Coverage Area: Endpoint

Darktrace brings its Self-Learning AI to your data, wherever it resides. This enterprise-wide coverage includes endpoint devices, where the technology delivers real-time detection of novel and sophisticated attacks, automatic threat investigations, and – through its own agents – targeted, autonomous response.

Key Benefits

- ✔ Full visibility of endpoint devices
- ✔ Self-learning threat detection across the business
- ✔ Investigates data alongside email, SaaS, cloud and network
- ✔ Autonomous Response with Darktrace agents

> "Self-Learning AI investigates behavior on the endpoint alongside behavior in Microsoft 365 and across our entire cloud environment."

Head of IT Infrastructure, Scope Markets

Detects Novel and Sophisticated Threats

Darktrace AI is data-agnostic, and builds a rich picture of your digital estate from the ground up. By extending visibility to endpoints, host-level data can be investigated alongside events across email, SaaS, cloud and the corporate network, boosting Darktrace's overall understanding across these diverse environments.

Enriches Existing Endpoint Solutions

Darktrace AI can be extended to the endpoint through its XDR partners: Microsoft Defender, CrowdStrike Falcon, and Carbon Black. This allows rich host-level data and alerts to be analyzed by Darktrace's Self-Learning AI. With Darktrace, security teams benefit from the full context around the origin and scope of a security incident – as well as advice for remediation. Every security event is automatically investigated, reducing time-to-meaning by 92%.

Autonomous Response at the Endpoint

Through Darktrace's own agents, Darktrace brings its award-winning Autonomous Response capability to the endpoint, enabling AI to take targeted, autonomous actions to contain emerging attacks in seconds.

Applied to the endpoint, Darktrace continuously evolves its understanding of 'self' in order to identify advanced cyber-threats. This rich understanding allows for threats to be neutralized in a matter of seconds, without requiring the presence of human teams.

Crucially, response actions are precise and surgical, stopping emerging cyber-threats in their tracks, without disrupting normal business.