

Darktrace Immune System: Products and Services

Powered by self-learning AI, the Darktrace Immune System learns normal ‘patterns of life’ to protect against unknown and unpredictable cyber-threats. By understanding the digital DNA of an organization as it evolves, the technology is adaptive in its analysis and pervasive in its scope, operating across email, cloud, and collaboration platforms, as well as endpoints, IoT, and the corporate network. More than 5,000 organizations worldwide rely on Darktrace to illuminate and interrupt the full range of cyber-threats, from novel attacks to insider threats.

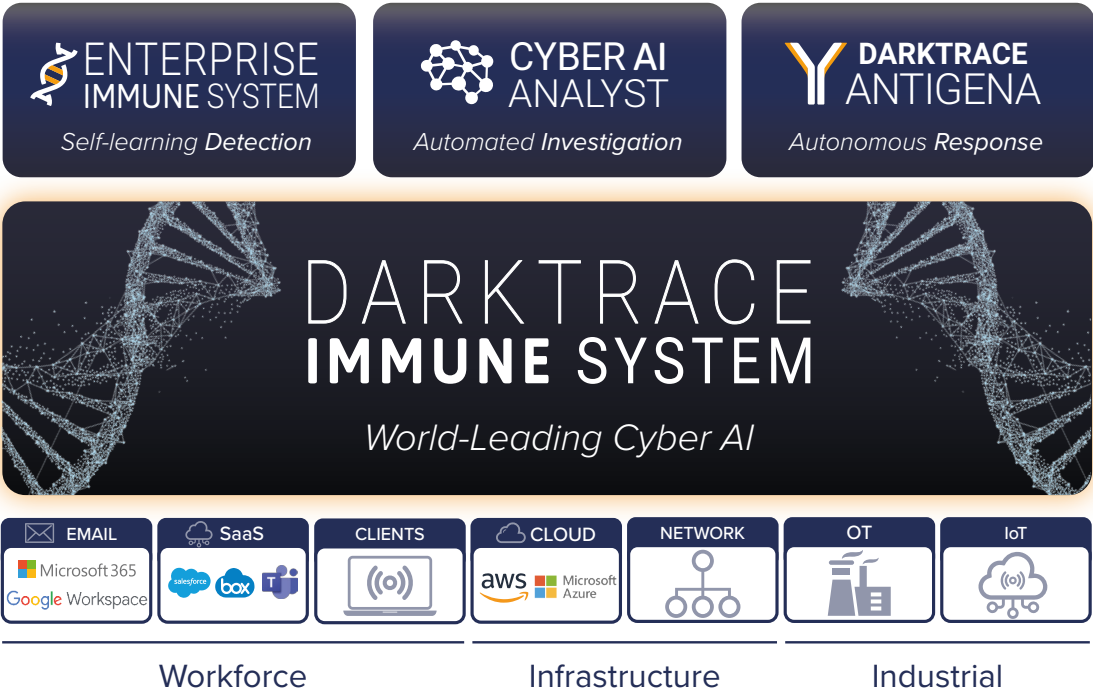
The Darktrace Immune System

The Darktrace Immune System is a core AI technology that leverages a combination of supervised and unsupervised machine learning in a unified platform, powering autonomous cyber-threat detection, investigation, and response.

Darktrace’s Cyber AI is self-learning, meaning that it does not rely on static rules or historical attack data but instead develops a continually evolving understanding of ‘normal’ for your dynamic workforce and diverse digital infrastructure. This includes unified protection across cloud, SaaS, and email platforms, as well as IoT, endpoints, and cyber-physical systems.

Like the human immune system, Darktrace’s ability to distinguish between malicious and benign behavior – without prior knowledge – enables it to identify cyber-attacks that would otherwise go unnoticed and unchecked.

With its Autonomous Response capabilities, Darktrace AI uses its bespoke intelligence to interrupt fast-moving attacks with surgical precision. By understanding 'patterns of life', Darktrace can instantly contain threats by enforcing ‘normal’ and sustaining typical operations by design.



The diagram illustrates the Darktrace Immune System architecture. At the top, three dark blue boxes represent core components: 'ENTERPRISE IMMUNE SYSTEM' (Self-learning Detection), 'CYBER AI ANALYST' (Automated Investigation), and 'DARKTRACE ANTIGENA' (Autonomous Response). Below these is a large central banner with a DNA double helix background, featuring the text 'DARKTRACE IMMUNE SYSTEM' and 'World-Leading Cyber AI'. At the bottom, a row of seven icons represents the system's scope: EMAIL (Microsoft 365, Google Workspace), SaaS (Salesforce, Box, T), CLIENTS (laptop icon), CLOUD (AWS, Microsoft Azure), NETWORK (network diagram icon), OT (factory icon), and IoT (cloud with sensor icon). These are grouped under three categories: 'Workforce' (covering EMAIL, SaaS, CLIENTS), 'Infrastructure' (covering CLOUD, NETWORK), and 'Industrial' (covering OT, IoT).

Cyber AI Analyst delivers AI Investigations that automatically triage, interpret, and report on the full scope of security incidents. By combining human expertise with the speed and scalability of AI, Cyber AI Analyst prioritizes incidents and writes reports that put teams in a position to take action.

Darktrace Product Suite



Enterprise Immune System: Self-Learning Threat Detection

- Learns normal 'on the job' to detect unknown and unpredictable cyber-threats
- Protects the dynamic workforce against zero-days, ransomware, and insider threats
- Covers the full digital DNA of an organization across cloud, endpoint, IoT, and the network
- Interfaces with Cyber AI Analyst to trigger autonomous investigations and reporting



Industrial Immune System: Identifying ICS Threats

- Learns normal 'on the job' to detect known and unknown malware, insiders, and operational risks
- Full visualization across OT, IT, and IoT, adapting as the environment evolves
- Interfaces with Cyber AI Analyst to trigger autonomous investigations and reporting
- Self-learning asset management across all vendors and technologies



Cyber AI Analyst: AI Investigation

- Augments human teams by automatically investigating the full scope of security incidents
- Writes reports that immediately put teams in a position to take action
- Combines the intuition and flexibility of human expertise with the speed and scalability of AI
- Investigations can also be triggered on demand or via third-party alerts
- Delivers time savings of up to 92% in time to triage



Antigena Network: Autonomous Response

- Takes surgical action to interrupt unpredictable and fast-moving attacks in seconds
- Operates dynamically, adapting to the threat as it unfolds
- Sustains usual operations during incidents by enforcing 'normal'
- Responds via self-directed actions or third-party integrations with existing defenses



Antigena Email: Autonomous Response

- Harnesses AI to 'understand the human' behind the email address
- Neutralizes malicious emails that other tools miss
- Stops spear phishing and impersonation attacks
- Surfaces AI Narratives that tell the story behind neutralized attack campaigns
- Cloud-delivered deployment and installed in minutes



Antigena SaaS: Autonomous Response

- Neutralizes unpredictable attacks in cloud and collaboration tools
- Decisions based on self-learning AI that 'understands the human' behind dynamic cloud accounts
- Reacts faster than any human, before damage is done
- Takes precise action while allowing the business to operate as usual

Darktrace Expert Services

A range of threat analysis and cyber intelligence services is available to customers, delivered by Darktrace Cyber Analysts or Darktrace Certified Partners. Darktrace Services are designed to cater to organizations of all sizes and across diverse industry sectors to give every company a custom fit.

Ask the Expert

- Rapid feedback and expert remediation advice from Darktrace Cyber Analysts
- Easy-to-use chat functionality
- 24/7 assistance

24/7 Proactive Threat Notification

- Comprehensive and proactive threat notification service around the clock
- Customer contacted immediately in event of attack
- Over 1,000 customers, covering both small and large companies
- Delivered by Darktrace Security Operations Centers (SOCs) in Cambridge, England, San Francisco, and Singapore

Immune System Integrations

The Darktrace Immune System harnesses an open and extensible architecture to seamlessly plug into your diverse ecosystem as it evolves. With one-click integrations, the platform can instantly ingest new forms of telemetry, share bespoke AI insights across established workflows, and interoperate with a wide range of technologies to deliver Autonomous Response across email systems, inline defenses, and collaboration platforms.

