DARKTRACE

Darktrace / NETWORK

The Industry's Most Advanced Network Detection and Response (NDR) Solution, Powered by Self-Learning AI.

Network Complexity on the Rise

Modern networks are expanding far beyond on-premises into virtual environments, cloud and hybrid networks. More than 50% of incidents will come from cloud network activity by 2029 [1], meaning defenders need a solution that can level the playing field against complex attacks that traverse multiple areas of a digital estate, including north-south and east-west traffic.

With 63% of employees working remotely or on a hybrid basis [2], the need to maintain network visibility over remote worker devices is increasingly important, however this is not something other NDR or EDR tools cover.

Old tools are blind to new threats

Most NDR vendors and network security tools such as IDS/ IPS rely on detecting known attacks with historical data and supervised machine learning, leaving organizations vulnerable to novel threats such as zero-days, variants of known attacks, supply chain attacks and insider threats.

This legacy approach means that at least one organization needs to be 'patient zero' - the first victim of a novel attack – before it can be detected elsewhere. Other NDR vendors also apply models that are trained globally and are not unique to each organization's environment, creating a high number of false positives and alerts that lack business context.

SOC teams are under pressure

Over 70% of SOC analysts report that they are experiencing burn-out [3], therefore it is necessary for organizations to leverage new approaches for combating network threats to reduce the pressure on their security team without compromising on security outcomes.

With 57% of organizations reporting that their SOC aggregation and correlation capabilities need improvement [4], SOC teams need to consider alternative solutions such as investigative AI to ease the burden on analysts, reduce alert fatigue and transform their network security operations to a more proactive state.

1 Gartner Market Guide for Network Detection and Response, 2024.
2 McKinsey Global Institute, 2023
3 Tines - Voice of the SOC Analyst, 2022
4 Gartner Peer Community One-Minute Insights - Modern Security Operations Center (SOC) Strategies, 2023

Key Capabilities of Darktrace / NETWORK

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

Business benefits

Increase operational efficiency
With Self-Learning AI that autonomously tunes itself, surfacing critical alerts, and removing the hassle of manual tuning.

Reduce the pressure on security teams
By leveraging Cyber AI Analyst. Operating like a human analyst, it automates investigations and reduces triage time.

Extend AI to your existing workflows
With hundreds of third-party integrations including firewalls, EDR, ZTNA, SIEM, SOAR, and ITSM solutions.

Stay in full control
With advanced customization options and response actions based on device types, IP ranges, office working hours and countless other parameters.

Go beyond NDR
By proactively preventing cyber-attacks and strengthening your security posture with the Darktrace ActiveAI Security Platform.

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

Gain full network visibility

Darktrace / NETWORK passively ingests network traffic from on-premises, virtual, cloud, hybrid environments and remote devices – extracting datapoints and analyzing both encrypted and decrypted packets from every connection to uncover unusual activity in real-time. Unlike other NDR vendors that process your data in the cloud as part of globally trained models, our industry leading Self-Learning AI is deployed locally and trained solely on your data without the need for a cloud connection - giving you tailored security outcomes without compromising on privacy.

Detect known and unknown threats

Darktrace / NETWORK takes a fundamentally different approach to other NDR vendors, detecting threats without relying on known malware signatures, external threat intelligence or historical attack data. Our Self-Learning AI learns what is normal for your network, detecting anomalous activity plus known and novel threats. Every connection in your network is continuously analyzed, mapped and modeled for a full picture of your devices, identities, connections and potential attack paths.

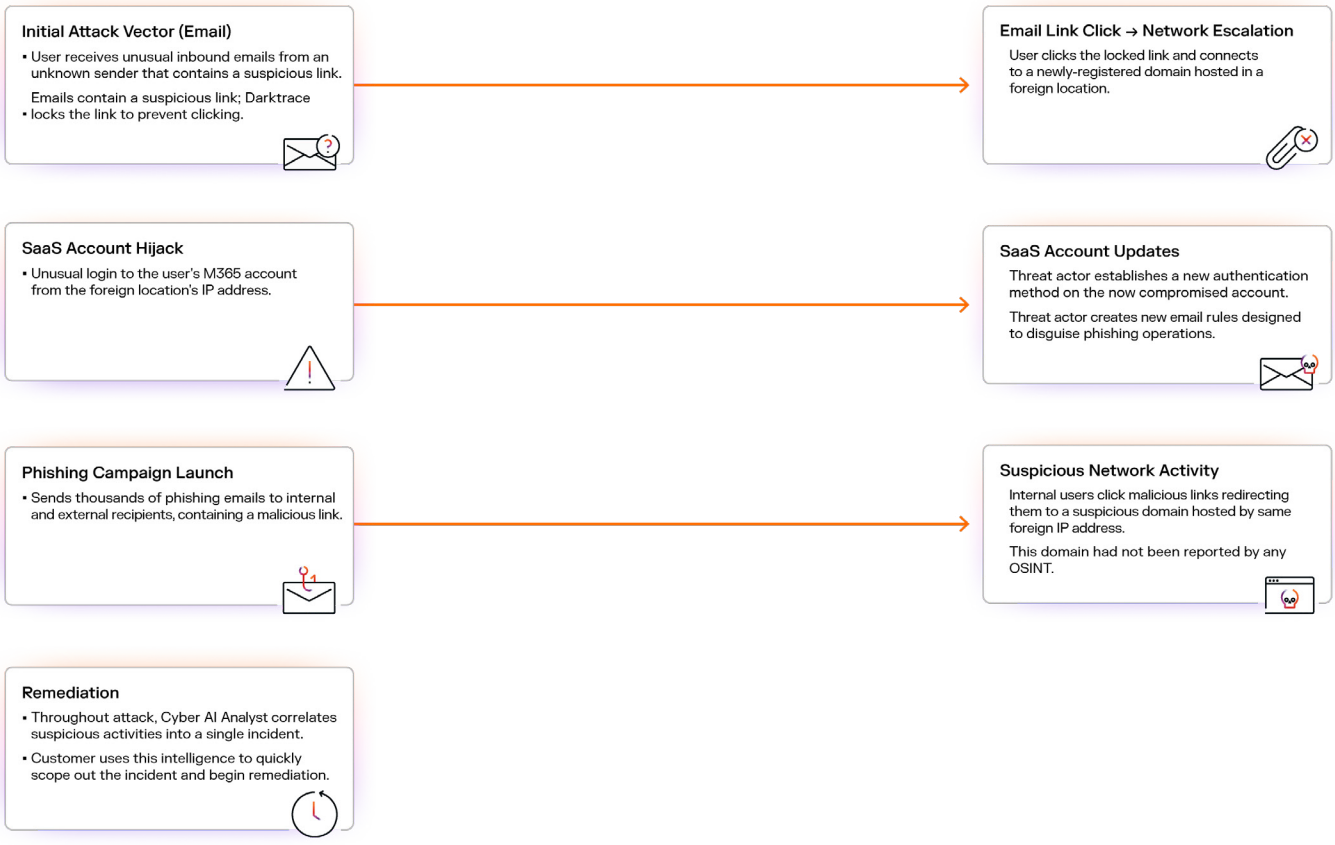
Our Self-Learning AI identifies any network behavior that could cause business disruption, providing unprecedented business context compared to packet sampling tools such as IDS/IPS and shining a light on both external and internal threats, from zero-days to supply chain attacks and insider threats.

Precision threat detection

Darktrace Self-Learning AI autonomously optimizes itself to cut through the noise and quickly raise genuine, prioritized network security incidents to your attention – significantly reducing false positives and saving you the hassle of continually tuning alerts manually. If desired, you can still maintain full control of your deployment and oversee how the output of our AI is processed with an intuitive model editor. Advanced users can directly change or disable every setting and create custom detections with ease and no need for costly development.

Detection Model Examples

Darktrace / NETWORK provides coverage for all 14 MITRE ATT&CK categories, detecting threats at every stage of the attack lifecycle without relying on historical data, static rules or signature-based methods. Here are just a few examples of the detection models that Darktrace / NETWORK can use to identify relevant anomalous behavior and threats in your network.



Internal Reconnaissance

- Device / Suspicious SMB Scanning Activity
- Device / Network Scan
- Device / RDP Scan
- Device / ICMP Address Scan
- Device / Suspicious Network Scan Activity other NDR providers.

Lateral Movement

- Device / Multiple Lateral Movement Model Breaches
- Anomalous Connection / Unusual Admin RDP Session
- Device / SMB Lateral Movement
- Compliance / SMB Drive Write

C2 Communication

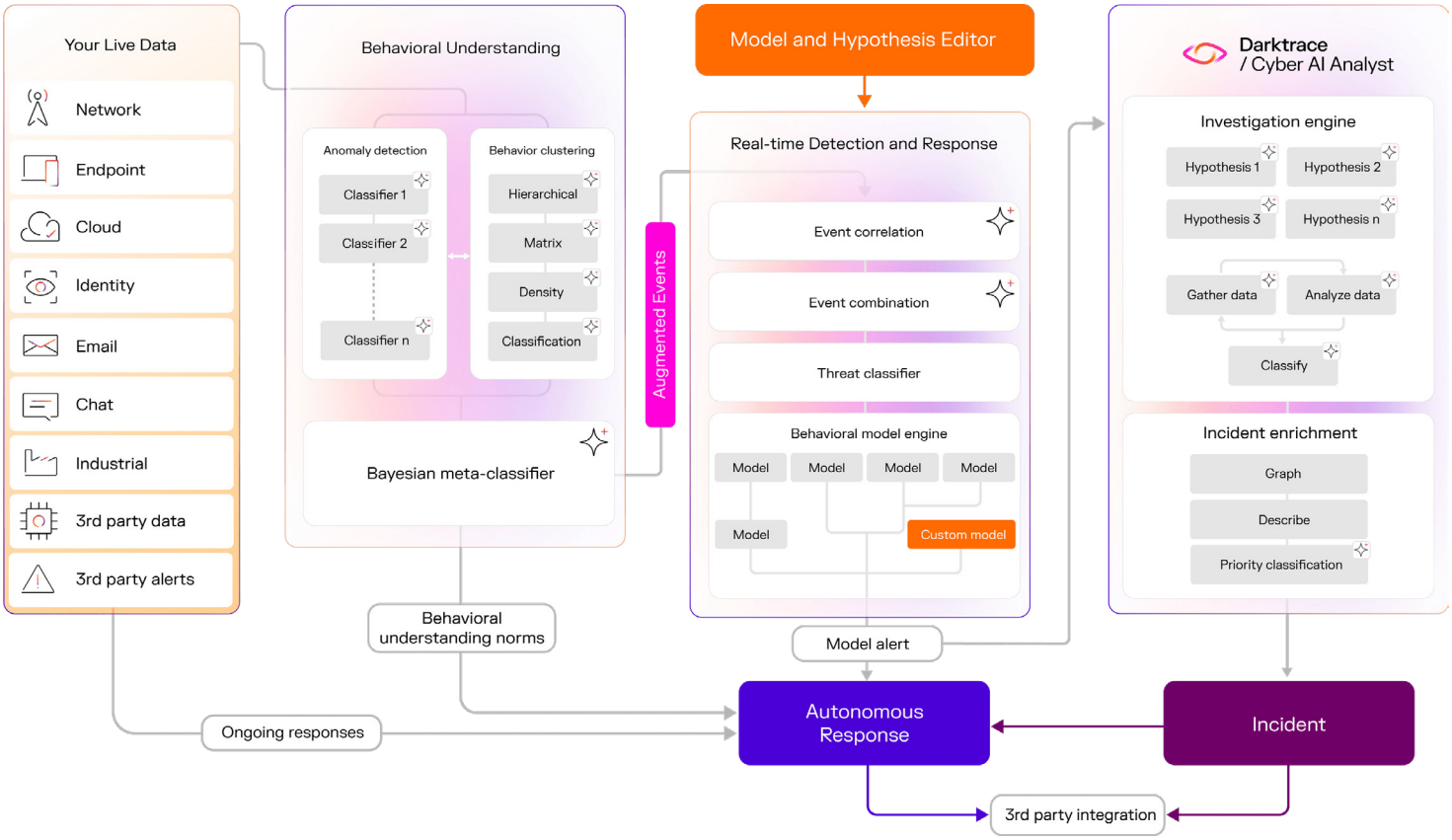
- Anomalous Server Activity / Outgoing from Server
- Anomalous Connection / Multiple Connections to New External TCP Port
- Anomalous Connection / Rare External SSL Self-Signed
- Device / Suspicious Domain

Exfiltration

- Unusual Activity / Enhanced Unusual External Data Transfer
- Anomalous Connection / Data Sent to Rare Domain
- Unusual Activity / Unusual External Data Transfer
- Compliance / FTP / Unusual Outbound FTP

Accelerate Investigations

With the Industry's First AI Analyst



Darktrace / NETWORK

Darktrace / NETWORK leverages the power of Cyber AI Analyst, bringing cognitive automation to your data, drastically reducing triage times.

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, reducing triage time.
- **Continuously analyze** and contextualize every relevant alert in your network.

By developing 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

- **Investigate** all network alerts and connect seemingly benign events, uncovering sophisticated threats and correlating related activities into a single incident.
- **Piece together** network anomalies which may appear harmless, helping discover advanced network threats across the entire kill chain, in real-time, and at scale.

With this approach Darktrace / NETWORK quickly uncovers zero-day attacks & insider threats, preventing your business from becoming patient zero.

Get complete business context

- **Correlate** alerts from across your environment including network, endpoints, cloud, OT, email, identities, and remote devices all into a single view.
- **Combine** your existing EDR with Darktrace / NETWORK and Darktrace / CLOUD to build a more effective XDR than EDR-first vendors can offer.
- **Extend** protection with the Darktrace ActiveAI Security Platform, adding proactive defense and automated recovery across your digital estate.

Neutralize Network Threats with the First Autonomous Response Solution Proven to Work in the Enterprise

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

At a glance:

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

Autonomous threat response

Darktrace / NETWORK 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 / NETWORK is the only NDR solution that can autonomously enforce a pattern of life based on what is normal for a standalone device or group of peers. Darktrace / NETWORK autonomously takes precise response actions in real-time to contain threats without disrupting business operations - either natively or via third party integrations. Actions can also be taken for remote user devices when combined with Darktrace / ENDPOINT, no matter where the endpoint is or whether they are off the corporate network.

Stay in full control

Darktrace / NETWORK autonomously takes the most effective response to network threats with little to no maintenance required and minimal initial setup. While most clients utilize our default response actions, you can still fully customize or create entirely bespoke response logic if desired. Make precise adjustments based on device types, IP ranges, office hours and various other parameters.

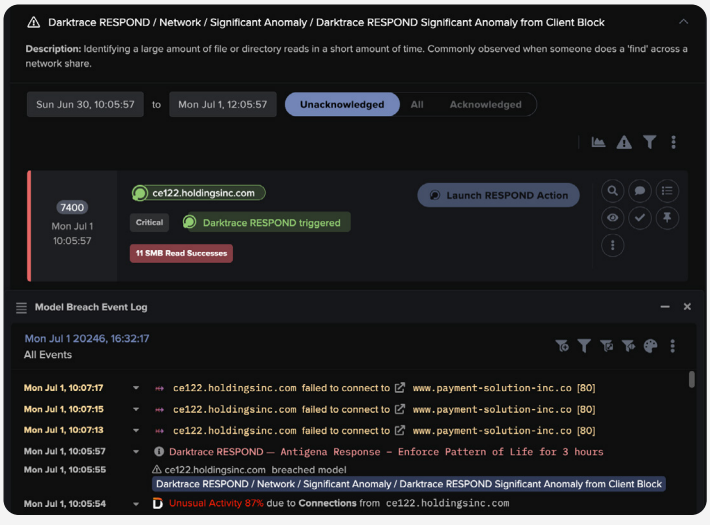


Figure 01: Get full visibility of the events leading up to an incident, including how our AI autonomously responds to protect your business.

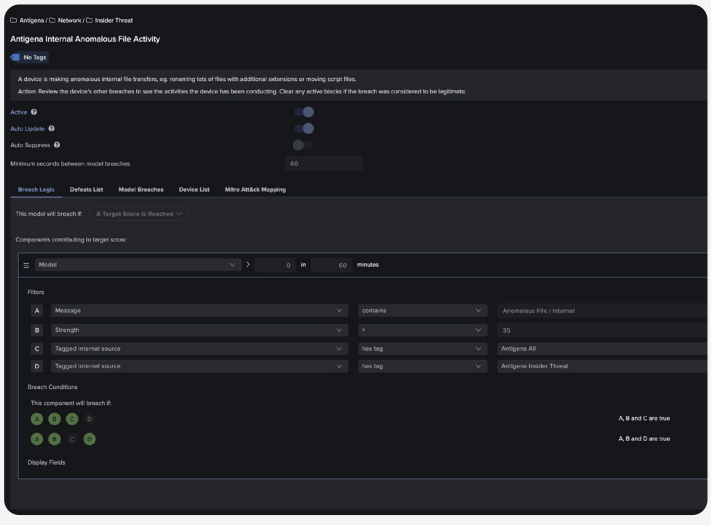


Figure 02: An example of the Darktrace Model Editor, which provides the ability to fine-tune response logic in granular detail if desired.

Industry leading NDR powered by Self-Learning AI

Detection
Detect known and novel threats across your entire network with Self-Learning AI that understands what is normal for your organization. Get full visibility and threat detection capabilities across your on-premises, cloud, hybrid and virtual environments, including remote worker endpoints.

Investigation
Leverage the power of Cyber AI Analyst to continually investigate and contextualize every relevant alert in your network. Cyber AI Analyst autonomously forms hypotheses and reaches conclusions just like a human analyst would, transforming your SecOps and going far beyond the capabilities of other NDR providers.

Response
Our Self-Learning AI autonomously responds to both known and novel threats in real-time, taking precise response actions based on a contextual and behavioral understanding of your organization to contain threats without impacting business operations.

Business benefits

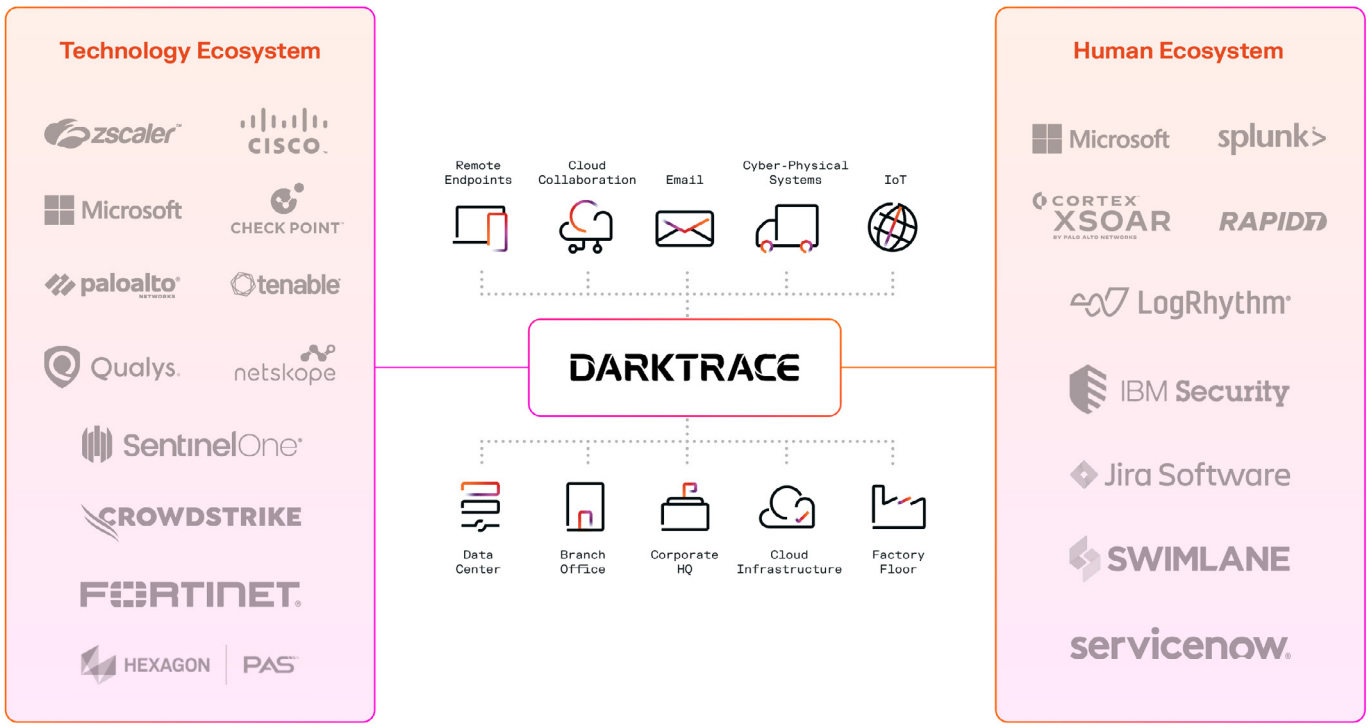
Protect your business
against known and novel threats in real-time, without relying on historical attack data, threat intelligence or a cloud connection.

Gain full network visibility
across on-premises, virtual, cloud, hybrid networks, including remote devices.

Augment your SOC team with AI
that automates the investigation and triage of security incidents at machine speed, saving a significant amount of time and resources.

Avoid business disruption with an autonomous response solution
that uses a contextual understanding of your business to take precise actions and contain threats in real-time, without impacting business operations.

Unify insights across your business
by contextualizing data from your network, cloud, identities, OT devices, email, endpoints, third party intelligence in a single solutions.



Integrating across the enterprise

Extend our AI to your existing tools

With hundreds of native integrations and an open API architecture, there's no need for complex and costly development. Darktrace / NETWORK takes targeted, native response actions to disarm threats in seconds while also integrating with third party firewalls, ZTNA, SIEM, SOAR and ITSM solutions to extend response capabilities to your existing technology stack. Alerts can be sent wherever needed to complement your existing workflows.

Darktrace / NETWORK also integrates with all major EDR providers such as Microsoft Defender, CrowdStrike and SentinelOne, contextualizing endpoint alerts with telemetry from rest of your environment to detect, investigate and respond to incidents more effectively.

Deploying Darktrace / NETWORK

From on-premises locations to hybrid cloud and virtual environments, Darktrace / NETWORK can be deployed for any type of network and for even the most complex or bespoke enterprise configurations.

Response actions can be taken either natively via Darktrace or via integrations with third party firewalls, EDR, ZTNA, SIEM, SOAR and ITSM solutions.

Deployment options

Analysis

Darktrace can be deployed in many ways to provide full visibility into your physical and virtual networks. Each deployment starts with the provision of a nominated 'master' instance of Darktrace, which can be deployed as a virtual instance or as a physical hardware appliance. 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 network locations. Where required, Darktrace / NETWORK can also be deployed using a hardware appliance that sits parallel to your network and passively ingests raw network traffic. This is typically achieved by connecting the Darktrace appliance to your core switch using a SPAN session. 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' across your network, which can be virtualized or physical. 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 scenario, 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. Your Darktrace representative can advise on the most appropriate deployment solution for your environment, especially for larger and/or distributed network configurations. Darktrace / NETWORK also collects data from host-based Client sensors that are deployed as part of Darktrace / ENDPOINT, integrated third-party services (such as SaaS or cloud applications) or from connected Darktrace products such as Darktrace / EMAIL, Darktrace / IDENTITY and Darktrace / CLOUD.

OT

Bring the detection and response capabilities of Darktrace / NETWORK to your operational technology (OT) devices. Darktrace / OT natively covers IT and OT providing visibility of OT, IoT, and IT assets in unison. Darktrace / OT is deployable in isolation and air-gapped environments without the need for any external connectivity, achieving greater visibility of OT and IT devices across all levels of the Purdue Model.

Extend Self-Learning AI Across the Enterprise

The ActiveAI Security Platform

Operational technology

Industry recognized solution for identifying IT & OT convergence.

Cloud

Extend detection and response capabilities to your hybrid cloud environment and gain complete enterprise coverage with Darktrace / CLOUD.

Email

Context aware email protection, beyond the inbox that seamlessly connects email and network telemetry.

Endpoint

Darktrace Network Endpoint eXtended Telemetry (NEXT) is revolutionizing NDR with the industry's first mixed-telemetry agent using Self-Learning AI.

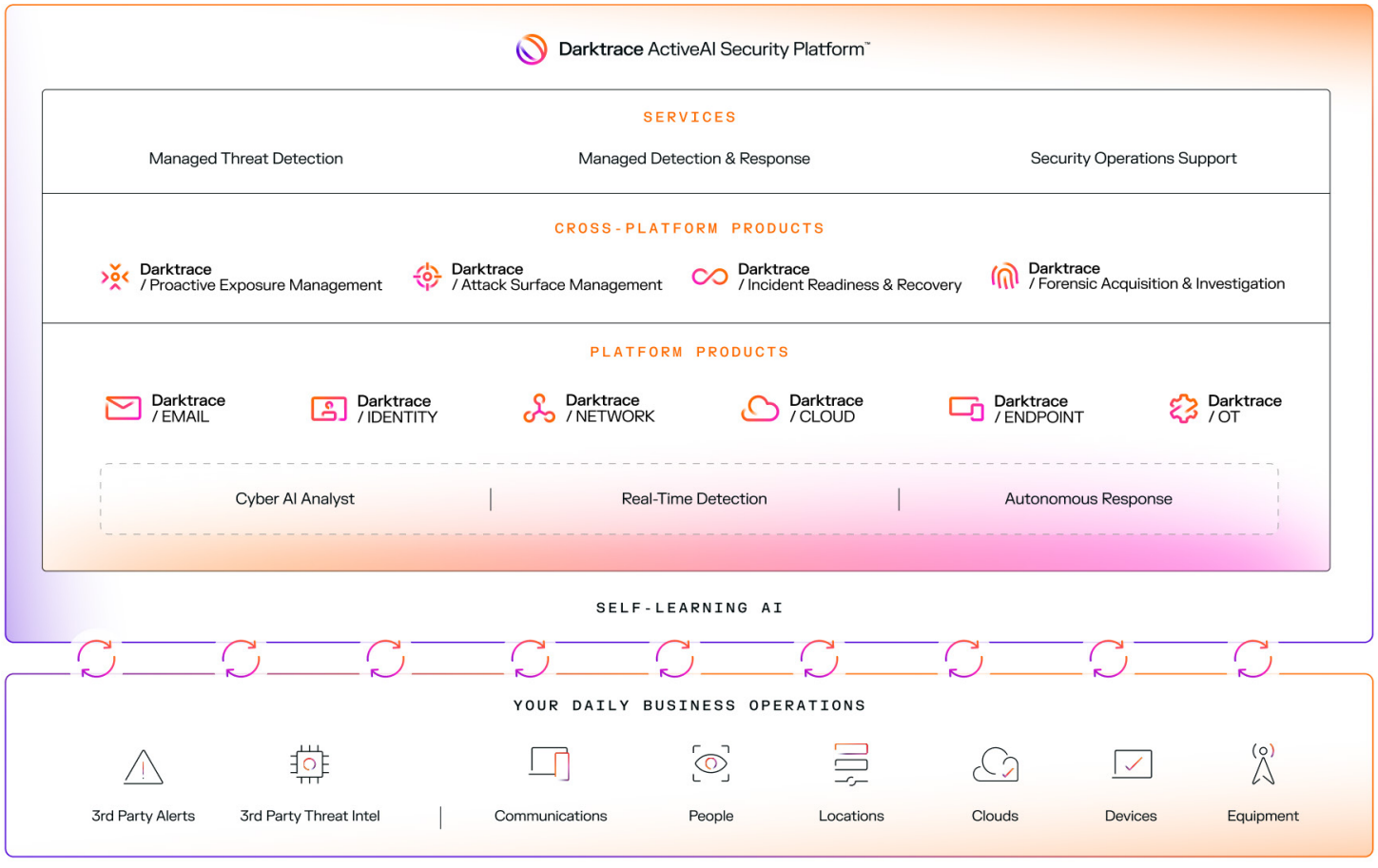
Gain insights to get ahead of threats

Darktrace / NETWORK 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

Helps 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.



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