed anywhere traffic flows; across public clouds, virtual networks, or containerized workloads like Kubernetes, ensuring continuous, scalable visibility as your infrastructure expands.

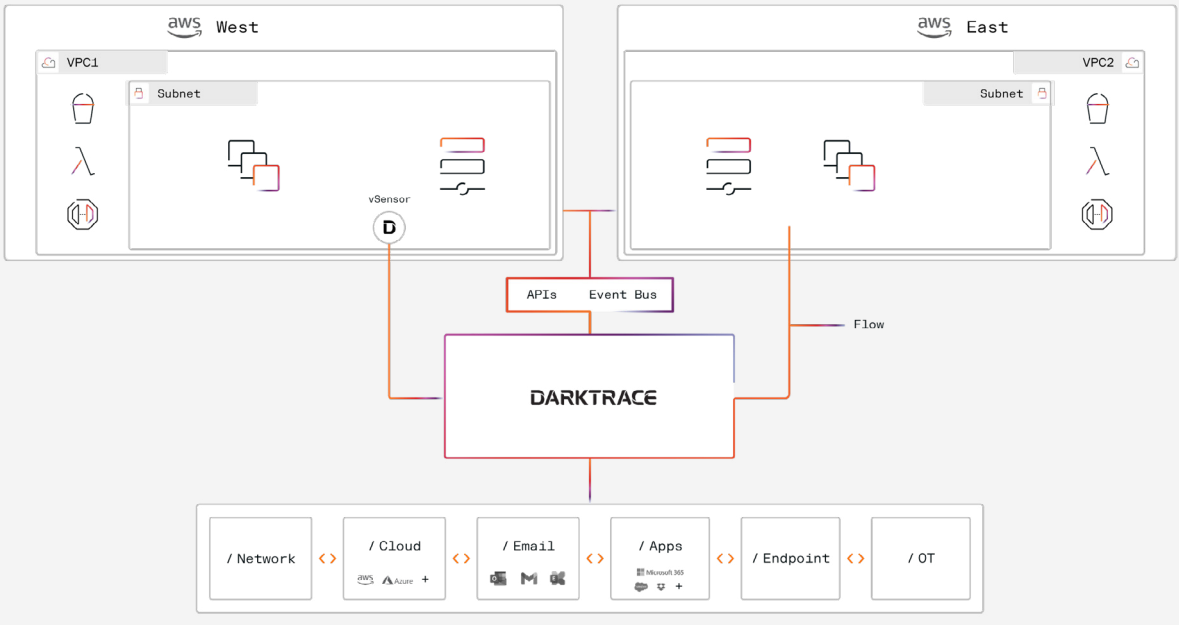
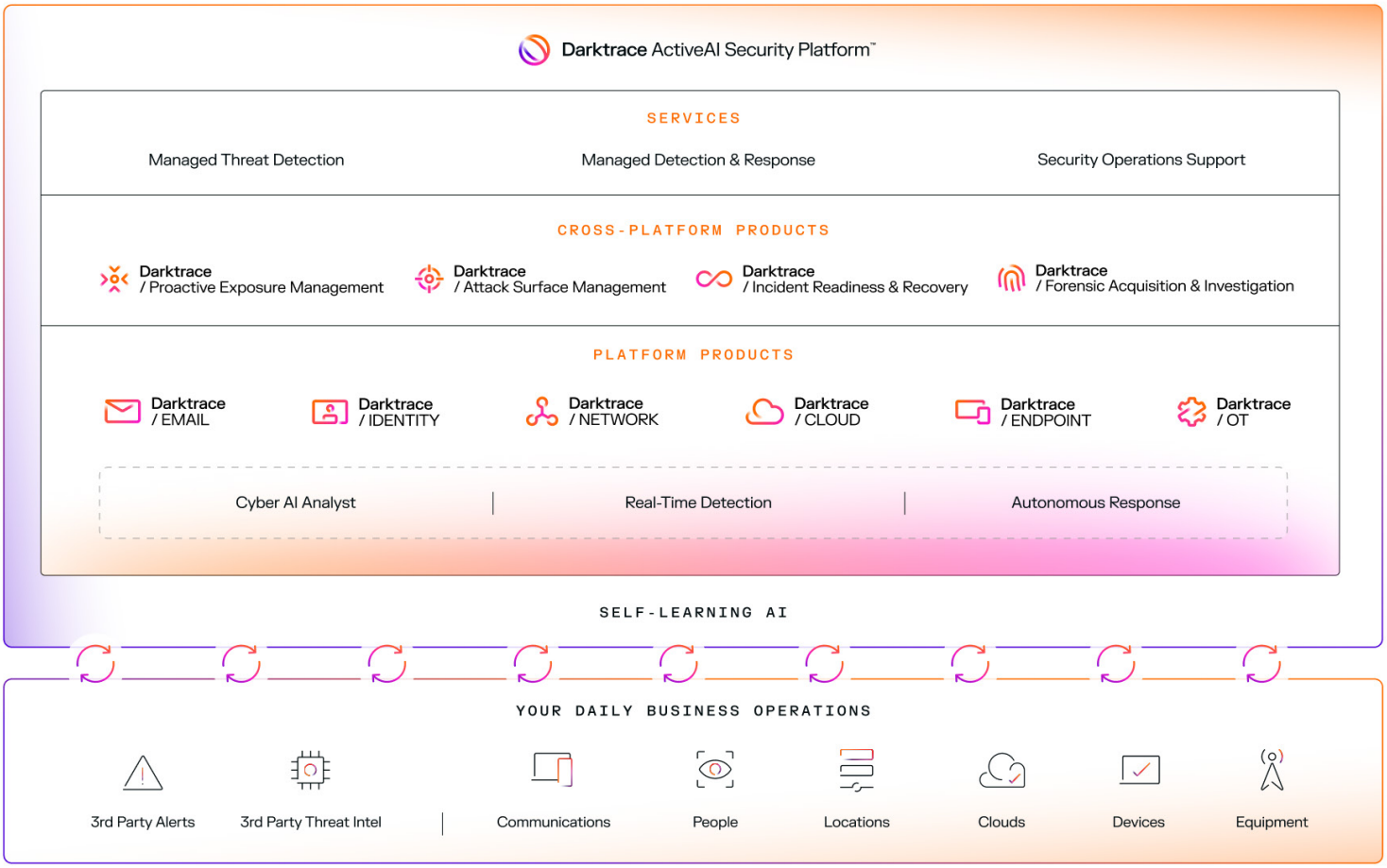


Figure 04: Darktrace / CLOUD deployment

Unified AI-driven protection across your entire digital ecosystem



Darktrace / CLOUD is part of the Darktrace ActiveAI Security Platform, which unifies protection across cloud, network, email, identity, and operational technology.

Powered by Self-Learning AI, the platform continuously understands how your organization operates to detect, respond to, and investigate threats in real time, wherever they emerge.

Darktrace / CLOUD works alongside Darktrace / EMAIL, Darktrace / NETWORK, and Darktrace / IDENTITY to provide end-to-end visibility and autonomous response across every attack surface. Integrated / Forensic Acquisition & Investigation adds instant evidence capture and automated root cause analysis, turning incidents into opportunities for continuous learning and resilience.

Through integrations with Darktrace / Attack Surface Management and / Proactive Exposure Management, organizations can proactively identify and mitigate both internal and external risks before attackers exploit them.

Together, the Darktrace ActiveAI Security Platform helps security teams prevent, detect, respond to, and recover from cyber incidents faster — uniting protection and visibility across the entire digital estate within a single, self-learning ecosystem.

About Darktrace

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,700+ employees who protect nearly 10,000 customers globally. To learn more, visit www.darktrace.com.

North America: +1 (415) 229 9100 | Europe: +44 (0) 1223 394 100 | Asia-Pacific: +65 6804 5010 | Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com