Why Darktrace?

Darktrace fundamentally transforms the ability of organizations to defend themselves in the face of diverse cyber-threats. Developed at our R&D center in Cambridge, UK, Self-Learning AI is the only technology on the market that builds an understanding of your unique business, rather than attempting to learn breaches. This enables the AI to autonomously detect, investigate, and respond to novel and sophisticated threats across the digital ecosystem – without the need for human input or fine tuning.

Key Benefits

- ✔ **Self-Learning AI**
  Detects threats that others miss
- ✔ **Autonomous Response**
  Fights in-progress attacks 24/7
- ✔ **Protection Everywhere**
  Covers cloud, email, network, IoT, endpoints, and OT
- ✔ **Augmented Intelligence**
  Saves up to 92% of security analysts' time

Independent Recognition: Over 200 Awards

Recognized by leading independent bodies including Forrester, IDC, Marsh, Gartner, and The Royal Academy of Engineering for our ground-breaking developments in the field of AI cyber security.

Over 6,500 Global Customers

More than 6,500 organizations in over 100 countries rely on Self-Learning AI to protect their digital ecosystem, including cloud and SaaS, corporate networks and IoT, Operational Technologies and ICS, and email.

Figure 1: Darktrace provides complete visibility across the digital estate in real time

> "Darktrace thrives in complex digital environments as the technology is adaptive, enabling it to detect and respond to threats that other tools miss."
>
> Jonas Knudsen, Research Director, IDC

Self-Learning AI: Learns Your Organization, Not The Breach

Darktrace's entire product suite is powered by Self-Learning AI, a technology based on unsupervised machine learning. At its core, Self-Learning AI works by building an evolving understanding of your organization from scratch, allowing it to identify subtle outliers indicative of threat.

Whereas other tools rely on lists of historical, previously encountered cyber-attacks, Darktrace learns about your organization by observing how users, devices, and applications typically behave, forming patterns and continuously revising its understanding in light of new evidence.

An Evolving Understanding

The technology requires no a priori assumptions, pre-programmed responses, or threat intelligence. Instead, Self-Learning AI autonomously creates a bespoke understanding of your organization in real time, evolving with your business, even through times of sudden and unexpected change.

A self-learning approach is critical as the threats that get inside your digital ecosystem will typically not be historical attacks but either novel threats that have evaded your existing defensive tools or malicious or negligent insiders and suppliers. With its understanding of 'normal' at the user, device, and peer-group level, Self-Learning AI is able to detect the subtlest signals of malicious activity as it emerges.

> "Darktrace is a unique product where machine learning/AI plays a core part in protecting, detecting, and responding to threats."
>
> Marsh Cyber Catalyst Insurers

Why Self-Learning AI is Ahead of the Game

While there is a trend towards the use of AI in cyber security solutions, this mostly manifests itself as systems that are trained on historical attacks in order to recognize repeat occurrences effectively in the future.

AI that is programmed using training data sets only delivers marginal gains on traditional, rule-based systems that use signatures, heuristics, and threat intelligence.

Conversely, Self-Learning AI is able to surface in-flight attacks that other tools miss and then take the right action, at the right time, to interrupt that attack, significantly reducing the overall risk of the organization as well as complementing existing security investments.

Figure 2: Self-Learning AI autonomously detecting a zero-day ransomware attack and stopping it in seconds

Surgical Interruption of In-Progress Attacks

Powered by Self-Learning AI, Darktrace responds to in-progress cyber-attacks at machine speed, with Autonomous Response tailored to shut down the attack while allowing normal business operations to continue.

You Can't Plan a Response to Unknown Threats

Today's threat actors are frequently outpacing and outsmarting human teams and the tools they rely on, with attacks often striking out-of-hours when no-one is around to action a response.

This has led to automated response solutions – SOARs, IPS, firewalls – which rely on pre-defined threat lists to prevent attacks. This usually results in broad and heavy-handed actions, and it can be a major engineering activity to configure and keep these tools up to date. And most successful attacks today are novel in some way – meaning configurations will not be in place to defend against them.

Real-Time Action Based on an Evolving Understanding

Self-Learning AI calculates the best action to take, in the shortest period of time, to respond effectively to a cyber-attack. The technology can react to situations it hasn't encountered before to maintain your key security objectives.

Crucially, the AI decides how to surgically react for itself to stop the in-progress threats, without the need for human input: specifically targeting the 'bad' behavior, interacting with your existing defenses and infrastructure, and continuing to monitor the incident in case the attacker changes tactics.

Thousands of organizations worldwide rely on Autonomous Response technology to take fast, proportionate action against in-progress attacks. Today, Darktrace AI responds to a cyber-threat somewhere in the world every second.

Interrupting Ransomware in Seconds With AI

Darktrace takes highly targeted action to interrupt the spread of ransomware. Because the technology learns your business, not the breach, it knows how to contain only the malicious activity, avoiding the unintended disruption of normal business operations.

Ransomware is, at the time of writing, the number one threat vector that Darktrace AI responds to with its Autonomous Response capability. In addition, Darktrace for Email provides the first line of defense for ransomware by using AI to identify spear phishing attacks before they reach patient zero.

> "The ransomware that we are up against today moves too quickly for humans to contend with alone – the way we stay ahead is by having Darktrace AI fight back precisely and proportionately on our behalf."
>
> **CIO, Ted Baker**

Protection of the Entire Digital Ecosystem

Darktrace protects the entire digital ecosystem – safeguarding users and data wherever they operate. Technologies that claim to offer holistic protection of the workforce are usually the product of bolting various point solutions together, but this cannot offer the level of defense that a fully integrated, autonomous AI system can.

Darktrace thrives on complexity, with more users, devices, and environments adding extra insights and depth to its capabilities. With this understanding constantly evolving as your business grows, Darktrace helps you to build cyber resilience over time.

Darktrace's AI delivers protection across:

- Hybrid and multi-cloud environments
- SaaS and collaboration platforms
- Email systems
- Industrial environments, ranging from nuclear power stations to car manufacturers
- IoT environments, ranging from smart cities to global shipping
- Data centers, whether traditional or virtualized
- Endpoint devices, including remote workers on and off the VPN

As well as unifying detection, Darktrace enables full visibility of your infrastructure. For today's security teams, technology must facilitate the ability to explore and see what's going on in multiple environments at will – rather than just simply outputting security alerts. With the Threat Visualizer, your team will gain total visibility of behavior across every environment in your business in real time.

Evolves With Your Business

It is a core principle of our product roadmap to continue to expand Self-Learning AI to wherever our customers are taking their digital businesses: from cloud and collaboration tools to endpoint devices.

As our relationship with you develops, keep us up to date with your future technology plans and we will continue to develop the coverage that keeps your organization safe and builds resilience.

> "Darktrace AI adapts while on the job, illuminating our network and cloud infrastructure in real time, and allowing us to defend the cloud with confidence. Darktrace is the single most valuable security tool my team uses today."
>
> CISO, Aptean

Figure 3: Darktrace's AI detects and responds to threats across the full range of cloud infrastructure and applications

Significant Time-Savings, Augmenting Human Teams

Autonomous, AI-Driven Investigations

Darktrace's Self-Learning AI autonomously investigates security incidents, connecting the dots between disparate signs of attack across different technologies and infrastructures. It then relates them to the attack lifecycle, includes the actions taken by Darktrace, and produces a natural language report that can be stored for historical record, shared with teams that need to take action, or distributed to senior management.

Darktrace will not only surface high-fidelity leads for investigation but it will also autonomously investigate 100% of those leads as an expert cyber analyst would, but now with the consistency, speed, and scalability of AI. This means the security team can rapidly understand what is going on in even the most complex of environments, without the need for additional research.

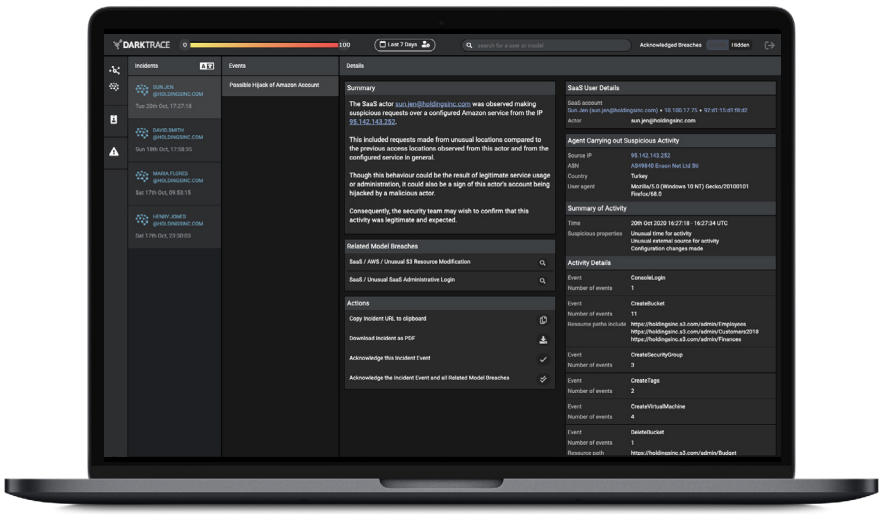

Figure 4: Cyber AI Analyst Incident Reports highlight the most pertinent information and provide a drill down into anomalies of interest

Freeing Up Time for Stretched Teams

The benefit to your organization is colossal: 100% of alerts are investigated and reported on in the language of your choice, 24 hours a day, 7 days a week. This enables your staff to focus on high-value, business-enabling, risk-management activities instead of mundane, in-the-weeds analysis that may be distracting from the company's core business needs.

By reducing triage time by up to 92%, security teams can quickly disseminate key intelligence, such as needed changes to firewalls or the desktops requiring clean-up, in just a few seconds after receiving the intelligence. They can also think more strategically about other preventative actions that could be taken to lower the overall risk to the organization.

There is no other vendor on the market able to offer autonomous, AI-driven investigation and analysis of cyber-threats.

> "Cyber AI Analyst has added real value to my team, especially the ability to launch on-demand investigations and query SaaS data or suspicious devices. The intelligence it gives us is clear and actionable."
>
> CISO, Calligo

Gartner Peer Reviews

"Working with Darktrace is nothing short of excellent. They provide a fantastic service, and their solution has been scaled as our network has moved into the cloud and staff working from home."

ICT Operations Manager, Services ★★★★★

"With Darktrace we have managed to prevent phishing attacks at a big scale, data loss prevention, and easily identify similar gaps in security. The products are qualitative, with great level of details [and] control."

Security Engineer, Services ★★★★★

"Darktrace is an essential component of our security platform, giving us unique and valuable capabilities to identify and remediate threats."

CTO, Financial Services ★★★★★

"Darktrace Antigena Email has proved an extremely reliable and effective solution."

CIO, Services ★★★★★

"If you take security seriously, you need this product."

IT Infrastructure Manager, Manufacturing ★★★★★

"Once deployed, you will find out that you have not seen anything before. The Darktrace appliance is fantastic."

Head of IT, Manufacturing ★★★★★

"Antigena was the exact solution we needed. It provided the organization with the benefits of an effective SOC without the costs, overhead, contractual risk, and implementation pains."

Senior Manager, Information Security & Compliance, Retail ★★★★★

"It is easy to use. Darktrace listens to its customers and continues to add features and improve its products. It is our first "go-to" for security."

Chief Technology Officer, Media and Entertainment ★★★★★

"Our business is able to view network traffic in fine detail, finally. With the integration of Antigena [...] we are able to leverage the force multiplier of machine learning as it relates to data security."

CIO, Government and Defense ★★★★★

"An advanced email security solution that does what others can't."

Director of Information Systems, Transportation ★★★★★

"Darktrace has quickly become my Threat Intelligence and Management team's favorite tool."

AVP – Enterprise Information Security, Financial Services ★★★★★

"Darktrace is visionary – the leadership team are engaged, and they continue to develop their capability."

Senior Director of Information, Miscellaneous ★★★★★