Darktrace/Network

DARKTRACE

AT A GLANCE:

- Respond faster to novel threats and abuses of trust
- Gain complete visibility of devices and their behaviors
- Reduce investigation time with AI-generated incident summaries

> Ransomware can spread across your network rapidly, so you need tools that can prevent that from occurring. **AI can autonomously take control and provide split-second reactions.**
>
> / CIO, City of Las Vegas

Self-Learning AI that understands your data

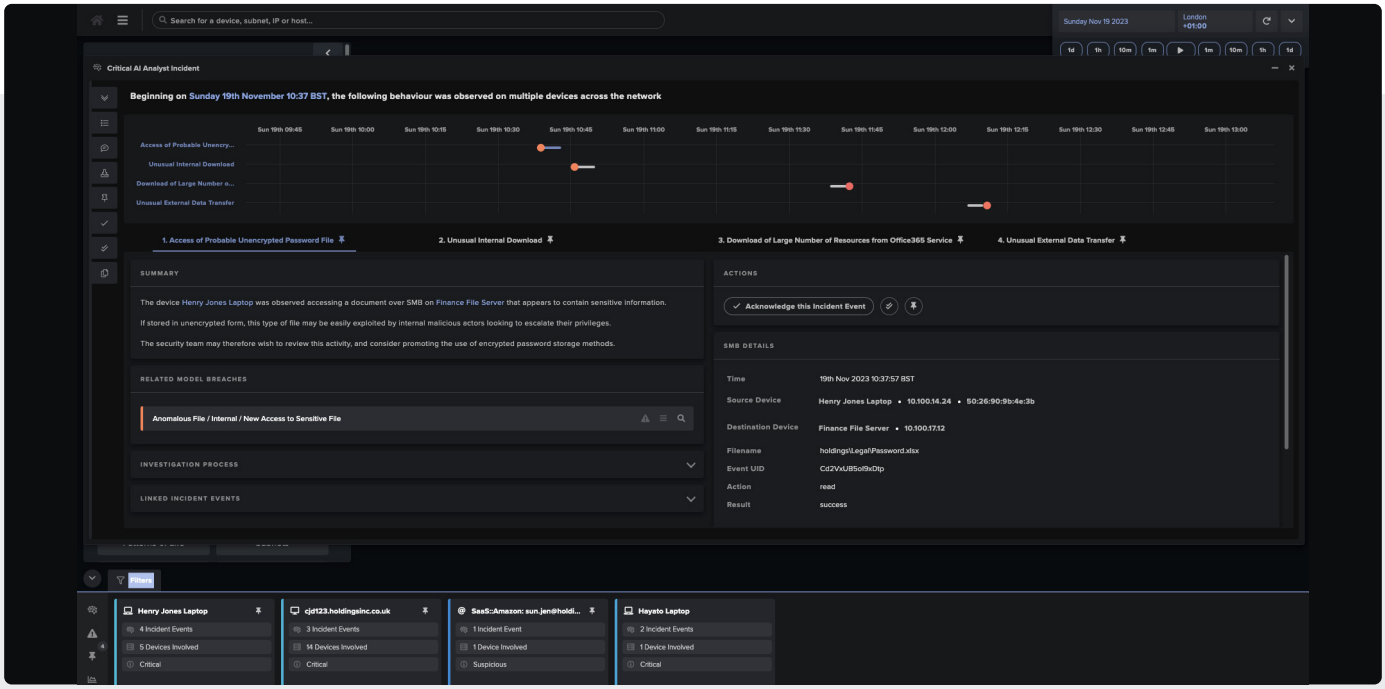
Where other cyber security solutions are trained to identify threats based on historical attack data and techniques, Darktrace/Network takes a fundamentally different approach.

It uses AI technology to build a dynamic understanding of 'normal' for your organization.

In doing so, it forms a bespoke and multi-dimensional understanding of every user, device, and all the complex relationships between them in your network.

Through learning the everyday dynamics of your organization, Darktrace/Network can identify the subtle deviations from normal activity that indicate emerging threats – both known and unknown. It can then take proportionate action to neutralize an attack within seconds, minimizing business disruption.

Darktrace/Network also combines with Darktrace's attack surface management and attack path modeling capabilities to allow defenders to prioritize on risk, while the AI hardens defenses around critical assets and attack paths.



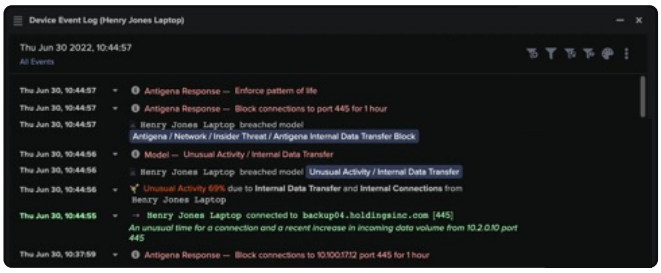
Neutralizes all network threats including:

- Ransomware
- Malware
- Novel Attacks
- Supply Chain Attack
- Credential Stuffing
- Crypto-jacking
- Insider Threat
- Mergers & Acquisitions

DARKTRACE / MITRE | ATT&CK

Maps to MITRE for immediate understanding

Darktrace/Network models are automatically mapped to the MITRE ATT&CK framework within the user interface to help teams classify the "what," "why," and "how" of cyber threats in their environments.



Reduce time to triage

Cyber AI Analyst connects individual threats to investigate attacks at speed and scale.

It uses Explainable AI built with natural language processing to produce understandable incident reports on critical events and the context around them.

For example, one customer has reported that AI Analyst gets its SOC team up to speed 20x faster.

In this way, your security team can save valuable time and direct their expertise to the high-value work that humans do best.

Autonomous response

Darktrace stops attacks in seconds with AI that minimizes business disruption by responding autonomously to attacks against networks.

It can take proportionate action; for example, blocking a specific connection over a port rather than quarantining a device. This allows business operations to run smoothly while remaining secure.

Autonomous response actions are customizable: users can set the parameters to determine how and when Darktrace should take action.

Features / Capabilities

- ✓ Easy to deploy, with hundreds of out-of-the-box AI models
- ✓ High-level triage down to low-level analysis around the clock
- ✓ Targeted, surgical responses
- ✓ Dozens of comprehensive integrations
- ✓ Fully configurable and customizable
- ✓ Can combine with Darktrace's attack surface management and attack path modeling capabilities

Gartner Peer Insights Customers' Choice 2022

Customers' Choice for Network Detection and Response

Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates.

Consolidate your Point Solutions with a Platform Approach

Cloud | Apps | Email | Endpoint | Network | Zero Trust | OT

Darktrace/Network combines with the rest of Darktrace's product suite, sharing insights across the digital estate to bring stronger, business-wide protection.

darktrace.com
info@darktrace.com

Scan to LEARN MORE