Why Partner With Darktrace as an MSSP

Darktrace’s world-class Self-Learning AI enables you to uplift and extend your security teams by providing autonomous detection, investigation, and response across your customers’ environments – allowing your team to focus on higher-level tasks that grow your business.

Key Benefits

✔ Detect Threats Others Miss
  Self-Learning AI that spots unknown attacks

✔ Autonomously Stop Attacks
  Fight in-progress attacks 24/7, without the need for human input

✔ Augment Human Teams
  Save up to 92% of analysts’ time

✔ Extend Existing Investments
  Seamless integration across the entire security stack for AI insights

✔ Streamline SOC Workflow
  100% visibility across the entirety of customer environments

Retrospective, Static, and Siloed: Why Current Defenses Are Not Enough

As the cyber-threat landscape has grown in complexity and scale, many organizations have turned to MSSPs to simplify the task of protecting their users, data, and infrastructure – relying on their partners to leverage the latest, cutting-edge technology to successfully combat novel and sophisticated threats.

But in practice, even ‘next-gen’ security tools are underpinned by the same old traditional approach to defense, relying on retrospective data sets and pre-conceived ideas of ‘bad’ to spot attacks. The difference between these solution and earlier defensive tools lies in tacked-on AI or machine learning at the end of product development – meaning they are able to spot known threats at greater speed and scale but are blind in the face of unpredictable attacks.

Furthermore, cyber security has evolved in silos, with isolated point solutions lacking the visibility and context needed to see how actions in one environment point to malicious activity in another. While many MSSPs deploy multiple solutions to traverse the full digital ecosystem, accidental gaps are inevitable – leading to unprotected users and data.

To compensate for this lack of contextual awareness, security teams are forced to take increasingly aggressive actions to contain the threat. In practice, this interrupts customer business operations when a proportionate and surgical response is needed.
How Darktrace Complements Existing Defenses

Learns on the Job

While traditional security tools are able to stop the majority of known threats, their reliance on historical attack data renders them unable to stop novel attacks that slip through the net.

Self-Learning AI builds an evolving understanding of its surroundings, spotting and stopping the full range of cyber-threats, regardless of whether the threat has been seen before. This includes advanced external attacks like ransomware, zero-days, spear-phishing, and supply chain risks, as well as compromised, careless, or malicious insiders with privileged access.

The technology learns ‘on the job’, developing an understanding of ‘normal’ for your customers’ digital ecosystems based on real-time data. It constantly evolves this understanding and protects users and sensitive data wherever it lives – across email, cloud infrastructure and applications, remote endpoints, industrial systems, and the corporate network.

Complements Existing Solutions

Darktrace harnesses an open architecture to seamlessly plug into diverse ecosystems as they evolve. With one-click integrations and custom templates, Darktrace can ingest new forms of telemetry, share bespoke insights across established workflows, and interoperate with a wide range of technologies.
Empowering Your Customers

Detects Novel Threats That Other Tools Miss

SIEM and EDR solutions are good for static use cases and malware-centric attacks. But in today’s new era of threat, organizations are facing much more complex attacks: targeted ransomware strains, zero-day exploits, supply chain compromises, spear-phishing, and insider threats, to name a few.

While Darktrace does detect known attacks, many customers love it for the ease with which it detects and stops never-seen-before and targeted threats. Real-world threat examples of this include autonomously stopping WastedLocker ransomware without signatures and identifying an APT41 intrusion 2 weeks before attribution.

Minimizes Cyber Disruption

Cyber-attacks are outpacing human security teams – with threats fully progressing in seconds, not minutes. As such, human response time is too long when dealing with ransomware encryption, rapid lateral movement, and data exfiltration.

While pre-programmed response solutions such as SOARs and EDRs attempt generally rely on hard-coded ‘if / then’ statements, Darktrace Antigena uses its inherent understanding of “self” to action a targeted response to contain threats without interrupting normal business operations.

Single Platform to Monitor Hard-to-Cover Environments

With Darktrace’s Threat Visualizer, MSSPs gain total visibility of behavior across every customer environment in real time – across hybrid, multi-cloud environments, email systems, industrial environments, endpoint devices, and many more.

Self-Learning AI thrives on complexity, with more users, devices, and environments adding extra insights and depth to its capabilities. Unlike traditional tools, Self-Learning AI correlates data points across the enterprise, continuously evolving and refining this understanding to provide contextual and dynamic defense that helps build cyber resilience over time.

Figure 2: Darktrace Antigena takes surgical and proportionate action to stop threats while maintaining normal business operations.
Coverage of Unknown Devices

SIEM and EDR solutions both excel at in-depth analysis of managed devices, but many threats come from parts of the digital business that neither SIEM nor EDR can cover: shadow IT, third-party devices, supply chain vendors, IoT and operational technology, BYOD, legacy devices, and devices which don’t support agents or loggers.

A fundamentally self-learning technology, Darktrace ingests all communication between assets within a given cyber ecosystem – meaning that devices, users, and data that security teams are unaware of will be protected as Darktrace learns ‘on the job’ from the data available in real time. Gaining coverage and visibility into these areas fills an important blind spot – leaving cyber-attackers nowhere to hide.

Customizable Defense Tailored to Your Customers

Some of your customers might prefer to dip in and out of the security solutions you operate. With Darktrace, they can easily do this – the user interface is designed to be light-touch and easy to understand. Even if a non-security person only has 10 minutes a day, they can gain a holistic understanding of their environment thanks to Darktrace.
Growing Your Business at Speed and Scale

Increased ROI, Cost Savings, and Efficiency Gains

Darktrace is highly efficient at detecting, investigating, and responding to cyber-attacks – no matter where or when they emerge. By using Self-Learning AI, you will achieve a much higher return on investment on your analysts.

Cyber AI Analyst, Darktrace’s AI investigation technology, automatically triages, interprets, and reports on the full range of security incidents, mimicking analyst intuition at AI speed and scale. It prioritizes the most relevant incidents and produces natural language threat summaries – putting your team in a position to take action.

Darktrace is designed to be easy to use, even for non-security specialists. This means junior analysts can quickly become highly-efficient threat hunters using Darktrace – they do not need a detailed understanding of the technology in the way SIEM and EDRs require to detect and escalate sophisticated attacks.

Create Easy, Impactful Services

It is easy to provide a 24/7 based monitoring service for your customers using Darktrace, with minimal analyst effort on your end. The technology uses machine learning to do the heavy lifting. This enables you to provide greater customization, be that dedicated, high-touch, premium threat hunting or bespoke threat use cases.

No Tuning, More Value, Faster Results

Darktrace is self-learning. This means it continuously revises its understanding of ‘normal’ in real time in order to grow alongside your customers’ businesses. While you can manually tune Darktrace, in most cases there is no need to. This enables analysts to spend time on what actually adds value.

Deploying Darktrace is extremely hands-off. It does not require upfront costs or resource investment in terms of configuration or tuning requirements. This means you can start showing value – real attacks, real threats, real security issues – to customers within 5-10 days after deployment.

World-Leading Support

Darktrace is committed to ensuring you have the support you need to succeed from day one, with dedicated account and alliance teams on hand. The Darktrace Global Partner Program empowers partners and their customers to keep pace with the evolving threat landscape.

Darktrace views our MSSP partners as part of a trusted community and an extension of our business. As such, you will have access to everything you need to thrive – from training programmes, to videos and documents on how to investigate incidents, to dedicated classes.

Figure 4: Cyber AI Analyst auto-generates Incident Reports that put teams in a position to take action

E: sales@darktrace.com  @darktrace  www.darktrace.com