DARKTRACE

Darktrace
/ ENDPOINT

Combat Known and
Unknown Endpoint Threats
with Self-Learning AI.

Maintaining visibility
of remote devices

With 63% of employees working remotely or on a hybrid basis[1], the need to maintain network visibility over remote worker devices off the corporate network or VPN is increasingly important, however this is not addressed by most Network Detection and Response (NDR) or Endpoint Detection and Response (EDR) solutions.

Relying solely on solutions like EDR or XDR that are based on process-level endpoint telemetry leaves blind spots for organizations. Without native network visibility, these solutions miss attacks that evade traditional detection rules and traverse multiple areas of a network.

Old tools are blind to new threats

Previously unseen threats and targeted attacks are often missed or detected too late by EDR solutions because of their reliance on historical attack data and external threat intelligence. This focus on 'known bad' means that these tools are unable to detect novel network attacks and other threats such as malicious insiders, supply chain attacks, data exfiltration and 'living off the land' attacks.

Existing solutions also lack the ability to take targeted response actions for network threats affecting endpoint devices. This can often result in the whole endpoint being quarantined to contain threats, causing disruption for the user and the business. Organizations need a solution that can take effective and targeted responses at machine speed to contain threats while maintaining normal business operations.

SOC teams under pressure

Over 70% of SOC analysts report that they are experiencing burnout[2], therefore it is necessary for organizations to leverage new approaches for combating cyber 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[3], SOC teams need to consider alternative solutions such as investigative AI to ease the burden on analysts, reduce alert fatigue and transform their security operations to a more proactive state.

1 McKinsey Global Institute, 2023.
2 Tines - Voice of the SOC Analyst, 2022
3 Gartner Peer Community One-Minute Insights - Modern Security Operations Center (SOC) Strategies, 2023

Elevate your endpoint defenses with Self-Learning AI

Detection

Detect known and novel network threats across your endpoint devices with Self-Learning AI that understands what is normal for your organization. Extend network visibility and threat detection capabilities to your endpoints and remote worker devices without relying on signatures or historical attack data.

Investigation

Leverage the power of Cyber AI Analyst to continually investigate and contextualize every network alert affecting your endpoints. Cyber AI Analyst autonomously forms hypotheses and reaches conclusions just like a human analyst would, transforming your SecOps and enhancing your teams.

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, signatures, threat intelligence or a cloud connection.

Gain full network visibility
across all your endpoints and remote devices, including users that are off-VPN.

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 endpoints, network, cloud, email, identities and OT devices in a single solution.

Key capabilities of Darktrace / ENDPOINT

Detect Known and Novel Network Threats Across Your Endpoints

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

Gain full visibility

Darktrace / ENDPOINT uses lightweight agents to analyze datapoints from every network packet and connection to uncover unusual activity in real-time, including remote devices or if users are off-VPN.

Unlike other 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 / ENDPOINT takes a fundamentally different approach to other security vendors, detecting threats without relying on known malware signatures, external threat intelligence or historical attack data. Our AI learns what is normal for your network, detecting anomalous activity plus known and novel threats.

Every endpoint connection in your network is continuously analyzed, mapped and modeled for a full picture of your devices. Our Self-Learning AI identifies any behavior that could cause business disruption, complementing your existing endpoint detection and response (EDR) solution to shine a light on internal and external threats, from zero-days to supply chain attacks and insider threats.

Precision threat detection

Darktrace Self-Learning AI autonomously Darktrace Self-Learning AI autonomously optimizes itself to cut through the noise and quickly raise genuine, prioritized 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.
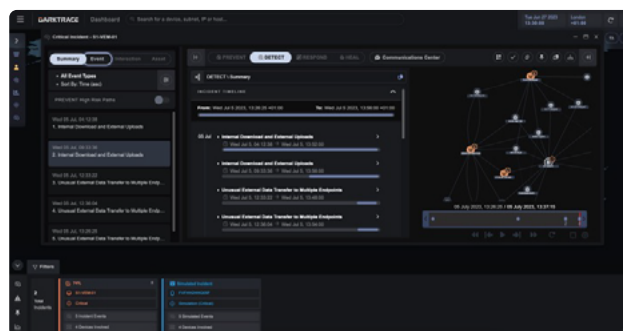

Figure 01: Darktrace / ENDPOINT learns what is normal network behavior for endpoint devices, detecting any anomalous activity and prioritizing anything that could cause business disruption.

Detection model examples

Darktrace / ENDPOINT provides coverage for all 14 MITRE ATT&CK categories, detecting network threats affecting your endpoints 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 / ENDPOINT can use to identify anomalous behavior and threats in your network.
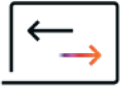
Lateral movement

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

File encryption

Compromise / Ransomware / Suspicious SMB Activity

Anomalous File / Internal / Additional Extension Appended to SMB File

Anomalous Connection / Suspicious Read Write Ratio

Compromise / Ransomware / Possible Ransom Note Write

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

"Darktrace is real AI. The system really trains itself, I never have to interact with any of the models. The system is astonishingly accurate."

■ **Josef Buttinger**
Corporate IT & Security Manager,
EV Group

Darktrace / ENDPOINT

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

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

Cyber AI Analyst continually analyzes and contextualizes every relevant 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 network, connecting seemingly benign events to uncover sophisticated threats and correlating related activities into a single incident. By piecing together endpoint anomalies which may appear harmless, Cyber AI Analyst autonomously identifies subtle malicious actions and uncovers advanced threats, tracking them across the entire kill chain in real-time and at scale.

This comprehensive approach to network investigations enables Darktrace / ENDPOINT to quickly uncover zero-day attacks, insider threats and much more, preventing your business from becoming patient zero and providing a far superior outcome compared to solutions that only focus on 'known bad' behavior.

Get complete business context

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

Add your existing EDR to Darktrace / ENDPOINT, 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.

"Self-Learning AI investigates behavior on the endpoint alongside behavior in Microsoft 365 and across our entire cloud environment."

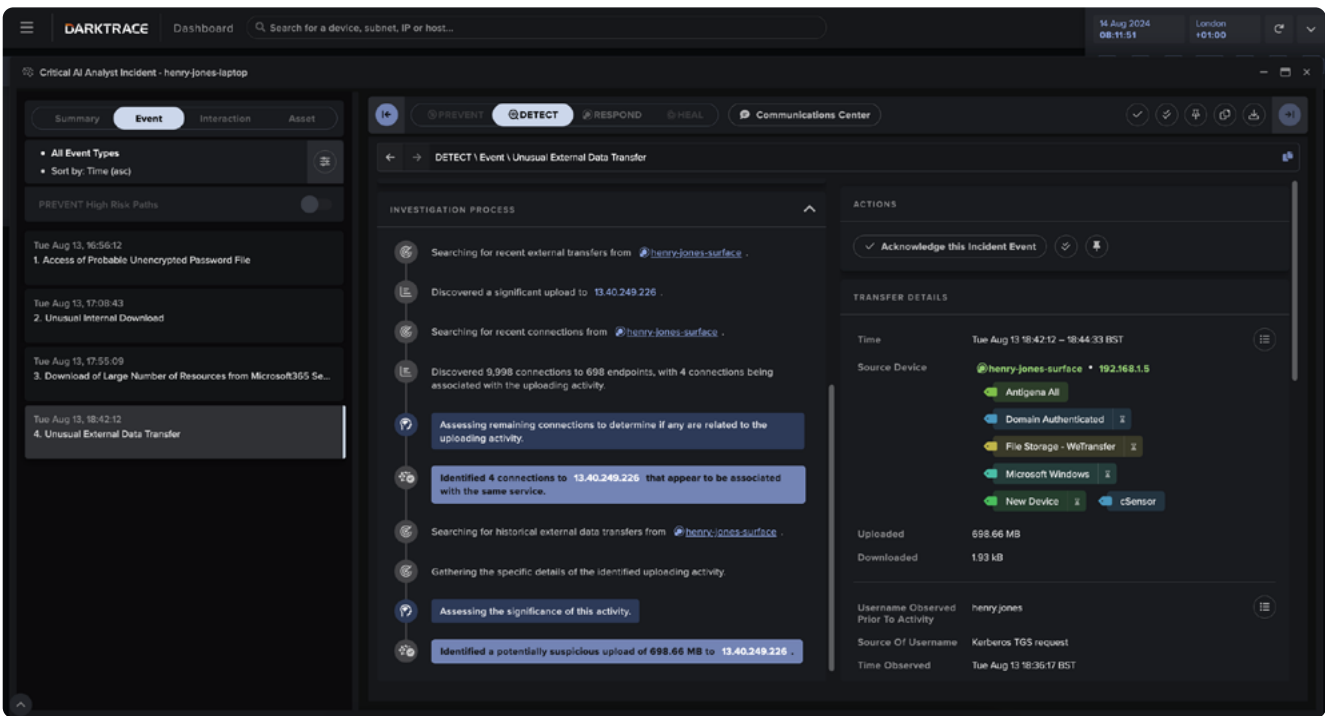■ **Terry Wright**
Head of IT Infrastructure,
Scope Markets

Figure 02: Cyber AI Analyst continually analyzes and contextualizes every relevant alert in your network affecting your endpoints 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.

Contain endpoint 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

- Harness the power of Cyber AI Analyst
- Augment your SOC team
- Automate alert triage and investigation
- Detailed network forensics
- Complete business context

Autonomous threat response

Darktrace / ENDPOINT 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 / ENDPOINT autonomously takes precise response actions in real-time to contain threats without disrupting business operations - either natively or via third party integrations. Actions can be taken for remote user devices no matter where the endpoint is or whether they are off the corporate network.
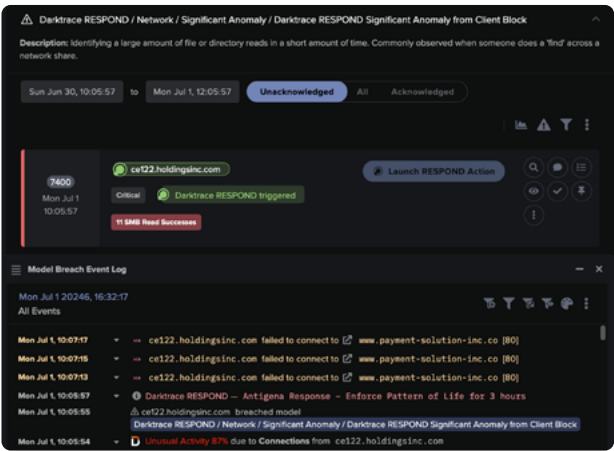
Stay in full control

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

If you'd still prefer to adjust response actions yourself, you can easily customize them with our intuitive model editor. Tweak 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: Get full visibility of the events leading up to an incident, including how our AI autonomously responds to protect your business.
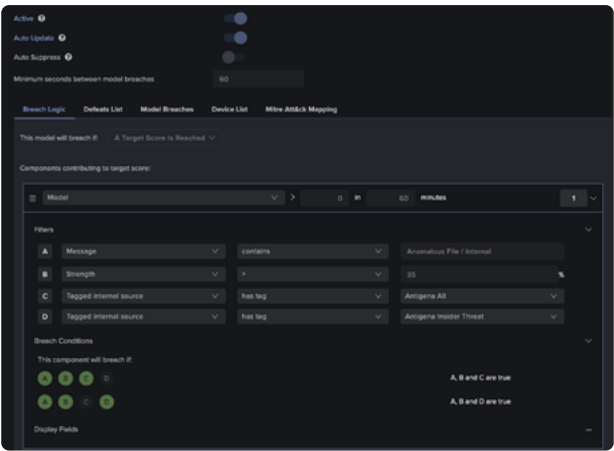

Figure 04: An example of the Darktrace Model Editor, which provides the ability to fine-tune response logic in granular detail.

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

"We feel safer knowing that Autonomous Response is monitoring and responding to all of these findings even when our team is unavailable."

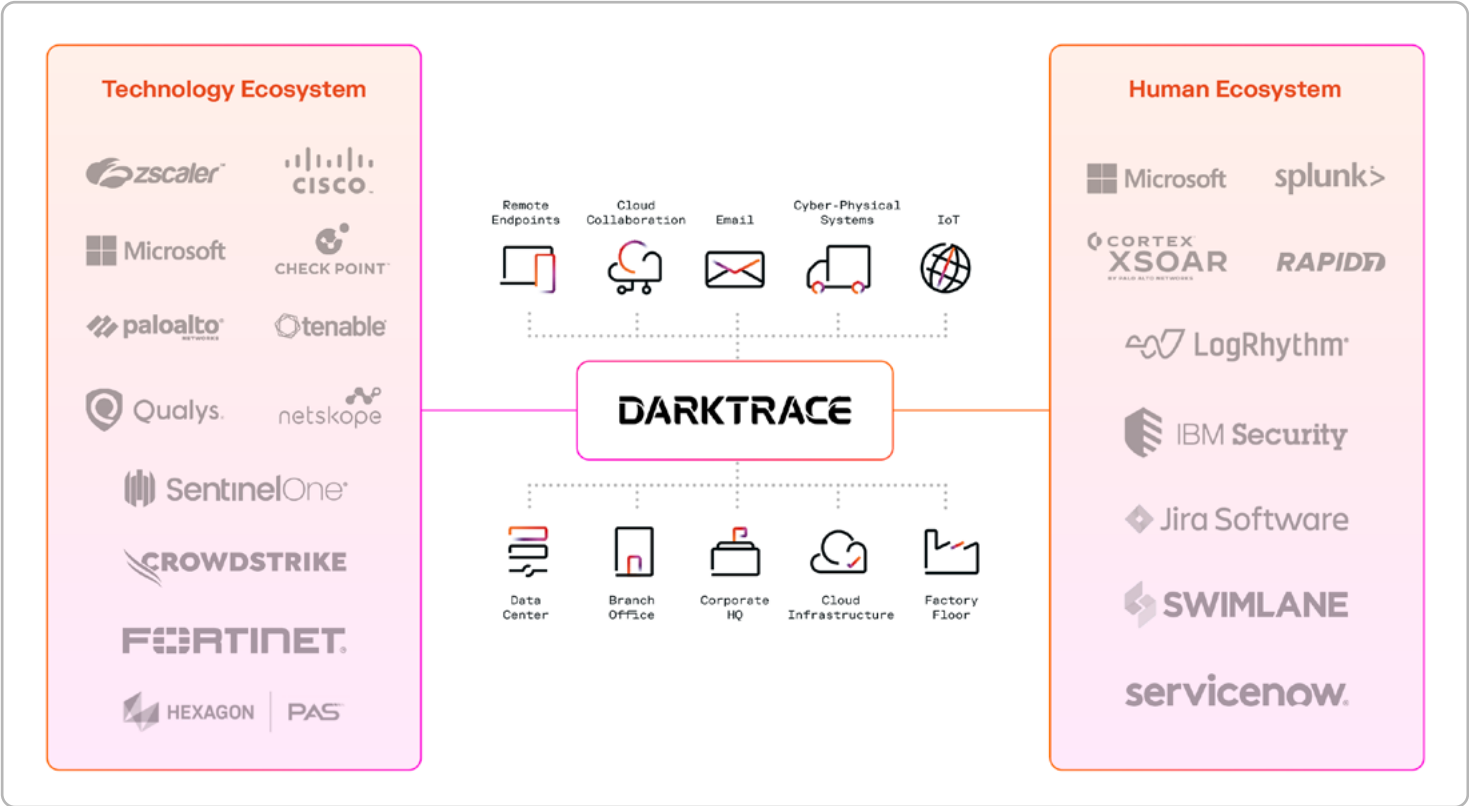■ **Richard Robinson**
Network Administrator // LSUA

Figure 05: Examples of the hundreds of native integrations that you can use with Darktrace to facilitate threat detection, investigation and response actions, as well as operational workflows.

Stay in the loop with the Darktrace Mobile App

The Darktrace Mobile App provides a streamlined user interface for on-the-go investigation and response, wherever you are.

Investigate anomalous endpoint activity that has been detected, approve autonomous response actions pending human confirmation, share alerts with colleagues and be notified when critical AI Analyst incidents are created.

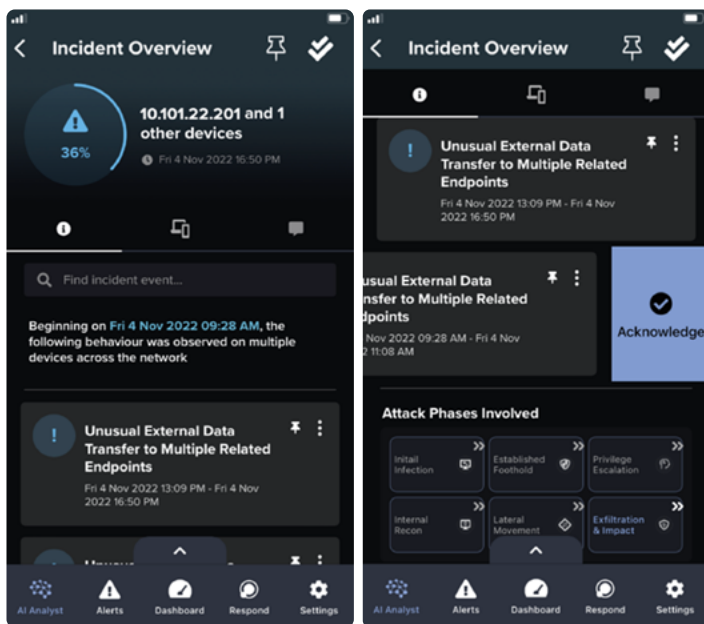The Darktrace Mobile App is available for Android and iOS.

Figure 06: An example of the Darktrace Mobile App interface.

Deploying Darktrace / ENDPOINT

The Darktrace / Endpoint cSensor agent extends network visibility, detection and response capabilities to your endpoint devices. This can include remote working devices and those that cannot be seen adequately using bulk network traffic mirroring or existing Darktrace sensors.

The agent monitors network activity on the endpoint, delivering key data and metadata to the central Darktrace Threat Visualizer environment, and if required, triggers autonomous response actions to restrict anomalous connectivity at the system-level.

Darktrace / ENDPOINT is best deployed alongside Darktrace / NETWORK to provide full network coverage alongside detection and response capabilities, however it can be deployed as a standalone product if desired.

Deployment options

Endpoints

The Darktrace cSensor is provided as an installation package for Windows, macOS or Linux endpoint devices. During installation, the agent is supplied with unique credentials that allow it to communicate securely with the cloud-based cSensor infrastructure.

The device monitored with the cSensor must be able to contact the cSensor infrastructure over HTTPS/443 for network traffic monitoring.

Supported operating systems:

- **Windows:** Windows 365, 11, 10; Windows Server 2022, 2019 and 2016

- **macOS:** macOS 12, macOS 13, macOS 14

- **Linux*:** Ubuntu 18.04+; RHEL/Centos 7+; Debian 9+; openSUSE 15.0+/SUSE Linux Enterprise 12.4+; Fedora (maintained versions)

Host utilization:

- Bandwidth utilization is minimal, averaging <1kB/s.

- Negligible CPU impact, <40MB RAM usage

- Installation Packages: macOS <30MB, Linux (all formats) <30MB, Windows <30MB

- Up to 40MB disk required.

Analysis

Darktrace can be deployed in a variety of 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 as a complementary solution to Darktrace / ENDPOINT 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.

*The cSensor is expected to be compatible with most Linux-based distributions with a kernel version >= 4.6, therefore, the package may be effective on distributions outside those explicitly listed above. The only supported architecture is x86_64.

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.

cSensors, once installed on an endpoint device, will analyze network traffic sent and received on any network interface and communicates this information to your Darktrace environment via cloud-based infrastructure. A combination of on-endpoint Deep Packet Inspection analysis - forwarding just relevant metadata to minimize bandwidth consumption - and cloud-based processing is performed. All data is transmitted securely over an encrypted communication mode using authentication details unique to your Darktrace environment.

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 as part of a Darktrace / NETWORK deployment. 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 / ENDPOINT integrates seamlessly as an extension of Darktrace / NETWORK, can collect data from 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 detection and response capabilities 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.

Achieve cyber resilience with the Darktrace ActiveAI Security Platform

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

Darktrace / ENDPOINT is a perfect complement to Darktrace / NETWORK. Extend the capabilities of Darktrace / NETWORK to your endpoints to achieve unprecedented network visibility, precision threat detection and autonomous response for known and unknown threats.

Darktrace / Incident Readiness & Recovery takes information from Darktrace / ENDPOINT 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.
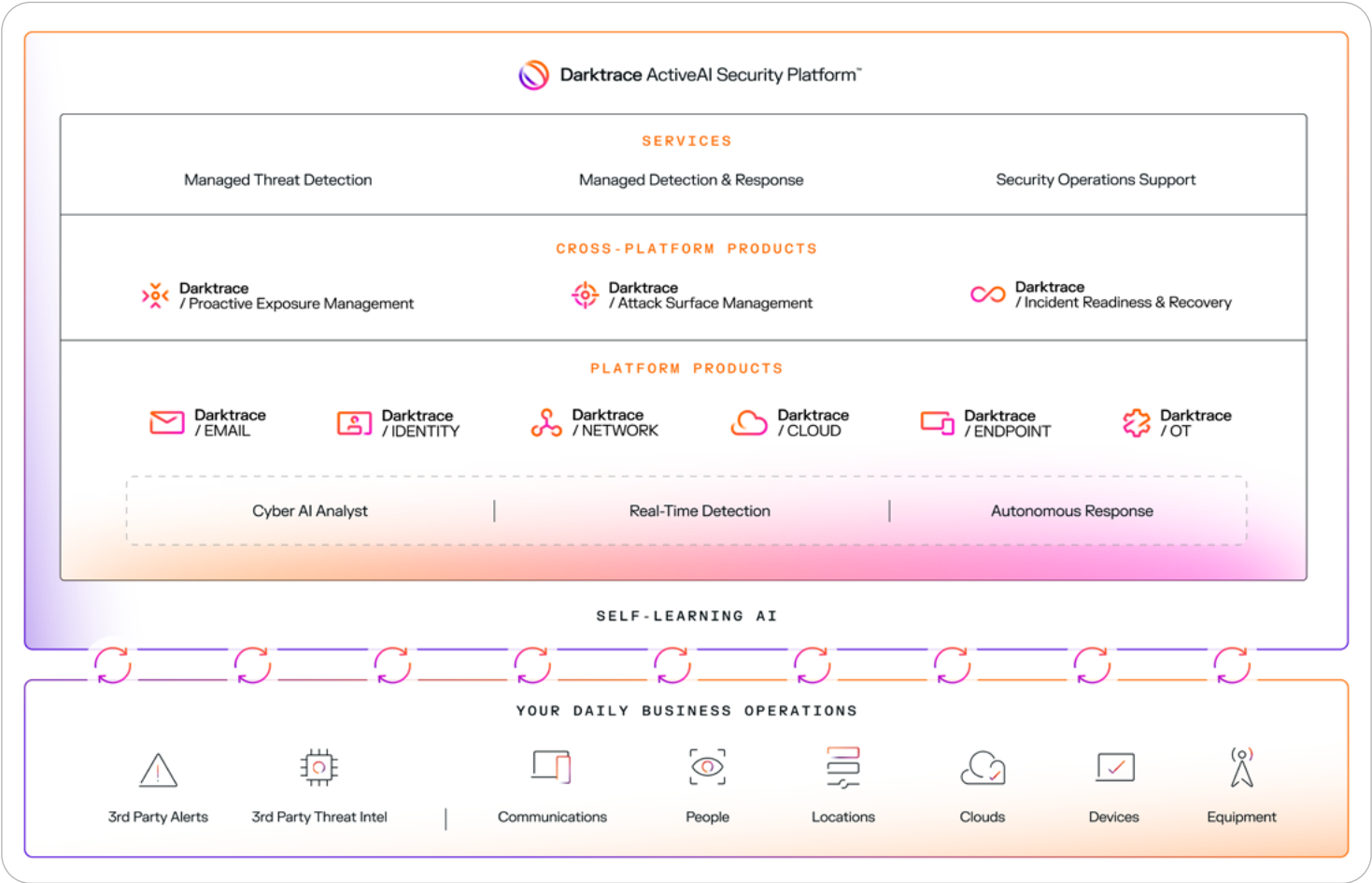

Figure 07: The Darktrace ActiveAI Security Platform.

Operational Benefits

Increase operational efficiency
with Self-Learning AI that autonomously tunes itself to significantly reduce false positives and the need for continuous manual tuning.

Reduce the pressure on security teams
by leveraging Cyber AI Analyst that autonomously investigates and triages every relevant alert and surfaces the most important incidents to your attention.

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 endpoint security
by proactively preventing cyberattacks and strengthening your security posture with the Darktrace ActiveAI Security Platform.

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.

"Self-Learning AI investigates behavior on the endpoint alongside behavior in Microsoft 365 and across our entire cloud environment."

■ **Senior Director of
Counter Threat Operations**
Royal Caribbean Group

"We have a strong Microsoft presence and Darktrace just integrates with our existing security platforms and profiles seamlessly; it makes a huge difference and centralizes our visibility."

■ **Head of Technology**
Community Housing Limited

"Darktrace was simple to deploy, effective in our needs for monitoring and response, and provided us all the information we needed."

■ **Senior Information Security Analyst**
AAA Washington

■ **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.