DARKTRACE/OT

DARKTRACE

The Most Comprehensive Prevention, Detection, and Response Solution Purpose Built for Critical Infrastructures

OT Threats are Evolving

Adversaries are taking advantage of any attack surface, meaning the rapid adoption of Industrial Internet of Things (IIoT) and IoT at not only industrial organizations, but most industry sectors, perpetuates a convergence of IT and OT systems.

This leads to an increase in vulnerabilities and exposures if security teams cannot see adversaries traversing both systems. This digital expansion illuminates a lack of alignment between engineers, operators, and security teams, hindering effective mitigation of cyber risks across both IT and OT environments. Coordination among these teams is crucial to align goals and strategies for comprehensive security.

Furthermore, attacks on OT systems, whether from nation-states, adversarial groups, or insiders, employ sophisticated techniques like "living off the land," emphasizing the need for heightened vigilance and advanced threat detection in safeguarding critical infrastructure and industrial networks.

Business Benefits

Converge IT and OT teams under a single communication platform
Protect all interconnected devices that drive production within a single trusted platform, from network and cloud connected IT systems to specialized OT assets

Defend your IT and OT assets with the same rigor
Combine end-to-end coverage of industrial protocols and devices with industry leading analysis of IT activity, providing both OT engineers and security operations confidence maintaining productivity and security at the same time

Maintain operational up time
Contain threats automatically without causing disruption to production with the industry's first and only trusted AI autonomous response for OT and critical infrastructure

Effectively mitigate risks with or without a patch
Leveraging MITRE mitigations, Darktrace guides security teams in executing preventative measures to reduce risks. In cases where patches are unavailable, mitigations elsewhere deny an attackers the and remove or reduce the risk

Use Cases

/ Living Off the Land Attacks

/ Containing corporate ransomware spillover

/ Malicious Insiders

/ Non-Malicious insiders/ third-parties

/ Zero-day exploits

/ Compromised OT remote access

/ Adversaries with established persistent or legitimate access

/ Supply chain attacks

OT Security Solutions Have Not Risen to the Challenge

The dichotomy between OT native and IT native solutions exacerbates visibility issues, leaving organizations vulnerable to cyber threats that exploit the gap between these two domains.

While some OT security vendors specialize in threat intelligence or use basic supervised machine learning for unconfirmed anomaly detection, they rely on knowledge of past attacks to detect threats, missing novel and zero-day threats. Furthermore, IT security vendors lack integration with OT systems, rely heavily on manual CVE identification and complicated patch management with a limited patching window of opportunity to apply them, leaving a significant percentage of known CVEs unresolved and no real time response to offer a hope of resolution. In fact, on average, vulnerabilities remain without patches for over 5 years.[1]

Conversely, IT Vendors cannot accurately identify OT devices, don't consider the unique infrastructure that makes up OT environments, are 'heavy handed' with response actions, and risk operational downtime for critical devices.

[1] https://research-information.bris.ac.uk/ws/portalfiles/portal/313646831/Catch_Me_if_You_Can.pdf

Revolutionizing OT Security with Darktrace/OT

The most comprehensive Prevention, Detection, and Response solution purpose built for Critical Infrastructures.

Darktrace/OT is the only OT cybersecurity solution that natively covers IT and OT providing visibility of OT, IoT, and IT assets in unison encompassing network and cloud-connected IT systems to specialized OT assets, achieving greater visibility of OT and IT devices across all levels of the Purdue Model.

Using Self-Learning AI technology Darktrace/OT is the industry's only OT security solution to scale bespoke risk management, threat detection, and response with a 92% time saving from triage to recovery[2]. This provides engineering and security teams with confidence to evaluate workflows, maintain security posture, and effectively mitigate risks from a unified platform without productivity loss.

Key Capabilities

Asset Management

Darktrace/OT uniquely identifies, visualizes, and secures, all devices across IT and OT protocols

Darktrace Asset Identification offers both active and passive scanning to identify devices for foundational technical information (MAC Address, Vendor, Firmware version, Model,etc.) and vulnerability data (CVEs and End-Of-Life status). The data is pulled into different interactive visualizations for security teams to explore the relationship between devices and quickly determine location and status, then guides security workflows with real time activity monitoring to accurately visualize live OT operations and relevant IT infrastructure, unlimited by visibility into only OT.

Automating asset identification and doing so in a comprehensive way across every part of the organization in real time, buys time for the security team to focus on investigation and bolstering defenses.

Operational Benefits

Passive and active automatic OT device identification
Behavior profiles for all OT, IT, and IoT assets, including PLCs, HMIs, and Workstations. All IP-connected devices are tracked and catalogued alongside serial-connected slots in Controller backplanes, with no effect on assets or their functions. Active polling options can be leveraged if desired

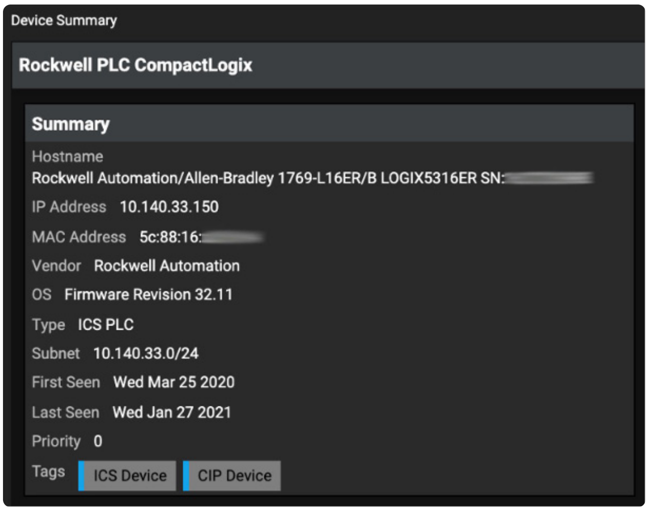
Unified workflows and visibility for IT and OT engineers
AI generates reports, explanation, and investigation in plain English to keep IT analysts & OT engineers on the same page while upskilling both teams

Reduce triage and investigation time of OT threats by 90%
Only Cyber AI Analyst automatically investigates all threats across IT and OT, prioritizing critical incidents, and summarizing findings to provide an easily understandable common ground for production engineers and security analysts to quickly converge, communicate, and take appropriate action

Identify novel threats without expensive threat hunting services
Our Self-Learning AI continuously adapts to understand normal, revealing suspicious activity No constant tuning or external connectivity needed to detect known and unknown threats

Contain threats at the earliest stages
Darktrace/OT allows security and production to agree on permitted actions for potential attacks before they occur, initiating precise response to stop and contain a threat while ensuring production continues all the time, every time.

Go beyond simple vulnerability scoring (CVE/CVSS) to generate bespoke Risk Analysis
Darktrace/OT combines its unique understanding of IT, OT, CVE data, and MITRE techniques, to map the critical attack paths across your infrastructure, then identify and prioritize risk based on an adversary's difficulty and effort to exploit a vulnerability and advance objectives



Device Summary

Rockwell PLC CompactLogix

Summary

Hostname
Rockwell Automation/Allen-Bradley 1769-L16ER/B LOGIX5316ER SN:[redacted]

IP Address 10.140.33.150

MAC Address 5c:88:16:[redacted]

Vendor Rockwell Automation

OS Firmware Revision 32.11

Type ICS PLC

Subnet 10.140.33.0/24

First Seen Wed Mar 25 2020

Last Seen Wed Jan 27 2021

Priority 0

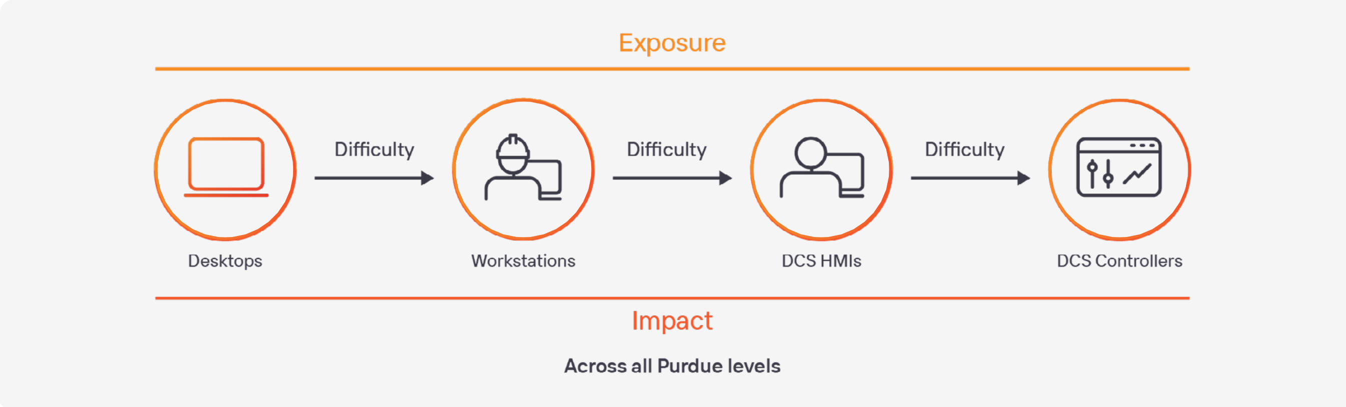
Tags ICS Device CIP Device

Figure 1: Device summary as identified by Darktrace/OT

[2] https://darktrace.com/news/darktrace-cyber-ai-analyst-investigates-threats-at-machine-speed-4

Vulnerability and Risk Management

Prioritize and effectively manage risks that cannot be solved with a patch, as well as those that can.



Moving beyond CVE data

Darktrace/OT is the industry's first OT Risk Management solution to go beyond simple vulnerability scoring (CVE/CVSS), generating bespoke Risk Analysis. Darktrace/OT combines its unique understanding of IT, OT, CVE data, and MITRE techniques, to map the critical attack paths across your infrastructure, contextualize risk and then identify and prioritize remediation and mitigation that based on the difficulty, exposure, and impact of a vulnerability most effectively reduce risk associated with your environment.

Contextualize vulnerabilities within your unique environment

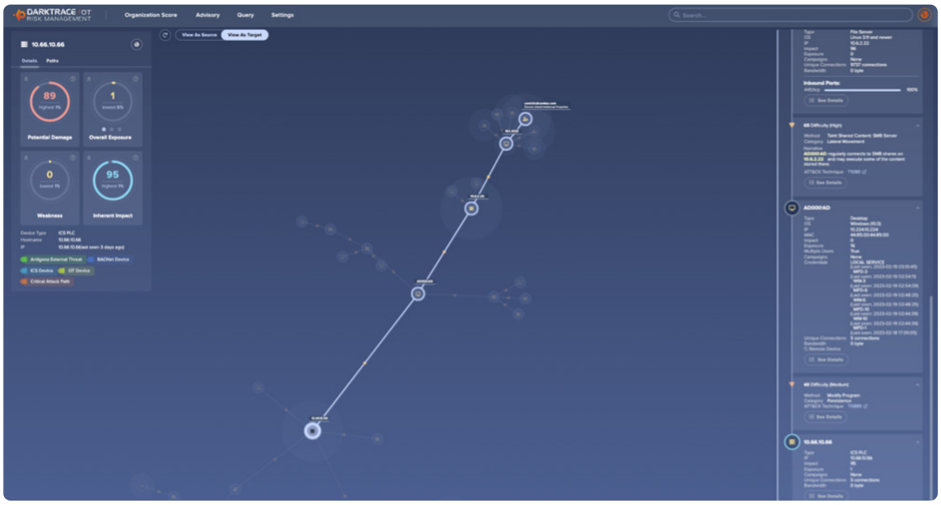
Darktrace/OT identifies CVEs associated with devices on your network, and Darktrace/OT contextualizes and ranks which CVEs are most likely to be targeted, exploited, and will have the most impact on your network. This vulnerability contextualization is largely done by attack path modeling which, through an understanding of the environment, identifies how accessible the vulnerable devices are within the network and the likelihood that an attack path would be engaged, along with the potential impact the execution of the attack patch would have on your organization.

Establish a realistic risk mitigation strategy

Darktrace/OT then prioritizes remediation actions security teams can take that will have most positive impact on overall risk. However, for many industrial organizations it's often the case that little or no remediations action can be taken. In this case, Darktrace presents and prioritizes mitigations such as eliminating unnecessary open ports on high impact devices to reduce the accessibility to a vulnerability for an attacker. This approach is only possible with Darktrace/OT's unique understanding of your infrastructure.

Communicate board level risk with APT Threat Mapping

Darktrace/OT is the only OT security solution that maps MITRE techniques used by known APT groups onto your unique attack paths, empowering security teams with insights into attack likelihood, chance of success, and potential impact within your unique environment. This gives security teams a practical attacker viewpoint into your unique risks by evaluating your defenses against different APT groups.



Device Type ICS PLC
Hostname 10.66.10.66
IP 10.66.10.66(last seen 3 days ago)

Figure 2: OT Risk Management Display of an Attack Path

Threat Detection & Investigation

Detect insider, known, and unknown threats at scale, without the unmanageable linear increase in operational workload as you scale and grow

Anomaly-based detection

Unlike all other approaches to OT security that rely on a constant stream known of threat data, Darktrace/OT leverages Self-Learning AI to understand your normal business operations, allowing you to detect anything that deviates from normal. This makes it possible to spot insider, known, unknown, and zero-day threats at scale. Because we work based on your raw network data, Darktrace can be safely implemented to provide a consolidated view into OT or both OT and IT environments without internet or external connectivity.

AI-driven investigation

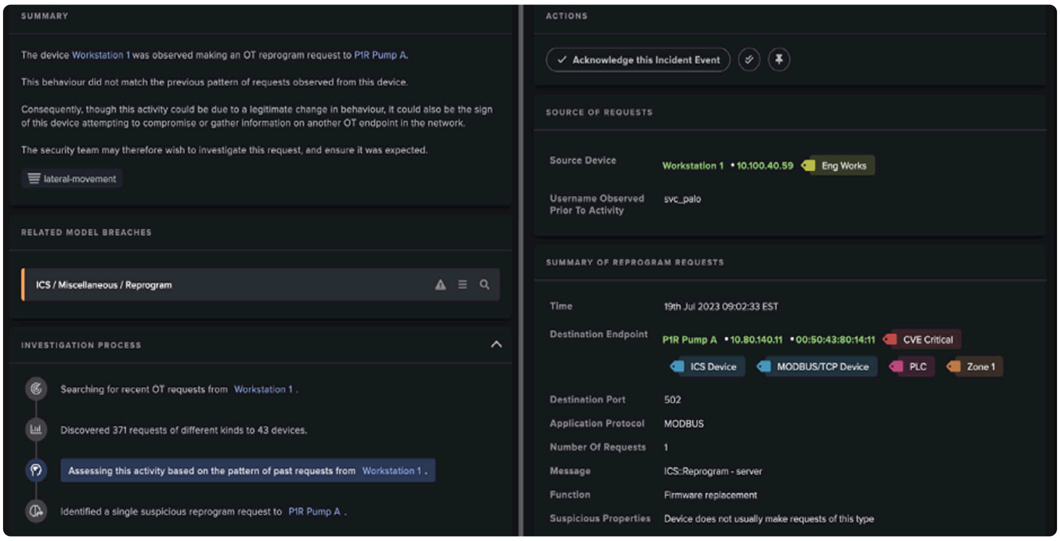
While AI is being used to detect anomalies, we also want to keep the human in the loop. Darktrace immediately understands, identifies, and investigates all anomalous activity in OT networks, whether human or machine driven and uses Explainable AI to generate investigation reports via Darktrace's Cyber AI Analyst. These auto-generated reports reduce triage and investigation time of threats by 92%[3], automatically investigating all threats across IT and OT, prioritizing critical incidents, and summarizing findings upskilling your IT and OT practitioners.

Capable of grouping seemingly disparate events under a single incident, organizations can swiftly understand the attack timeline, affected assets and relevant technical information thanks to a easily understandable narrative of the incident. Facilitating prompt and clear communication that enables more accurate remediation actions.

Cyber AI Analyst improves critical infrastructure operators' ability to report major cyber-attacks to regulatory authorities. Considering that 72 hours is the reporting period for most significant incidents — and 24 hours for ransomware payments — Cyber AI Analyst is no longer a nice-to-have but a must-have for critical infrastructure.

Unifying IT and OT security teams

These reports build common ground for production engineers and security analysts to quickly converge, communicate, and take appropriate action significantly reducing the OT security knowledge and skills gap. It is also possible to route the output of these investigations to an organization's established processes and procedures.



SUMMARY

The device Workstation 1 was observed making an OT reprogram request to P1R Pump A.

This behaviour did not match the previous pattern of requests observed from this device.

Consequently, though this activity could be due to a legitimate change in behaviour, it could also be the sign of this device attempting to compromise or gather information on another OT endpoint in the network.

The security team may therefore wish to investigate this request, and ensure it was expected.

RELATED MODEL BREACHES

ICS / Miscellaneous / Reprogram

INVESTIGATION PROCESS

1. Searching for recent OT requests from Workstation 1 .
2. Discovered 371 requests of different kinds to 43 devices.
3. Assessing this activity based on the pattern of past requests from Workstation 1 .
4. Identified a single suspicious reprogram request to P1R Pump A .

ACTIONS

SOURCE OF REQUESTS

Source Device: Workstation 1 • 10.100.40.59 Eng Works

Username Observed Prior To Activity: svc_palo

SUMMARY OF REPROGRAM REQUESTS

Time: 19th Jul 2023 09:02:33 EST

Destination Endpoint: P1R Pump A • 10.80.140.11 • 00:50:43:80:14:11 CVE Critical ICS Device MODBUS/TCP Device PLC Zone 1

Destination Port: 502

Application Protocol: MODBUS

Number Of Requests: 1

Message: ICS::Reprogram - server

Function: Firmware replacement

Suspicious Properties: Device does not usually make requests of this type

Figure 3: AI Analyst incident reporting on a potential insider threat with complete investigation process explained. A statistically unusual reprogram command was observed source device engineering workstation and destination PLC

[3] https://darktrace.com/news/darktrace-cyber-ai-analyst-investigates-threats-at-machine-speed-4

OT Response

Darktrace/OT is the industry's first and only trusted AI autonomous response for OT and critical infrastructure.

Operators and engineers often exhibit reluctance towards active response mechanisms in OT networks, fearing potential disruptions to critical operations. However, when threats emerge at their nascent stages, all involved parties want immediate measures to quarantine and neutralize them before they can affect OT systems.

OT-centric security vendors typically identify threats only after they've breached OT systems, offering human incident response services or limited response capabilities through integration, thus leaving security teams with inadequate means to counter ongoing attacks while ensuring the availability of critical systems in real-time. However, asset owners recognize the imperative of not just detecting but halting threats at their earliest stages to safeguard operations.

Highly configurable response actions

Darktrace distinguishes itself by working hands on with organizations to leverage its comprehensive understanding of network behavior to initiate precise responses only as permitted by end users. These responses are entirely optional and highly configurable beginning with prompting human confirmation before taking action.

When the security team gain trust with the AI's proposed decision making, which typically occurs within the fist year of deployment, response actions can be executed autonomously. This represents the industry's pioneering autonomous response capability for OT and critical infrastructure that can halt and contain malicious actions at their earliest stages while ensuring uninterrupted production.

These actions encompass temporary denial of specific connections or quarantining devices, preventing them from compromising sensitive OT systems. Darktrace collaborates closely with owner-operator organizations to tailor response applications and integration, thereby maximizing protection against threats originating or occurring between Purdue levels 5-3.

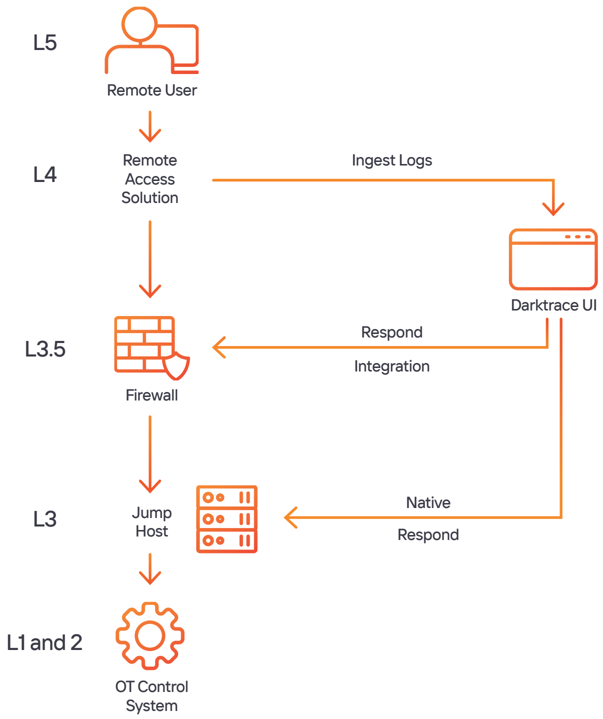


Figure 4: Darktrace typically deploys response down to level 3 of the Purdue Model, ensuring containment without business disruption

Deploying Darktrace/OT

In our unified view we can deploy devices into your environment whether IT, DMZ, OT, Cloud, or all the above, providing local monitoring no matter where your operational technology infrastructure is.

Unlike the standard master and collector deployment, Darktrace/OT appliances analyze ingested traffic locally, each appliance is capable of acting as a master or directing analyzed traffic to designated masters, allowing deployment in complex, local, and remote environments with bandwidth limitations, customized site by site access and organization wide fleet security management views.

Darktrace/OT is deployable in isolation and air gapped environments without the need for any external connectivity because the AI powered analysis of traffic is performed onsite and has no requirement for external connectivity or adjustments to segmentation to ingest threat intelligence data.

Darktrace/OT passively ingests network traffic with virtual and physical options. Deep Packet Inspection on specialized OT protocols and present IT protocols learn normal activity of devices and users even when ingesting encrypted and proprietary OT protocols.

All hardware build and operations are handled in house by Darktrace for efficiency and support significantly increasing logistical and technical support capabilities for large and sensitive deployments.

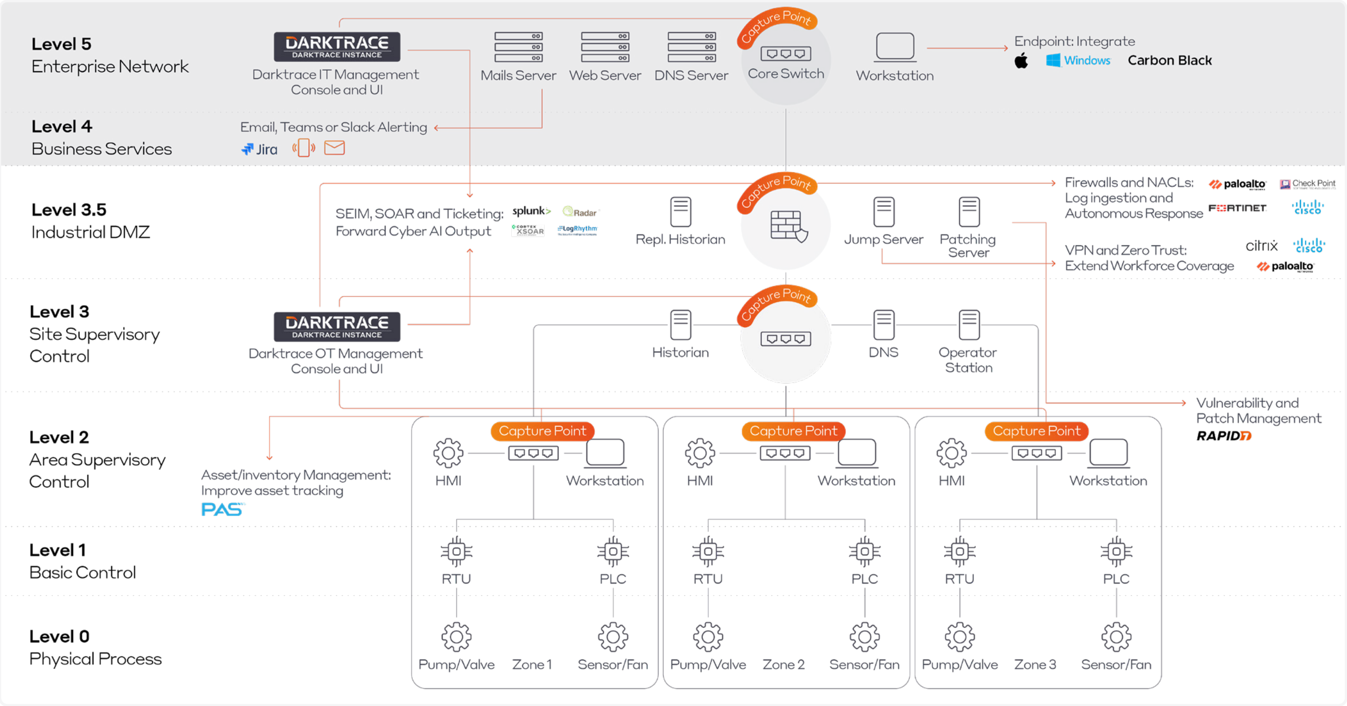


Figure 5: Example of Darktrace deployment

Darktrace/OT Features and Capabilities

Incident phase + feature	Role of AI	Description
PREVENT		
Asset management	Autonomous categorization and cataloguing of assets and CVE data	• Darktrace provides relevant asset and CVE data across OT devices Purdue levels 1-5 • Active and Passive asset inventory • CVE tracker • Subnet explore (OT data flow topology)
Risk & vulnerability management	• Attack path modeling • Cyber risk scoring • Prioritizing mitigation and remediation	• AI driven contextualization and scoring of OT risk and network vulnerability. • AI leverages CVE data, attack path modeling, and open source data providing tailored and prioritized vulnerability mitigation and remediation suggestions that effectively reduce risk
DETECT		
Threat detection and alerting	• Anomaly based detection • Investigate and prioritize critical alerts	• Darktrace's machine learning approach provides unprecedented awareness across both our IT and OT networks • Detects sophisticated threats and never-before-seen TTPs • Capable of detecting OT insider threats • AI led investigation of events across IT and OT upskills your team explaining its detection reasoning and every stage of an incident
RESPOND		
Incident Response	Precise and customizable response	• Allows incident responders and end users to contain attacks in the earliest phases before they threaten operations • Easily configurable and customizable human confirmation and autonomous response • Customizable, native, or integrated response options through SRA, Zero Trust, IPS solutions and more

Darktrace/OT ActiveAI Security Platform

Darktrace/OT is supported by the Darktrace ActiveAI Security Platform bridging the gap between IT, Cloud, IoT, and OT/ICS infrastructure. While many solutions lack the capability to aggregate data from IT and OT resulting in unknown gaps in visibility, Darktrace/OT learns from your entire digital estate to provide unparalleled visibility on IT, OT, and how they interact. With data from the cloud, SaaS, endpoints, OT, email, and more in one easy to read UI, Darktrace unifies workflows for security practitioners in complex OT and IT environments.

Darktrace is the first of its kind to provide proactive cyber defense in a single holistic platform. To achieve this, Darktrace pioneered the use of ActiveAI Security that continuously learns from your day-to-day business operations, applying context from your enterprise data ingested from internal native sources including email, cloud, operational technology, endpoints, identity, applications and networks, and external sources of third-party security tools and threat intelligence. Through this approach, Darktrace provides the ability to visualize and correlate security incidents uninhibited by the siloed approach of individual point.

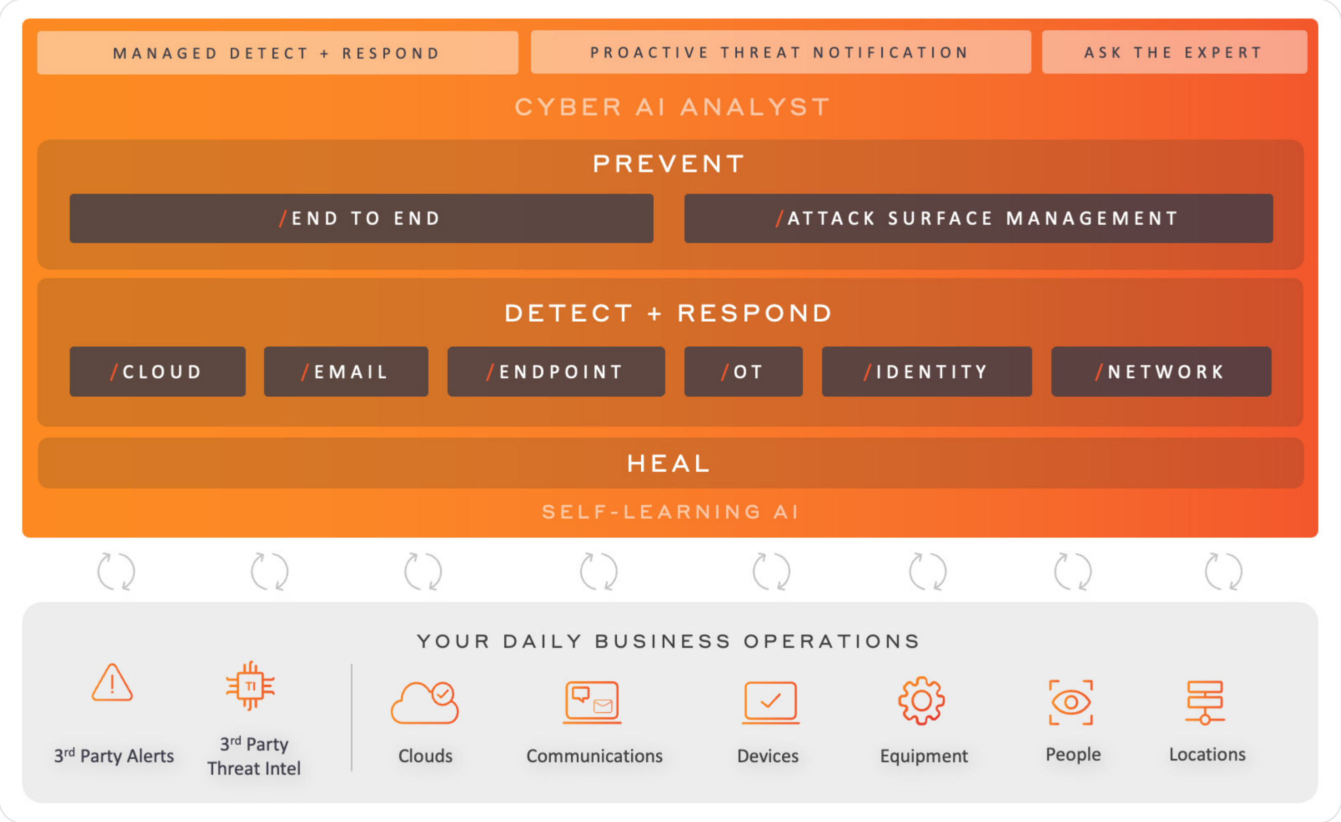


Figure 6: The Darktrace ActiveAI Security Platform

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its 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 achieve an optimal state of cyber security. Breakthrough innovations from its R&D Centers have resulted more than 165 patent applications filed. Darktrace employs 2,300+ people around the world and protects over 9,200 organizations globally from advanced cyber-threats.

Scan to
LEARN MORE

DARKTRACE
Evolving threats call for evolved thinking™

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
Latin America: +55 11 97242 2011
info@darktrace.com
darktrace.com