Product brief

Darktrace RESPOND/OT

DARKTRACE

Darktrace RESPOND™ Overview

Darktrace is made up of four interconnected product families: PREVENT™, DETECT™, RESPOND™ and HEAL™. Darktrace RESPOND takes action – autonomously or with human confirmation – to stop in progress cyber-attacks at their earliest stages. Response capabilities can be applied across Operational Technology, SaaS, email, cloud, and more.

Uniquely, Darktrace RESPOND/OT can either take native actions, ranging from severing connections to isolating devices, or it can integrate with firewalls and other security tools via API to take customized actions, ensuring that the most appropriate response is taken, or policy is enforced, wherever a threat appears.

Autonomous, always-on action to contain and disarm attacks within seconds.

Responding to Threats in Industrial Environments

Pain Points

OT-centric security venders provide human incident response offerings and limited native response capabilities through a small set of integrations.

End users have little technological capability to stop an ongoing attack and maintain availability of critical systems in real time.

Basic OT security methods – e.g., vulnerability tracking and patching, threat intel sharing, rules, signatures/pre-defined behavioral profiles – do not stop in-progress attacks or insider threats from sophisticated adversaries leveraging zero-day target specific TTPs.

Darktrace Solutions

Darktrace works hands-on with owner operator organizations to define the scope and nature of where RESPOND/OT can be applied and integrated to ensure the availability of the protected systems while maximizing their protection from threats emanating in Purdue levels 5-3.

All Darktrace response actions can be configured temporally (response action set for X hours) and can be set to be taken autonomously or in human confirmation mode.

RESPOND actions can be as tailored as blocking specific connection between 2 devices or as general as quarantining a device or user.

OT Engineer dashboard provides an operations-focused dashboard for on site or remote-control engineers to leverage RESPOND/OT at the site level.

OT Explore enables a top-down visualization of the OT environment for SOC or central industrial security management to leverage respond across the entirety of the organization.

Responding in OT Environments

Leveraging Darktrace's native response features, organizations work with Darktrace to customize how they want Darktrace RESPOND/OT applied. These options vary from on a device-by-device basis, device type by device type, or subnet by subnet basis.

Although RESPOND/OT can be applied to devices Purdue levels 1-5, many organizations first rollout RESPOND/OT in human confirmation mode functional on only IT devices not critical to process control automation within an industrial operation. This rollout helps security personnel, and site owner operators become comfortable taking actions in real time to mitigate in-progress threats to operations while not affecting availability of any industrial systems.

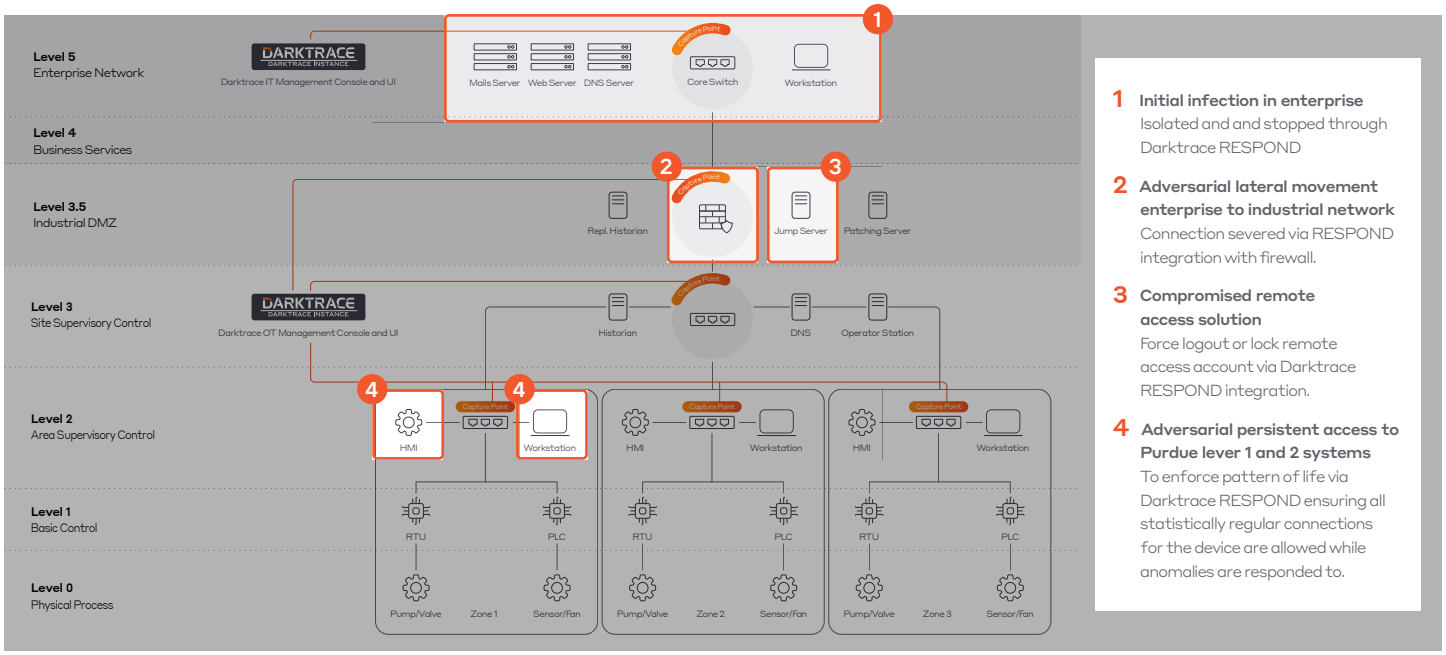

Figure 1: Different use cases and points of response for RESPOND/OT across the Purdue model.

RESPOND/OT via Integration

Darktrace also works with industrial organizations to integrate RESPOND/OT with existing security technologies to increase response capabilities and enforce security policies.

Typical RESPOND/OT integrations include:

Firewalls // Remote Access Solutions // EDR

Custom integrations and responses via custom integration are supported by the Darktrace/OT development team. Please reach out if a desired integration is not listed within the Darktrace/OT integration white paper.

See OT integration list: https://darktrace.com/integrations

Case Study: Enforcing policy and IR with Darktrace RESPOND/OT

Darktrace/OT monitors connections in and out of the OT environment at a large geographically distributed organization. This organization uses a Secure Remote Access Solution (SRAS) to grant remote personnel access to OT systems.

Because Darktrace DETECT ingests logs from the SRAS, it was able to alert the security team to a suspicious remote access attempt. DETECT determined the user's remote access account has become compromised, and a malicious actor is attempting to access critical control systems.

Darktrace RESPOND autonomously blocked the remote connection by updating Firewall rules via an integration. Even without the integration, Darktrace can respond by taking a native response against the jump host, such as blocking matching internal connections to prevent the attacker from reaching further OT devices.

Additionally, the victim organization leverages Darktrace to enforce incident management policies. While Darktrace autonomously responds to the compromised remote access, the security team is prompted with additional human confirm- able respond actions:

- Block all incoming connections to the industrial control system via Darktrace pushing preset rules to the firewall at the security perimeter.
- Isolate the endpoint device of the user with compromised endpoint device via Darktrace/Endpoint.
- Force logout or lock the remote access account of the end user via integration with the remote access solution.