DARKTRACE

Darktrace ActiveAI Security Platform

Move beyond XDR to a proactive AI approach that automates investigations to transform your SOC and builds cyber resilience

The reality of cybersecurity solutions

The advent of AI in offensive tools and rise of cyber-crime-as-a-service have drastically increased the speed, sophistication, and success of cyber security attacks. Multi-domain and multi-stage attacks now dominate the adversarial approach, delivering new threat variants at machine speed against an enterprise's infrastructure, applications, and people, until they successfully exploit a weak point.

When it comes to defense, traditional, reactive cyber security solutions cannot keep up.

- Old Detection Paradigm: Nearly all rely on existing threat data for detection, only stopping what is known, chasing the latest update, and creating a sea of alerts for unknown threats with a flood of false positives leading to alert fatigue for SOC teams
- Lack of contextualized visibility: Point solutions provide depth of visibility but are not able to draw context across multiple IT domains.
- Inefficient cross-platform insights, needing human intervention: Recent approaches like eXtended Detection and Response (XDR) stitch together suspicious events across the enterprise, but still depend on human validation, remain reactive and have inadequate domain coverage like in email, where 22% of attacks start.[1]

Security teams are at a breaking point, with too many alerts, too little time, and fragmented support from a bloated vendor stack. They need a consolidated security approach that combines AI, data-driven context, and the ability to close gaps in visibility over policy and process to improve mean times to identify and contain threats.

Business benefits

Detect known, unknown and novel threats up to 3 months faster with the industry's only platform built on self-learning AI[2]
Unlike traditional security tools that rely on existing threat data and signatures for detections, get AI that deeply understands your business environment to catch unknown threats by contextualizing user, email, device, application, endpoint, network and cloud activity to understand your normal 'pattern of life' that is unique to your business

Gain unprecedent visibility across your entire enterprise
Minimize potential risks and damages across your entire digital presence with threat detection, autonomous response, and recovery for network, OT, cloud, email, applications, and your identities

Get better outcomes than XDR, with automated alert investigations including 3rd Party alerts
Integrate alerts from third-party security tools like EDR and network with ease and eliminate manual alert triage by having every relevant alert investigated and triaged by the Cyber AI Analyst to identify critical incidents

Preventive cyber resilience hardens your environment before an attack
Gain a pioneering platform that includes Proactive tools that identify & prioritize exposed assets, attack paths, and vulnerabilities that let teams stop threats before they occur

Remediate and recover from each unique incident in as little time possible with tailored automated playbooks:
Save critical time during emerging incidents with bespoke AI-generated playbooks that are unique to both your environment and the incident in question

Investigate every relevant alert through automated alert triage and reduce risks
Go from investigating a few alerts to investigating ALL relevant alerts through automated alert investigations done by Cyber AI Analyst, reducing risks significantly and ensuring that important alerts are not missed (which happens due to SOC capacity constraints)

Transform and expand the capacity of your SOC team to focus on Proactive Measures
When analyzing 30 alerts a day, Cyber AI Analyst typically provides a SOC with the equivalent of 5,000 additional hours (or ~3 Full Time Employees) of Level 2 analysis and written reporting annually. This can be scaled to far more as needed, enriching security operations by producing high level incident alerts with full details so that human analysts can focus on Level 3 tasks.[3]

Gain cost savings of up to 40% with an AI-led platform approach[4]
Don't be limited by Gen AI and chat-based LLMs that can only augment not investigate. Instead, get significant cost savings with the Darktrace Platform that provides self-learning AI, real-time detection, Cyber AI Analyst and autonomous response capabilities

Unified reporting eases communication to key stakeholders
Get ahead of board requests with proactive notifications on the latest threats & prioritization of people, process, and technology risks

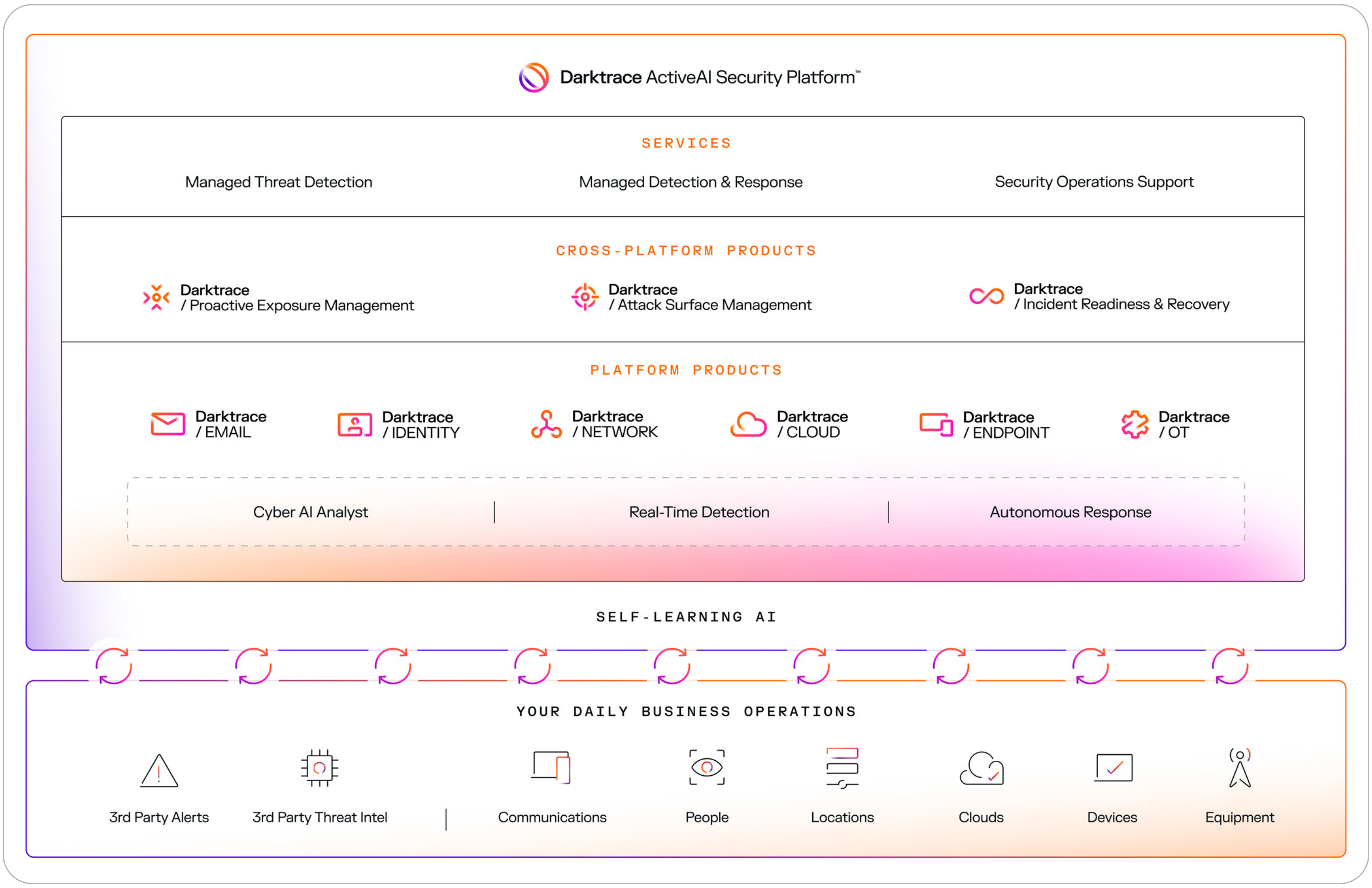
[1] Darktrace Customer Insights

[2] AI Neutralizes Hafnium Cyber Attack in December 2020 Darktrace | Darktrace Blog

[3] Internal Darktrace Research

[4] M-Trends 2023 Mandiant Special Report

Darktrace ActiveAI Security Platform



The Darktrace ActiveAI Security Platform is designed for your Security Operations Center to eliminate alert triage, perform investigations, and rapidly detect and respond to known and unknown threats, whilst exposing risk gaps across your technologies and processes so your team can shift to a proactive cyber approach. The solution is built on Self-Learning AI that continuously trains from your ever-changing business data wherever it is deployed, with further enrichment from external threat intelligence and third-party alerting.

This learning is not limited by yesterday's threat data but looks at deviations of your unique business operations, revealing even the subtlest indicators of malicious intent that may pose a threat to your business, known, unknown, and never before seen. Security operations process is transformed by our trusted Cyber AI Analyst, the investigative AI which continuously performs full investigations of relevant Darktrace and third-party alerts.

The result shifts the existing process of triaging few alerts from the thousands per day, to triaging all relevant alerts, eliminating the manual process and automatically prioritizing attacks, leveling up your team to review investigative results and perform deep secondary analysis if needed, or spend time closing security gaps.

Threats are contained in real-time by Darktrace ActiveAI Security's autonomous response, paired with bespoke incident response playbooks to support the recovery process during your most critical incidents. In addition to handling incidents as they arise, the platform delivers insights for the proactive identification of exposed assets, vulnerabilities, and attack paths so that potential risks can be addressed before an attack occurs.

This improves the entire security posture - including training people via attack and phishing simulations to ensure human readiness.

Key capabilities

Unprecedented visibility across the enterprise with a Self-Learning AI

Traditional cybersecurity vendors have set focus areas within an IT domain, where they can use their expertise of known attack data to determine what is a threat and whether it should be prioritized. Even for those using machine learning-led behavioral detections, they rely on training supervised machine learning models on historical attack data based on what they have seen before, not whether the activity is unusual for the enterprise.

In this way, they focus on the breach rather than the business and have little enrichment beyond their specialty coverage area. Darktrace lets security operations teams experience a new approach to visibility that keeps machine pace with the threat landscape, surfacing what is most important to your business.

- Apply AI algorithms and compute power across network, OT, cloud, email, applications, and your identities to develop a sophisticated understanding of your unique business data that saves time on integrations and vendor management.
- Continuous real-time learning that changes its alerting criteria as your business grows and adapts to reduce necessary detection engineering.
- Unlike some XDR solutions, we safeguard your data privacy by keeping the learning of your business separate from the learning of other enterprises. Darktrace's models are distinct to you.
- Chain anomalies together to reduce the time between detection and understanding.

Detection and Response to sophisticated, multi-domain threats

Our AI's visibility allows it to identify subtle behavioral anomalies that indicate a cyber-attack. Once these are detected, the AI can respond autonomously with precision to only neutralize the malicious activity. Since it understands your business, it allows normal, safe operations to continue, therefore maintaining security while minimizing business disruption.

/ NETWORK: Complete network detection from obfuscated downloads, C2, and encryption activity to privilege escalation, data gathering, and exfiltration. Take targeted actions including blocking matching network connections over exploited protocols and ports or enforce a workstation to halt unexpected activities.

/ EMAIL: Expose sophisticated spear-phishing, impersonation, supply chain attacks, and business email compromise, all mapped to subsequent application behaviors. Strip links, convert attachments, and hold emails entirely depending on the extent and nature of the threat. Even strengthen security around your users, boosting data loss prevention with AI that recognizes misdirected emails and improving efficiency with upcoming enhancements to user-reported phishing workflows.

/ CLOUD: Provide total cloud protection surfacing real-time threats and misconfigurations based on true cloud risk across your workloads, containers, and Kubernetes. Darktrace takes selective actions that account for careful cloud planning such as 'detaching user profiles' for those abusing their permissions.

/ IDENTITY: Gain advanced visibility of application user behavior from unusual authentication, password sprays, account takeover, resource theft, and admin abuse. Take targeted actions including the forced 'log-off' of a user or temporary disable an account to give the team time to verify legitimacy.

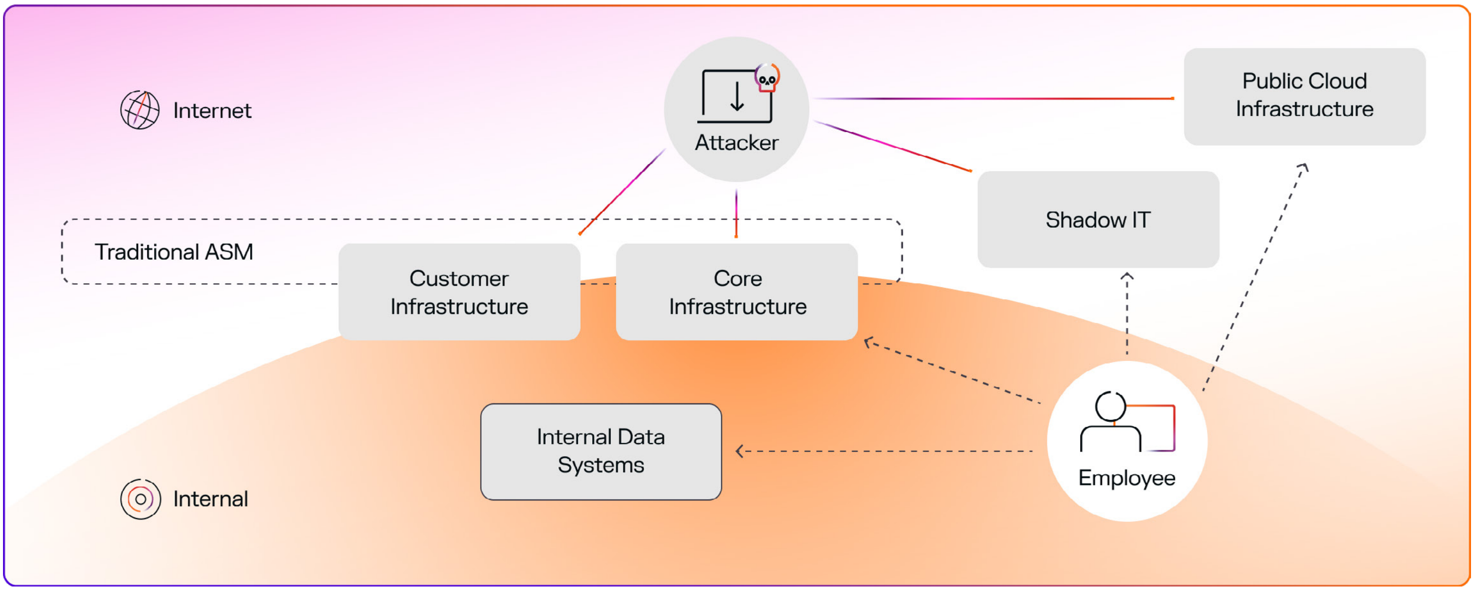
/ OT Industrial (OT): Understand anomalous behaviors occurring across over 50 diverse industrial protocols, including Modbus, S7, CIP and BACnet. Uniquely highlight threats where IT and OT converge, including unwanted communication or malicious peripherals.

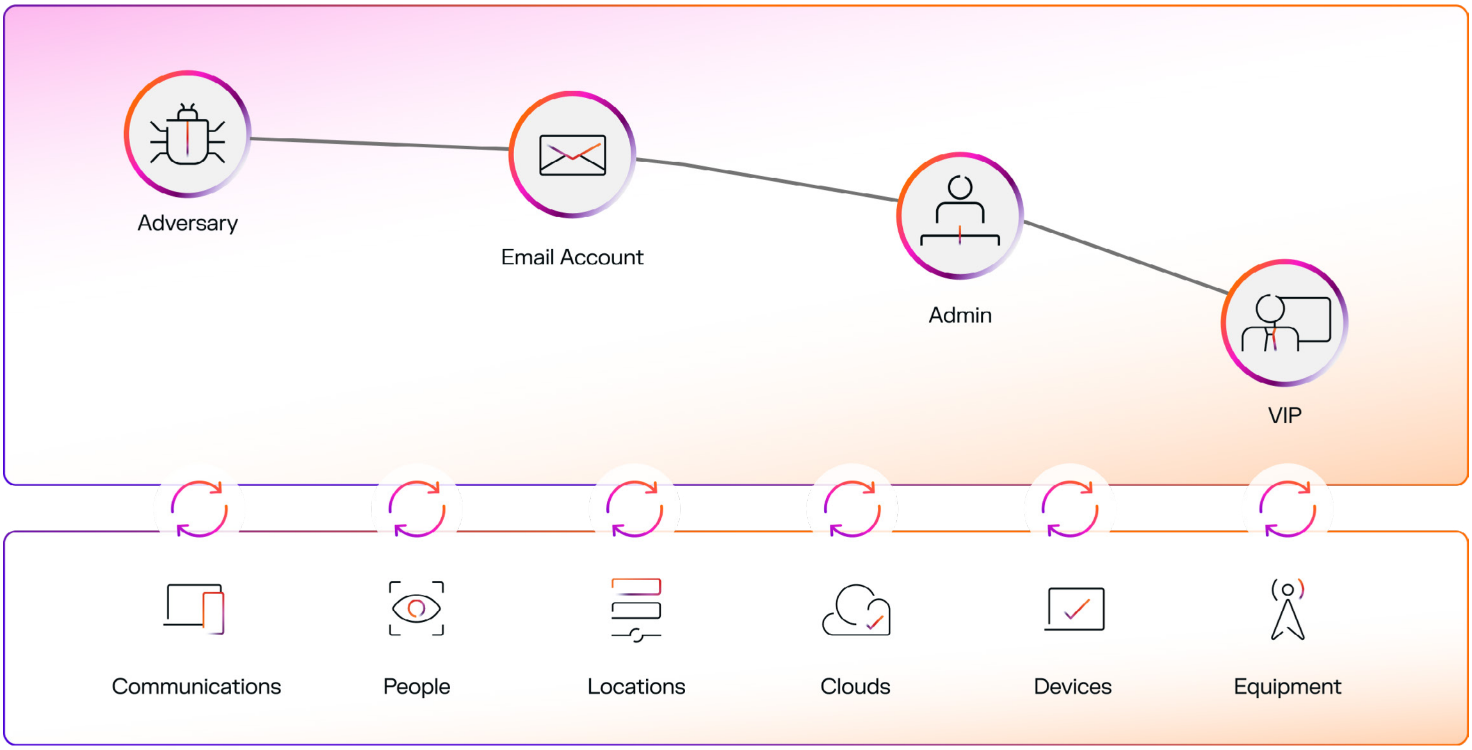
Autonomous responses contain threats before they escalate, easing the burden on the security team so it can focus on more than firefighting. Since the AI understands your business behaviors, it can take targeted actions that stop attacks while still allowing regular operations, therefore minimizing business disruption. All actions can be set to active or human confirmation modes, based on your needs in different times of the day, out of hours, or against certain threats.

Gain insights to achieve a proactive cyber defense

Use Darktrace / Attack Surface Management to surface hidden assets and prevent security control failures. Receive protection against shadow IT, brand abuse, cyber-squatting, and the latest vulnerabilities relevant to you with Darktrace's industry leading Newsroom.

With Darktrace / Proactive Exposure Management analysis, apply context and prioritization to possible risks and attack paths across each of your coverage areas, based on a joint understanding of probability, patch latency, interactivity of involved assets, position in business or security hierarchy, and the difficulty of likely attack methods. Users can take this context and then review individual devices for vulnerabilities to prevent attack paths from being exploited.





The Darktrace ActiveAI Security Platform delivers cyber resilience across every stage of the attack lifecycle and protects your data wherever it resides

* This figure was derived by summing the estimated time a human analyst would take to view and comprehend the results of all the data gathering calls that AI Analyst made during its investigations.

Drastically reduce investigate time with Cyber AI Analyst

Our investigative AI, Cyber AI Analyst, goes beyond a typical XDR. Using these products, the existing triage process becomes overwhelming, with both a data and human overload. Under time sensitive conditions, analysts must use multiple capabilities to filter through countless alerts, identify meaning, extract implications, and sort out false positives.

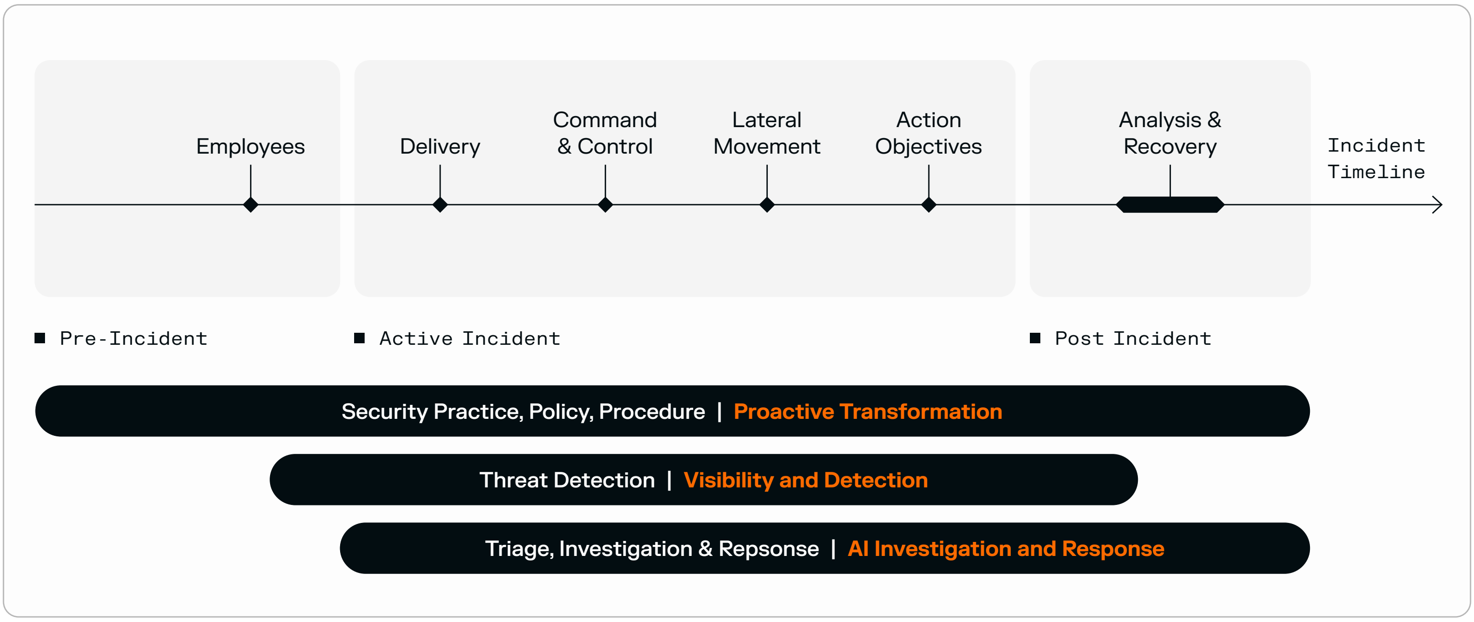
Cyber AI Analyst takes that pressure away. It automatically investigates every relevant event, reducing thousands of individual alerts into only a few incidents that require review.

From here, analysts have everything they need to decide next steps, validate containment actions, or see the steps they need to take to recover. This redefined process is more thorough, reducing the human incident handling process to minutes while behavioral containment stops the threat within seconds, giving your team more time to spend on their proactive security posture

Investigation results are mapped to an incident timeline and come with a complete narrative containing the threat details and recommendations for mitigation or recovery. Organizations can tailor how an investigation is performed to ensure consistency and alignment with their own internal policies and workflow.

Based on internal research, when analyzing 30 alerts a day, Cyber AI Analyst typically provides a SOC with the equivalent of 5,000 additional hours (or ~3 Full Time Employees) of Level 2 analysis and written reporting annually. This can be scaled to far more as needed, enriching security operations by producing high level incident alerts with full details so that human analysts can focus on Level 3 tasks.

■ Internal Darktrace Research


Employees
Delivery
Command & Control
Lateral Movement
Action Objectives
Analysis & Recovery
Incident Timeline
■ Pre-Incident
■ Active Incident
■ Post Incident
Security Practice, Policy, Procedure | Proactive Transformation
Threat Detection | Visibility and Detection
Triage, Investigation & Repsponse | AI Investigation and Response

AI-assisted readiness and recovery

Darktrace / Incident Readiness & Recovery boosts your incident readiness across each element of security operations: your people, processes, and technologies.

Give your security team confidence with incident simulations, allowing SOC teams to overcome human stress responses by practicing with realistic attack drills in their own environments.

Understand where your security and IT technologies can improve their potential with simple readiness reporting that audits your stack, integrations, and what could pose a risk during the real incident response process.

Speed up critical decision-making time with AI-generated playbooks that give SOC teams the optimal steps to recovery based on active investigations in your environment.

Scale and succeed with Darktrace Services

Darktrace offers a range of services to ensure your team is supported with additional expertise and scalability.

Darktrace Managed Threat Detection: will augment your team's investigation efforts by letting our own SOC triage the highest priority alerts in your environment and jumpstart the threat response. In a time where analysts are overburdened by responsibilities, we bring additional support and experience when you most need it.

Darktrace Security Operations Support: grants your team access to world-class cyber security analysts for guidance through any emerging problem- from incident explanations during live threat investigations to questions around Darktrace technologies.

Darktrace Managed Detection & Response service brings the maximum level of support, with our experts' facilitating SOC triage and a level of threat containment response, regular reviews of operational efficiency, communication about Darktrace's latest threat research findings, and unlimited collaboration. Together, these provide focus areas to build up the customer's overall resilience.

Operational benefits

A security stack that stacks
Ingest and correlate platform-native data along with telemetry from your existing third-party tools to maximize ROI and see your complete security profile within one UI, spanning from proactive prevention to reactive response

Accelerate response time to stop attacks in their tracks
Autonomously identify and contain known, unknown, and never seen threats, before they escalate with targeted actions for every incident

Eliminate alert triage with automated investigations and expand your SOC capacity
Free your security team from the pressure of triage and manual detection engineering

Preventative cyber resilience helps you close gaps before they are exploited
Proactive tools allow you to harden your security stack, reduce real alerts, and predict the next likely stages of an attack

Follow your own path and deploy at your own pace
Add capabilities at-will to address your scaling security needs

Deployment

Delivery Model

- On-Prem
- Private Cloud
- Hybrid.

Additional options for specific platform areas:

- Darktrace/NETWORK and Darktrace/OT can be deployed:
- On-Prem
- Private Cloud
- Hybrid
- Darktrace/CLOUD deployed Agentless, Agented, or Hybrid
- Darktrace/EMAIL deployed with API or Journaling and API

Darktrace portfolio

- **Email Security**
- **Cloud Security**
- **OT/CPS**
- **ASM**
- **Network, Detection and Response**

Adoption

At its core, the Darktrace ActiveAI Security has five core coverage areas, with additional coverage, services, and capabilities offered to expand your protection depending on your organization's security needs.

Darktrace / NETWORK
Network Detection and Response

Darktrace / OT
Operational Technology Security

Darktrace / EMAIL
Cloud Email Security

Darktrace / CLOUD
Cloud Detection & Response Cloud Native Application Protection

Darktrace / IDENTITY
Identity Threat Detection and Response in Applications

Through Darktrace's accessible proof of value trials, businesses can experience any Darktrace product in their own environments and participate in detailed workshop sessions with our specialists.

New customers
Darktrace offers multiple entry points to the Darktrace AI Security Platform starting with our core coverage areas / NETWORK, / OT, / EMAIL, / IDENTITY and / CLOUD - which includes Real-time Threat Detection, Autonomous Response & Cyber AI analyst capabilities

From here, expand your protection by adding to your coverage with additional domains, services, and cross platform products like Attack Surface Management, Proactive Exposure Management and Incidence Readiness & Recovery.

Existing customers
To experience the capabilities of Darktrace ActiveAI Security, Darktrace recommends at least the following products, / NETWORK, / EMAIL or / CLOUD, Attack Surface Management, Proactive Exposure Management and Incidence Readiness & Recovery.

■ 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.

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