Why Darktrace?

Core Differentiators

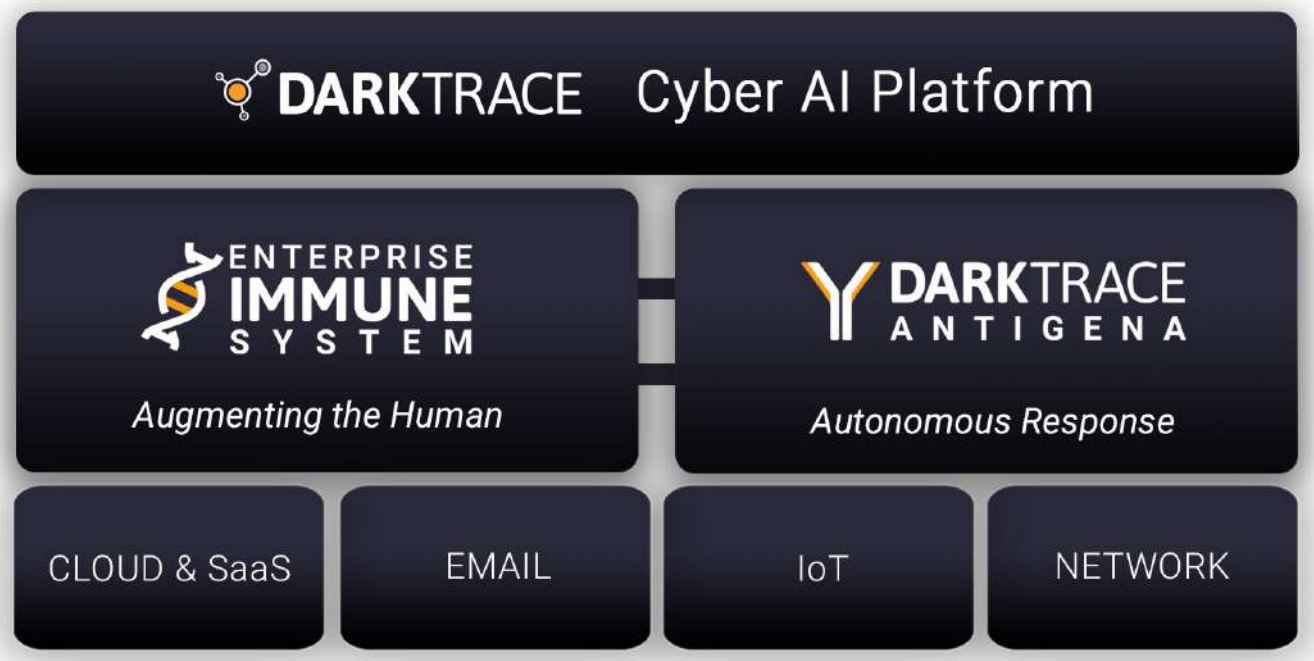
Darktrace is the only platform that:

- Learns normal 'on the job' to detect novel attacks and insider threats
- Provides unified and bespoke protection across email, cloud, IoT, and network
- Neutralizes attacks at machine speed and with surgical precision
- Automates threat investigations at speed and scale, reducing time to triage by 92%

The purpose of this document is to provide clarity on Darktrace's unique status within the area of AI for cyber defense. Founded and headquartered in Cambridge, Darktrace is a global technology company that has been at the cutting edge of Cyber AI for over 6 years.

In competitive trials or otherwise, businesses pick Darktrace time and time again because we can offer more coverage, faster detection, and – with Antigena – autonomous response. This is demonstrated by our $1.65bn valuation (as of Sept 2018) and market share, with over 3,000 companies around the world now relying on our technology to protect their global organizations.

Within this document we have provided some powerful independent analyst validation, most notably from respected industry specialist Alissa Knight, who in her recent report 'Patterns of Life' (Aite Group) states: "Darktrace is the only vendor I have ever awarded 5/5." We have also highlighted fundamental areas in which we are differentiated from other technologies that position themselves as competitive to Darktrace.



Unique approach and impact for your business

Based on our knowledge of other technologies on the market, Darktrace is unique in the following ways:

1. Darktrace is the only platform that learns on the job to create bespoke protection for your organization

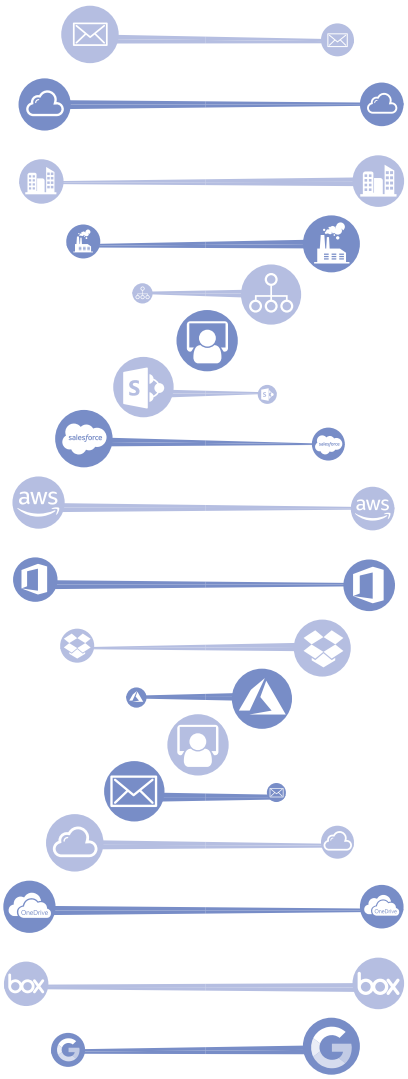
Attacks getting inside of organizations is inevitable in the current era, and finding these in-progress attacks by pre-conceiving of everything that might go wrong is no longer possible.

Darktrace uses the analogy of the human immune system – your protective defenses know about historical attacks and act like a protective skin, while the Enterprise Immune System complements this by learning about the people, systems, and data in your digital business and detecting the strange and unusual activities that are the hallmarks of an emerging attack. Fundamentally, we don't try and catch in-progress attacks because of what they look like, we catch them when they try to act.

Darktrace is the only company with technology that truly learns 'on the job', solely from your business. This creates a bespoke understanding of the 'DNA' of your organization to enable early threat detection. The threats that get inside your digital environment will typically not be historical attacks, but novel threats that have evaded your existing defense tools, or inappropriately behaving employees and third parties.

There is an increasing trend toward the use of AI in cyber security and in particular this manifests itself as AI systems being trained on historical attacks to be able to recognize repetition efficiently in future. Whether such an approach is applied on the endpoint as next-gen AV or in the networks and cloud, Darktrace believes this is just a marginal gain versus traditional systems that are derived from historical attacks to produce rules, signatures, heuristics, and threat intelligence.

Conversely the advanced threat detection approaches of the Enterprise Immune System are truly complementary to your existing investments and significantly reduce the overall risk of the organization by leaving attackers with nowhere to hide.



2. Darktrace is the only platform offering total coverage of your digital business

Darktrace became famous for bringing the immune system approach to networks, but we didn't stop there. It is a core objective of the product roadmap to continue to expand the immune system anywhere that customers are taking their digital business.

At this point in time, the immune system can cover:

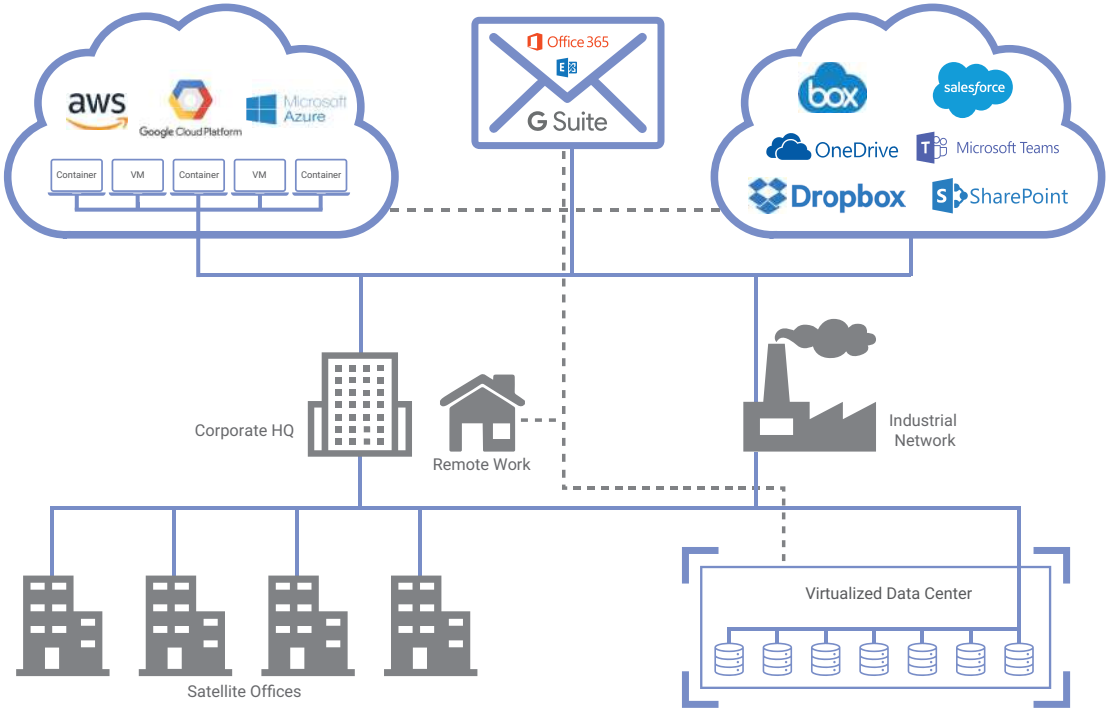
- Public and private cloud environments like AWS (with VPC Traffic Mirroring), Microsoft Azure (with the Azure vTAP), Google Cloud, whether traditional computing workloads or modern approaches like containers, kubernetes, etc.
- SaaS environments like Salesforce, Office365, SharePoint, OneDrive, Google Suite, Dropbox, Box, etc.
- Email systems so that in-progress attacks that come from malicious emails can be tracked and interrupted after the first victim (patient zero) not the 200th.
- Industrial environments ranging from nuclear power stations to chocolate factories to car manufacturers and Formula 1 racing teams.
- IoT environments ranging from smart buildings and smart cities to semi-autonomous global shipping, and soon will extend into Earth's orbit on swarms of micro-satellites.
- Data centers whether traditional or virtualized, ranging from small to enormous.
- And of course, campus networks, where it all started.

Increasingly, threat actors aren't limiting their attacks to one technology at a time, and as defenders it is essential that protections are unified across one's entire digital business. Something as simple as a compromised password can result in an attack against multiple facilities at once. Being able to see this in real time is essential for meaningful incident management – it no longer makes sense to handle security on a per-technology basis.

As well as unifying detection, Darktrace believes strongly in enabling full visibility. For today's security teams, tooling must facilitate the ability to explore and see what's going on in multiple environments at will – rather than just simply outputting security alerts.

As our relationship with you develops, keep us up to date on your future technology plans and we will continue to develop the coverage that keeps the business safe at the speed at which you want to modernize.

> "Darktrace software flags cyber-threats within cloud-integrated networks – regardless of where they originate."
>
> **- Forrester**



3. Darktrace Antigena is the only technology that can interrupt attacks in seconds, even if you've never conceived of them in advance

Many customers find that their incident responders are under immense time pressure to react to fast-moving or out-of-hours attacks. Whilst it's common for the market to offer integrations into workflow or SOAR systems for taking actions (this is also possible with Darktrace's immune system), all of these workbooks have to be specifically configured by your team and can be a major engineering activity to produce and keep up to date.

Autonomous response is the next level of maturity where our platform can react to situations it hasn't encountered before to maintain your key security objectives. Perhaps that is interrupting lateral movement, ransom attacks on data, or ensuring that unexpected data loss is always suspended until the security team has a chance to investigate.

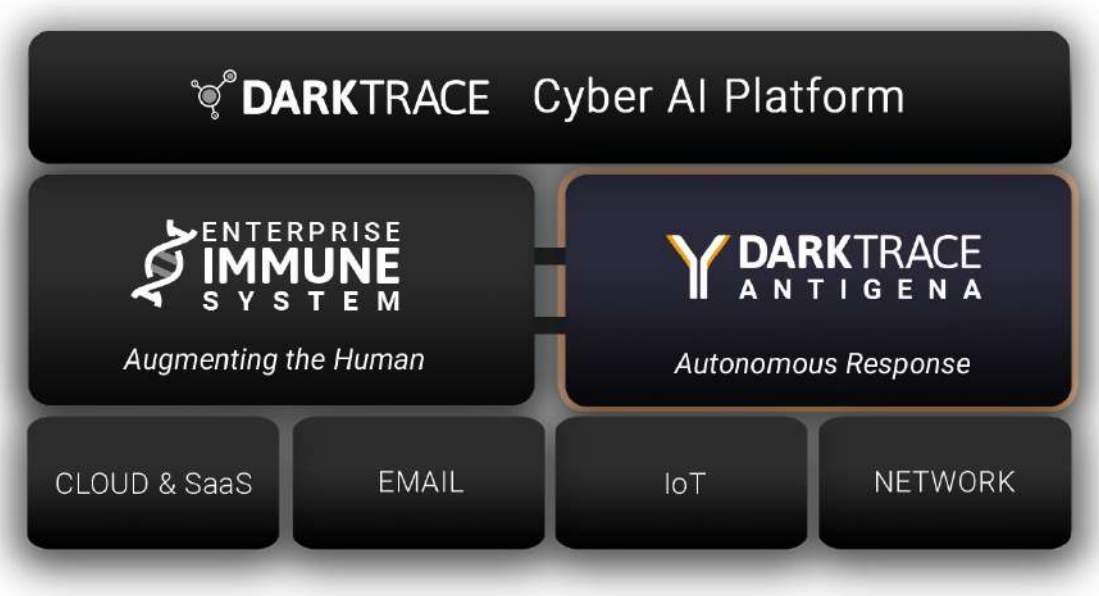
And crucially, the system decides how to surgically react for itself: specifically targeting the bad behavior, interacting with your existing defenses and infrastructure, and continuing to monitor the incident in case the attacker changes tactics and further intervention is needed.

This is only possible because the platform has truly learned on the job to understand how your business operates. This means that infected systems can remain in the network without being a threat, while allowing employees and systems to continue to perform their roles.

Darktrace invented Autonomous Response in 2016, and it is now in use in hundreds of customer networks worldwide. Today, Antigena is responding to a cyber-threat somewhere in the world every 3 seconds and the concept has been embraced by Gartner as a key goal of security modernization for the future.

In addition to taking actions within networks and cloud (available now) and SaaS (available in next release v4.1), Antigena Email expands this protection into email. By correlating the AI's understanding of the infrastructure, SaaS, and email environment, Darktrace is in the unique position of being able to detect an infection in any environment, and automatically perform root cause analysis to see if this originated via email. If so, it will instantly protect all other employees.

We call this strategic autonomous response – where learning from Patient Zero enables the strategic protection of the rest of the business, without human intervention. From an operations perspective, someone still needs to clean up the laptop of the first victim, but that's much better than cleaning up 200 or worse.



4. Darktrace augmentations offer AI-driven investigation at speed and scale

Many teams are under significant time pressure and don't have resources available to conduct full investigations into security events. This can sometimes lead to important facets of incidents being overlooked. Maybe some of the command and control activities are missed, maybe additional devices are infected but are overlooked. Or perhaps valuable time is spent documenting incidents rather than spent managing risk.

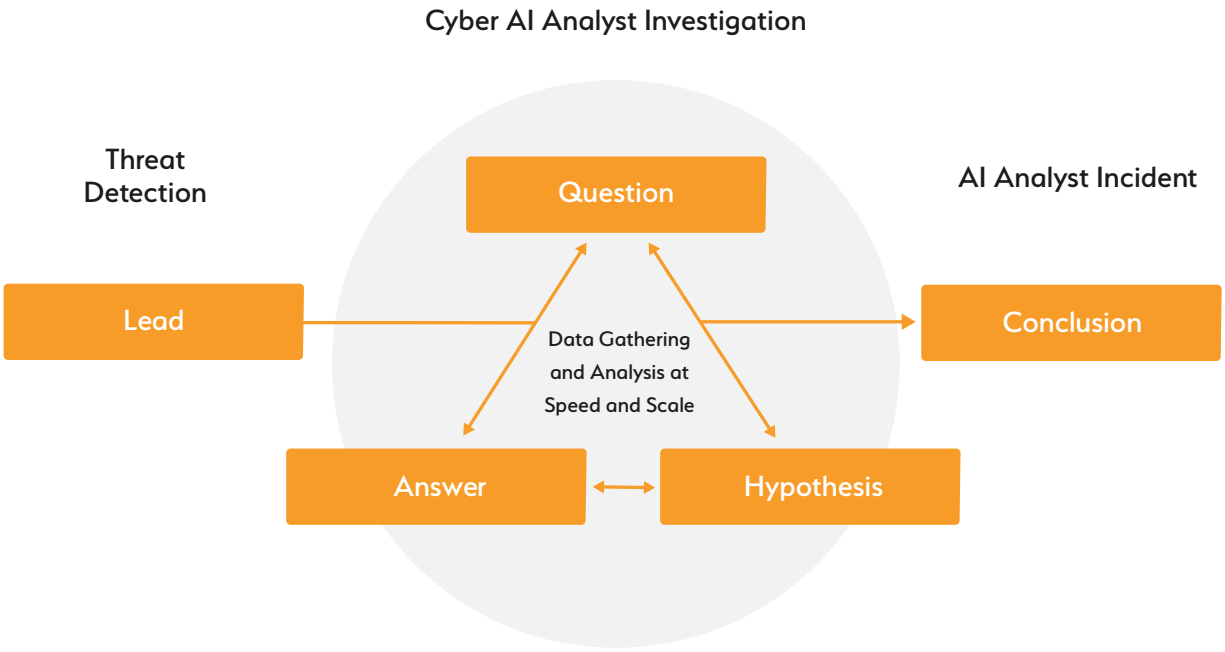
Darktrace's recent release of the AI Analyst now provides for full investigation of incidents to automatically connect the dots on the signs of attacks across different technologies and infrastructures, relating them to an attack lifecycle, including autonomous responses, and producing both a dynamic situational dashboard and written reports (in sentences and paragraphs) that can be stored for historical record, shared with teams that need to take action (e.g. network team for blocking, or desktop team for clean-up), or shared with management.

So not only will the platform surface high-fidelity alerts/leads for investigation, it will also automatically investigate 100% of those leads in a similar way an expert human 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 environment, without the need for research.

Take a moment and let this sink in; 100% of alerts are investigated and reported, in the language of your choice, 24 hours a day, 7 days a week. This enables your human 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.

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 of receiving the lead/alert. They can also think more strategically about other preventative actions that could be taken to lower the overall risk for the organization.

According to Chris Kissel, Research Director at IDC, "By automatically investigating security events, the AI Analyst helps reduce noise more than any other technology." There is no other vendor in the marketplace able to offer the same AI-driven investigation and analysis of cyber-threats.



Independent Validation

At the 2019 Gartner Security and Risk Management Summit, a senior analyst at Gartner, David Mahdi, made the case for AI-enabled autonomous response in the conference's opening keynote presentation. In addition, a second Gartner analyst, Lawrence Pingree, in his keynote stated that "the next phase in our journey toward autonomous security is autonomous response decision-making."

While it is of course important that Gartner has acknowledged autonomous response as essential in today's cyber-threat landscape, Darktrace was the company that pioneered autonomous response against emerging cyber-threats and has done so for the last 3 years.

Aite Group's 'Patterns of Life' report (available upon request) mentions Darktrace in the context of other technologies. The author is Alissa Knight, a well-respected security expert and practitioner who is frequently quoted in top-tier publications, such as Forbes. Key quotes include:

On Technology and Competition

"After having reviewed all the solutions available, it's my opinion that Darktrace is one of the few in the network threat analysis space doing it right. Its ability to see and autonomously respond to the known knowns and unknowns is unparalleled by any other product out there and, with its expanded capabilities, has ushered Darktrace to the leader of the pack in the network threat analysis team of rivals."

"Based on the resulting scores from each category, my overall score for the Darktrace solution is a five out of five and is the first time I've ever given a perfect score to any vendor."

Feature	Rating out of a possible 5
Installation	●●●●●
UX	●●●●●
Prevention	●●●●●
Components	●●●●●
Architecture	●●●●●
Detection	●●●●●
Support experience	●●●●●
Pricing	●●●●●
Overall	●●●●●

Source: Aite Group

On Technical Support

It is worth highlighting that technical support is provided as standard to all Darktrace customers at no additional cost. Based on conversations with a Darktrace customer, Knight observed:

"The customer has had zero complaints regarding its interaction with Darktrace technical support. Unlike other vendors it has worked with, every support engineer it has historically interacted with over its three-year relationship with Darktrace has been a senior engineer with event analysis experience."

"A customer will initially be assigned an analyst dedicated to the account and, in the customer's experience, it has been a senior analyst with deep knowledge of security event analysis and the product itself. According to the customer's experience with the support personnel, Darktrace engineers have always had a deep understanding of packets, ports, threats, etc., which isn't typically emblematic of vendors it has worked with in the past. Darktrace was very hands-on the first month the customer had the device."

> "My overall score for the Darktrace solution is a five out of five and is the first time I've ever given a perfect score to any vendor."
>
> **- Aite Group**

Conclusion

Darktrace is the inventor of self-learning AI systems for cyber defense, and by market capitalization and number of customers is the clear leader in the field. We have the broadest product set to support your full business setup, with a heavily invested, fast-moving product development arm. Recent breakthroughs like AI Analyst, just six months after the release of Antigena Email, show that our appetite and ability to solve real-world customer problems is huge.

We are proud to be one of the world's leading technology companies operating on a global scale. Industry experts and analysts agree that while other technologies are starting to adopt our approach, none has been able to develop the capability, deployability, and usability that we are world-renowned leaders for. With over 3,000 customers in every industry vertical, our platform is transforming the way enterprises are protecting their digital infrastructure.

Core Differentiators

Darktrace is the only platform that:

- Learns normal 'on the job' to detect novel attacks and insider threats
- Provides unified and bespoke protection across email, cloud, IoT, and network
- Neutralizes attacks at machine speed and with surgical precision
- Automates threat investigations at speed and scale, reducing time to triage by 92%

> Darktrace's ability to see and autonomously respond to the known knowns and unknowns is unparalleled by any other product out there and ushered Darktrace to the leader of the pack in the network threat analysis team of rivals.
>
> **- Aite Group**

For more information:

Book a demo now

Download Antigena White Paper

Hear from our customers