DARKTRACE HEAL™

DARKTRACE

Changing Organizations, Evolving Threats

In a constantly changing threat landscape, security teams face limitations in preparing for and responding to emerging cyber security incidents due to human resource constraints, process deficiencies, and inadequate technical solutions that fail to meet real-world requirements.

It's important for CISOs to be aware of both the readiness of their technology – including proper configuration for effective use – and their security team's ability to handle the recovery from a cyber-attack. As organizations continuously evolve, playbooks remain static and unchanged, resulting in a mismatch between attacks and response plans.

135% increase

in 'novel social engineering' attacks in 2023 amidst widespread availability of ChatGPT[1]

[1]Based on the average change in email attacks between January and February 2023 detected across Darktrace/Email deployments with control of outliers

Darktrace HEAL™ uses AI to understand your business data to ensure **readiness to recover** from an active cyber-attack and to **rapidly restore** the business to an operational state.

Continuously assess and optimize the incident response readiness of your teams and technology

Is everything going to work when I need it to? Including my people?

- Incident Simulations and Readiness Drills
- Readiness Reporting

Address incidents early and recover quickly

How can I get ahead of an in-progress attack?

- Bespoke, AI-Generated Playbooks
- Automated Remediation and Recovery Actions

Save valuable time with automated reporting and easy collaboration

How can I maximize the time of my limited team?

- Automated Incident Reports
- Secure Collaboration & Communications
- Technology Integrations

Features Spotlight

Readiness Analysis

Be prepared for anything

Uses Darktrace's existing understanding of you – the devices and communications gathered from Darktrace DETECT – to establish: how ready are you for a cyber-attack? With continuous evaluation, organizations can gain a clear understanding of their cyber resilience and how to improve their risk posture most effectively.

Incident Simulations and Readiness Drills

Practice like it's real so you're ready when it is

Ensure readiness to respond to incidents through threat simulations that run real-world incidents adapted to your organization. By running and tracking simulated incidents, teams can identify weak points and gaps in their response plans.

Recovery Decision Engine

Get back up and running

When incidents occur, adapts responses automatically to precise incident details, rather than forcing one universal playbook to function for all. It automates much of the recovery process, and where necessary, presents recommendations to human teams based on real-time developments - enacting, delegating, and tracking actions to remediate and recover assets.

Secure Collaboration and Communications Channel

Get the right people in the room

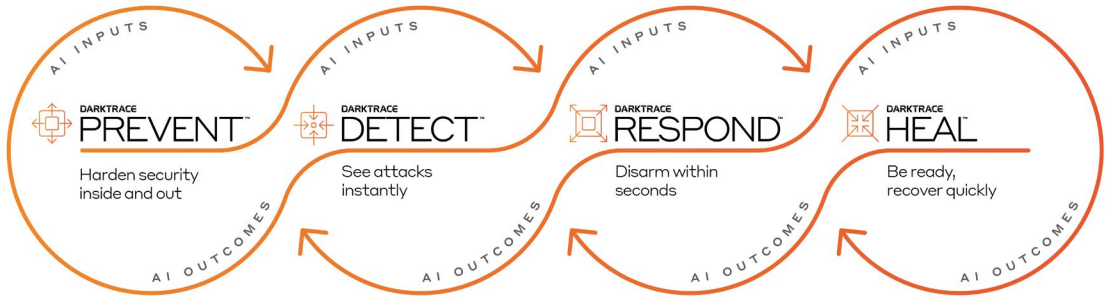
Centralizes and coordinates teams by integrating Darktrace HEAL with their teams' communications channel, enabling users to quickly gather the correct incident responders while easily transferring essential information.

Full Loop Incident Report

Save time with automatic report generation

Completed and planned HEAL actions, decisions, and notes are also automatically recorded and combined in an exportable PDF with incident analysis and containment information for a detailed report on the incident.

Darktrace HEAL completes the Cyber AI Loop, an always-on security ecosystem with autonomous feedback continuously improving the state of security.



Darktrace automatically feeds information from HEAL into the Cyber AI Loop during and after the incident to optimize future responses. By communicating with this ecosystem, the system can predict the next steps an attacker might take and harden defenses in preparation.

For example:

DETECT & RESPOND provide **HEAL** with critical context and active containment activity to inform HEAL decision-making

Recently healed assets are more closely monitored and safeguarded by **DETECT** for a certain time after the incident

HEAL leverages **PREVENT**'s context into critical attack paths and potential impact when prioritizing actions during the recovery process

Requirements: Darktrace HEAL requires Darktrace DETECT to be deployed across at least one of the following domains: Network, Cloud, Endpoint, OT

darktrace.com
info@darktrace.com

Scan to LEARN MORE