DARKTRACE

Darktrace / OT

The most comprehensive OT security solution purpose built for critical infrastructures

Threats facing critical infrastructure across IT, OT, IIoT, IoT, and cloud are increasing. Nation-states, insiders, and cybercriminal groups are becoming more sophisticated using techniques such as "living off the land," and supply chain attacks to penetrate OT environments.

Darktrace / OT is the most comprehensive OT security solution purpose built for critical infrastructure. By learning "normal" across IT, OT, and IoT assets, it autonomously detects, investigates, and responds to novel attacks before they disrupt operations.

Key Capabilities

Comprehensive asset visibility

- Discover and monitor assets across OT, IT, IoT, and IoMT using passive and active identification. Darktrace maps device relationships and exposure across the Purdue Model, with tailored operational and governance views.
- Supports DPI for 100+ protocols, with metadata from 40+ OT-specific protocols powering Pattern of Life AI models. Integrates with ServiceNow for automated asset syncing.

Risk management beyond CVEs

- Go beyond static vulnerability lists with bespoke risk scoring that models how adversaries could move through your network, factoring in segmentation posture, firewall misconfigurations, asset criticality, and whether devices are actually reachable.
- Darktrace correlates MITRE techniques, CVE severity, EOL status, KEV data, and business impact to prioritize mitigations where they matter most.

Anomaly-based detection and AI-led investigation

- Detect unknown threats in real time by learning what's "normal" across IT and OT. Cyber AI Analyst auto-triages and explains incidents, reducing investigation time by up to 90%.
- Extend detection to HMIs, engineering workstations, and contractor laptops using Network Endpoint eXtended Telemetry (NEXT) for OT, a lightweight collector that enriches CVE context, flags anomalies, and supports root-cause analysis, even in segmented environments.

Governance & compliance reporting

- Automates alignment to IEC-62443-3-3, mapping controls to required security levels and surfacing misconfigurations. Simplifies audit prep and removes spreadsheet-heavy reporting.

Trusted response for OT

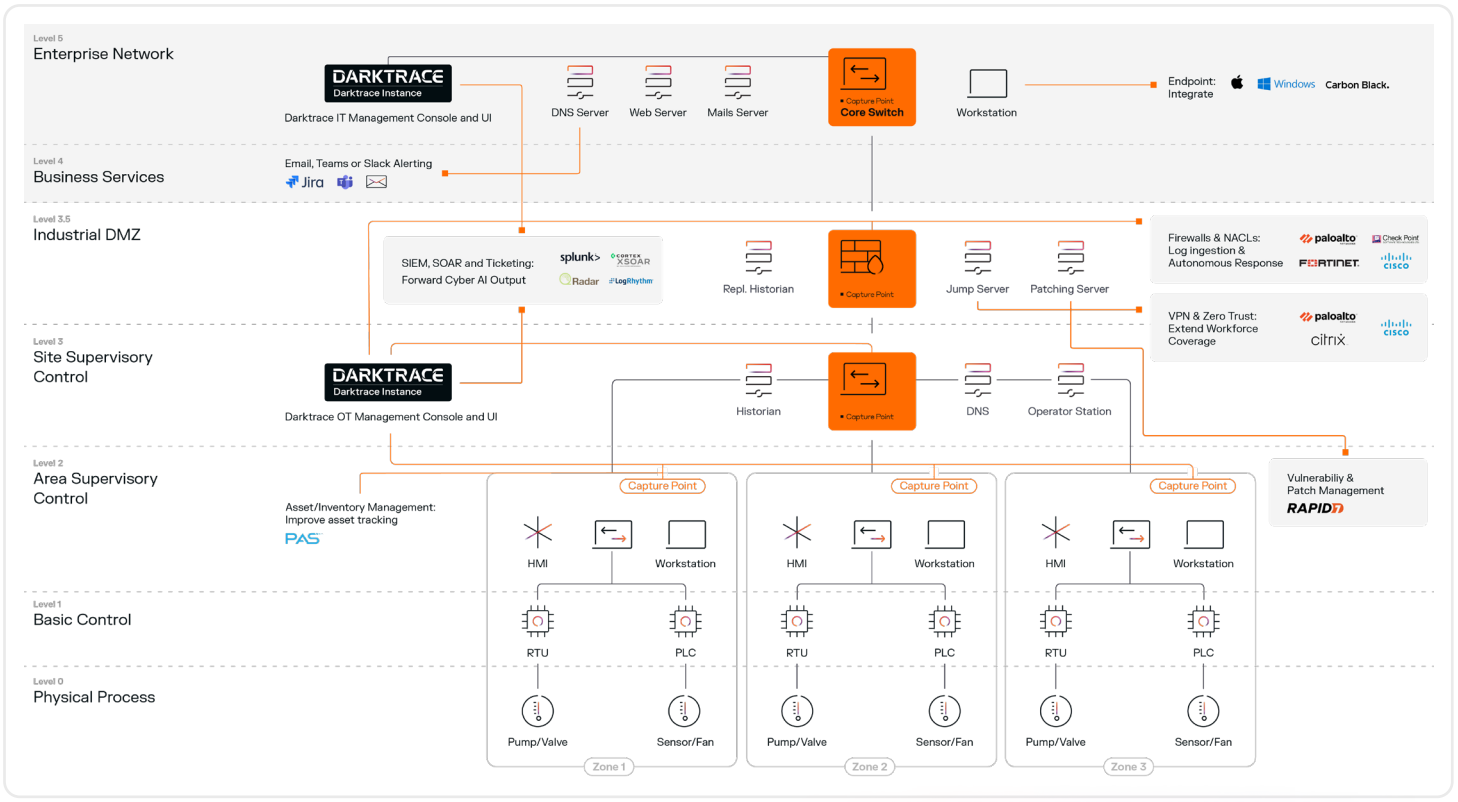
- Contain threats early with autonomous response that enforces known-good behavior, isolates compromised devices, or blocks risky communications without operational disruption.
- Supports human-in-the-loop or automated response execution through native controls or firewalls and other enforcement tools.

Operational overview for engineers

- A dedicated dashboard for OT engineers, showing asset health, changes, risk levels, and alerts without IT-centric noise. Highlights reprogramming activity, device roles, and anomalies for faster triage and collaboration.

Business benefits

- **Converge IT and OT teams** on a single trusted platform.
- **Defend critical production systems** while maintaining uptime.
- **Reduce audit fatigue and compliance costs** with automated IEC-62443 mapping.
- **Effectively mitigate risk** with or without patches by leveraging MITRE-aligned mitigations.
- **Safeguard against** sophisticated threats like ransomware spillover, malicious insiders, and supply chain attacks.



Fast and flexible deployment

Darktrace / OT deploys across IT, OT, cloud, and airgapped environments without external connectivity. Appliances virtual and hardware analyze traffic locally, supporting complex distributed sites and bandwidth-limited environments. Passive monitoring and deep packet inspection ensure visibility across proprietary and encrypted OT protocols, without disruption

Built to align with your IT, OT, and security workflows

Darktrace / OT integrates seamlessly into your existing security stack, with support for SIEM, SOAR, CMDBs, zero-trust tools, and firewalls. Extensive APIs and active response integrations ensure smooth data sharing, orchestration, and enforcement across asset management, vulnerability workflows, and operational controls.

Achieve resilience with the Darktrace ActiveAI Security Platform

Darktrace / OT is part of the Darktrace ActiveAI Security Platform, which unifies visibility and defense across email, cloud, endpoint, network, and OT. By learning from your unique digital estate, the platform helps proactively prevent attacks, accelerate recovery, and strengthen cyber resilience all within a single interface.

Operational benefits

- **90% faster** triage and investigation with Cyber AI Analyst.
- **Full asset coverage** across IT, OT, IoT, IoMT and industrial protocols.
- **Precise and configurable** autonomous response to contain threats without production disruption.
- **Unified workflows** with plain-English AI reports that upskill IT and OT teams.
- **Track operational anomalies** without navigating IT-centric workflows, with a dedicated operational overview dashboard that tailors information for OT engineers.
- **Fewer** false positives, shorter incident chains, and more resilient operations.

"We chose Darktrace / OT for monitoring and threat detection because it was purpose built for critical infrastructure. After trying Darktrace within our environment, we felt very confident it was the best solution for our needs."

- **Chief Security Officer**
  EverLine