Darktrace Antigena

Darktrace Antigena is the world's first proven Autonomous Response technology for the enterprise. The system operates as an AI decision-making framework that neutralizes fast-moving and unpredictable attacks in seconds, while sustaining normal operations by design.

Key Benefits

- ✔ Makes decisions and takes action to stop fast-moving and unpredictable attacks
- ✔ Responds dynamically and adapts to persistent and creative techniques
- ✔ Sustains normal operations during incidents with surgical response
- ✔ Reacts faster than automated attacks and human responders
- ✔ Operates across email, network, and collaboration tools

The Limitations of 'Automated' Response

Security teams in the digital age are overwhelmed, under-resourced, and ill-prepared for the shape of things to come. Cyber-threats have become increasingly automated and unpredictable, and digital environments have become more complex and diverse. Together, these trends have limited our ability to predict how future attacks might manifest themselves inside an organization and respond effectively.

The complexity of digital business and speed of new-age attacks means that many foundational aspects of threat protection are no longer a human-scale problem; most of the industry agrees that meaningful improvements in this area will come in large part from intelligent automation. Yet, 'automated' response technologies – from SOAR and AV, to CASBs, IPS, and email gateways – have delivered a fundamentally limited form of augmentation in practice.

While these tools can be useful, they all share a crippling reliance on policies, playbooks, and historical attack data to generate a pre-programmed response. These technologies might react faster than humans, but their static and pre-programmed nature often leads to unreliable detections, clumsy quarantines, and brittle actions in the face of hands-on operators or machine-speed ransomware that sweep through large and complex infrastructure in seconds.

Darktrace Antigena: Autonomous Response

Throwing more humans at the problem is no longer a viable option, yet the adoption of pre-programmed automation has merely caused more disruption, created more human work, and failed to account for unexpected attack scenarios.

To address these challenges, Darktrace Antigena delivers adaptive Autonomous Response that harnesses the power of artificial intelligence to respond to novel attacks with surgical precision. When the Darktrace Immune System detects an emerging threat, Antigena acts in seconds to interrupt the attack before it can escalate, while adapting as and if the threat develops or switches to fallback mechanisms.

Autonomous Response operates as a dynamic, self-learning framework that decides the appropriate response to attacks in light of an evolving and far-reaching understanding of your unique digital environment. Attackers rarely confine themselves to a silo, which is why Autonomous Response not only operates intelligently, but also makes decisions and takes action across diverse digital environments – from email, cloud, and collaboration tools, to IoT and the corporate network. This leaves attackers with nowhere to hide and meaningfully reduces the overall risk of an organization.

Responds to Unpredictable Attacks

The rules, policies, and playbooks that power pre-programmed response tools not only generate unreliable detections, but also only respond to attack scenarios that humans have conceived of in advance. For the unpredictable threats that get through, Darktrace Antigena leverages self-learning AI to recognize and react to high-fidelity detections without human intervention.

This is only possible because the underlying AI technology learns 'on the job' how your organization operates, enabling an Autonomous Response that can reliably neutralize the full range of attacks that deviate from an organization's 'patterns of life' – from novel strains of ransomware and targeted phishing campaigns, to insider threats and unexpected data loss, and even to APT attacks leveraging zero-day vulnerabilities.

Takes Dynamic and Surgical Action

Pre-programmed response tools typically take action via a simple block or broad-brushed quarantine. This applies a one-size-fits-all approach and inevitably leads to actions that are either too disruptive – as even a minor signature match could get a client kicked off the network – or too brittle, as a pre-programmed response is unable to adapt to the digital maneuvers of polymorphic malware or a resourceful insider.

By contrast, Autonomous Response is grounded in self-learning technology that learns and adapts to the people and patterns in an organization as it evolves. In the face of persistent attacks, self-learning AI enables Darktrace Antigena to dynamically adapt to the shape of a threat as it unfolds, responding proportionately to real-time behavior.

Autonomous Response is a fundamentally surgical technology. By understanding normal behaviors and relationships, the AI need only enforce the 'pattern of life' of an infected device, suspicious email, or compromised user to neutralize an attack while maintaining operational integrity.

Reacts at Speed and Scale, 24/7

Time is of the essence in incident response, and a blunt, automated action or delayed human response can often lead to devastating business interruption or critical data loss. Yet even a global team of human operators managing a patchwork of static point solutions are no match for advanced attacks that hide across systems, leverage legitimate credentials, or break down the doors and move laterally in seconds.

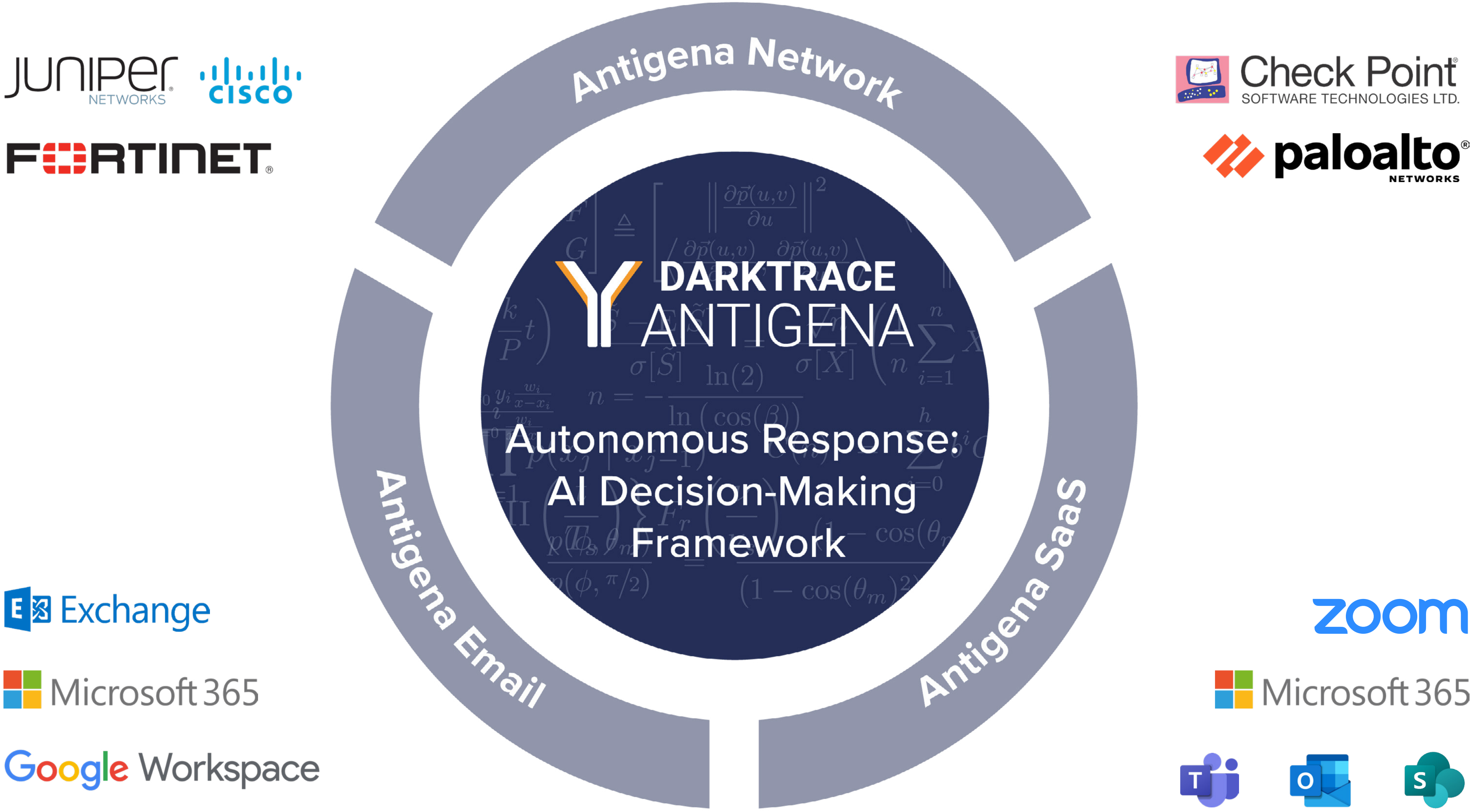
Darktrace Antigena not only reacts to unpredictable attacks with dynamic and surgical precision but also operates everywhere at once – 24/7, without getting bored, tired, or distracted. Depending on your deployment scenario, its scope can also span the full digital DNA of an organization and its workforce.

This breadth enables Autonomous Response to protect organizations at scale, without adding any overhead in terms of managing rules, signatures, scripts, or playbooks. With self-learning AI, the system can respond autonomously and surgically, whether the attack involves a spear phishing campaign, compromised credentials, ransomware, or a disgruntled employee stealing data in the cloud or corporate network.

> "The next phase in our journey towards autonomous security is Autonomous Response decision-making."
>
> Lawrence Pingree, Research VP, Gartner

Darktrace Antigena Product Suite

Darktrace's Autonomous Response technology provides an AI decision-making framework that can be deployed via three distinct yet interoperable products: Antigena Network, Antigena Email, and Antigena SaaS.



Antigena Network

Antigena Network neutralizes novel attacks and insider threats across the corporate network and Internet of Things.

While pre-programmed response tools tend to rely on simplistic pattern matching and static logic, Antigena Network's decisions are informed by an ever-evolving understanding and awareness of normal and benign behavior. In this way, self-learning AI delivers a categorically different response that understands how, when, and where to neutralize an emerging threat, while allowing the business to operate as usual.

This also means that Autonomous Response can be effective across a diverse variety of threats – even those that are novel and unexpected – and can scale up to protect large and complex organizations without introducing more human work.

Core use cases include:

- **Machine-speed ransomware** – Contains novel strains of malware and ransomware before they can escalate.
- **Insider threat and account takeover** – Interrupts malicious insiders and unexpected data loss.
- **IoT compromise** – Stops attacks from spreading or exfiltrating critical data via IoT devices.
- **Compliance** – Can be configured to respond to non-compliant behavior and connections.

> "Darktrace Antigena can autonomously and precisely contain in-progress attacks far quicker than our human teams can, ensuring our operations stay on track."

Shane Wilcox, Information Systems Manager, Layton Construction

AI Decision-Making

While each decision is grounded in Darktrace's core, self-learning AI, the range of actions Darktrace Antigena can take falls into one of two broad categories of response:

Tactical Response

With Tactical Response, Antigena Network generates self-directed actions that neutralize attacks in seconds. Each response is surgical and anchored in the system's granular understanding of 'normal' for every user, device, and peer group, as well as the organization as a whole. This enables Darktrace Antigena to intelligently judge which events merit Autonomous Response, while maintaining business as usual during incidents.

Strategic Response

With Strategic Response, Antigena Network acts as the 'AI brain' of the entire security stack, leveraging high-confidence detections to hand off and integrate with third-party systems as a mechanism for response. Through active integrations, Antigena Network can seamlessly plug into and enhance your existing security stack, informing firewalls and network devices about attacks that have gotten through.

FORTINET

paloalto NETWORKS

Check Point SOFTWARE TECHNOLOGIES LTD.

JUNIPER NETWORKS

CISCO

Antigena Email

Antigena Email is a self-learning technology that neutralizes targeted email campaigns and impersonation attacks that evade the email gateway.

By understanding normal 'patterns of life' for every user and correspondent, Antigena Email is the only technology that truly 'understands the human' behind email communications. This enables the AI to intelligently determine whether a given email meaningfully deviates from normal interactions between sender, recipient, and the wider organization, instantly revealing the subtle signs of a novel threat.

Unlike static gateways, Antigena Email treats recipients as dynamic individuals and peers when analyzing inbound, outbound, and lateral email traffic. When the AI identifies a threat, Antigena Email responds autonomously and proportionately, making a unique decision for each email to ensure legitimate mail flow is always allowed to continue.

Core use cases include:

- **Spear phishing and payload delivery** – Neutralizes malicious links and attachments in targeted phishing campaigns.
- **Social engineering** – Responds to visually similar domains and solicitation attempts, even in 'clean' mail without payloads.
- **Supply chain risks** – Recognizes and reacts to external account takeover of trusted contacts.

> "We were shocked by the things our traditional tools didn't catch that Antigena Email did."

Gabe Cortina, CTO, Bunim/ Murray Productions

Surgical 'Set and Forget' Technology

While pre-programmed tools require maintenance and manual corrections, Antigena Email's surgical decision-making enables the solution to be a truly 'set and forget' technology.

By adapting to evolving behavioral patterns autonomously, Antigena Email can accurately distinguish between benign and malicious, and instantly determine the most appropriate action for each unique situation. This self-learning understanding allows the technology to neutralize malicious emails before they can make an impact, while greatly reducing or directly off-setting admin workload.

Antigena Email Dashboard and Narratives

For operators who wish to gain seamless oversight of their email risk profile and trends over time, Darktrace offers a dedicated dashboard designed to illuminate the bigger picture and influence an organization's security strategy accordingly. Key areas of focus include metrics on which users are most exposed and in what ways an organization may be at risk.

Antigena Email also generates digestible, natural language Narratives that tell the story behind neutralized attack campaigns. These Narratives are surfaced in plain English and allow operators to quickly understand what happened and why – without having to make sense of the raw data.

Microsoft 365 Exchange

Gmail Google Workspace

Antigena SaaS

Antigena SaaS neutralizes unpredictable attacks in cloud and collaboration tools.

From Microsoft Teams to SharePoint, Antigena SaaS responds with surgical precision when trusted cloud accounts are being used carelessly or for malicious purposes.

Unlike policy-based defenses, the technology takes action in light of a multidimensional understanding of digital behavior across hybrid and multi-cloud environments. This enables swift and targeted action that stops SaaS attacks while allowing normal business operations to continue unimpeded. Security operators investigating unusual SaaS activity can also trigger Darktrace Antigena actions directly as desired.

Core use cases include:

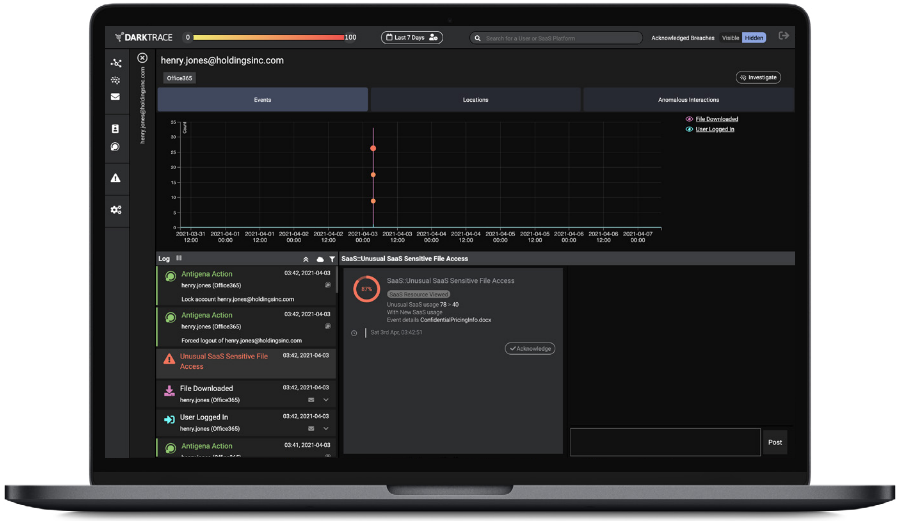
- **Insider threat** – Neutralizes admin abuse and insider data theft.
- **Compromised credentials** – Surgically interrupts account takeovers and brute-force attacks.
- **Remote personnel risks** – Stops accidental data loss, manipulation, and destruction.

> “I rely on Darktrace to be autonomous and just sit there, do its thing, and stop threats quickly. You could pay another person to sit there 24/7 and you still wouldn’t get the same value, and that’s especially true of Autonomous Response for cloud services and collaboration tools.”

John Wager, Head of Technology and People, Saddleback

Darktrace SaaS Console

The Darktrace SaaS Console is a dedicated user interface designed to highlight malicious or risky behavior occurring across your diverse cloud footprint. This allows security teams to visualize and monitor security incidents and Antigena SaaS actions in one centralized location.



Antigena Action 03:42, 2021-04-03
henry.jones (Office365)
Lock account henry.jones@holdingsinc.com

Antigena Action 03:42, 2021-04-03
henry.jones (Office365)
Forced logout of henry.jones@holdingsinc.com

Unusual SaaS Sensitive File Access 03:42, 2021-04-03

File Downloaded 03:42, 2021-04-03
henry.jones (Office365)

User Logged In 03:42, 2021-04-03
henry.jones (Office365)

Antigena Action 03:41, 2021-04-03

SaaS::Unusual SaaS Sensitive File Access

SaaS::Unusual SaaS Sensitive File Access
SaaS Resource Viewed
Unusual SaaS usage 78 > 40
With New SaaS usage
Event details ConfidentialPricingInfo.docx
Sat 3rd Apr, 03:42:51

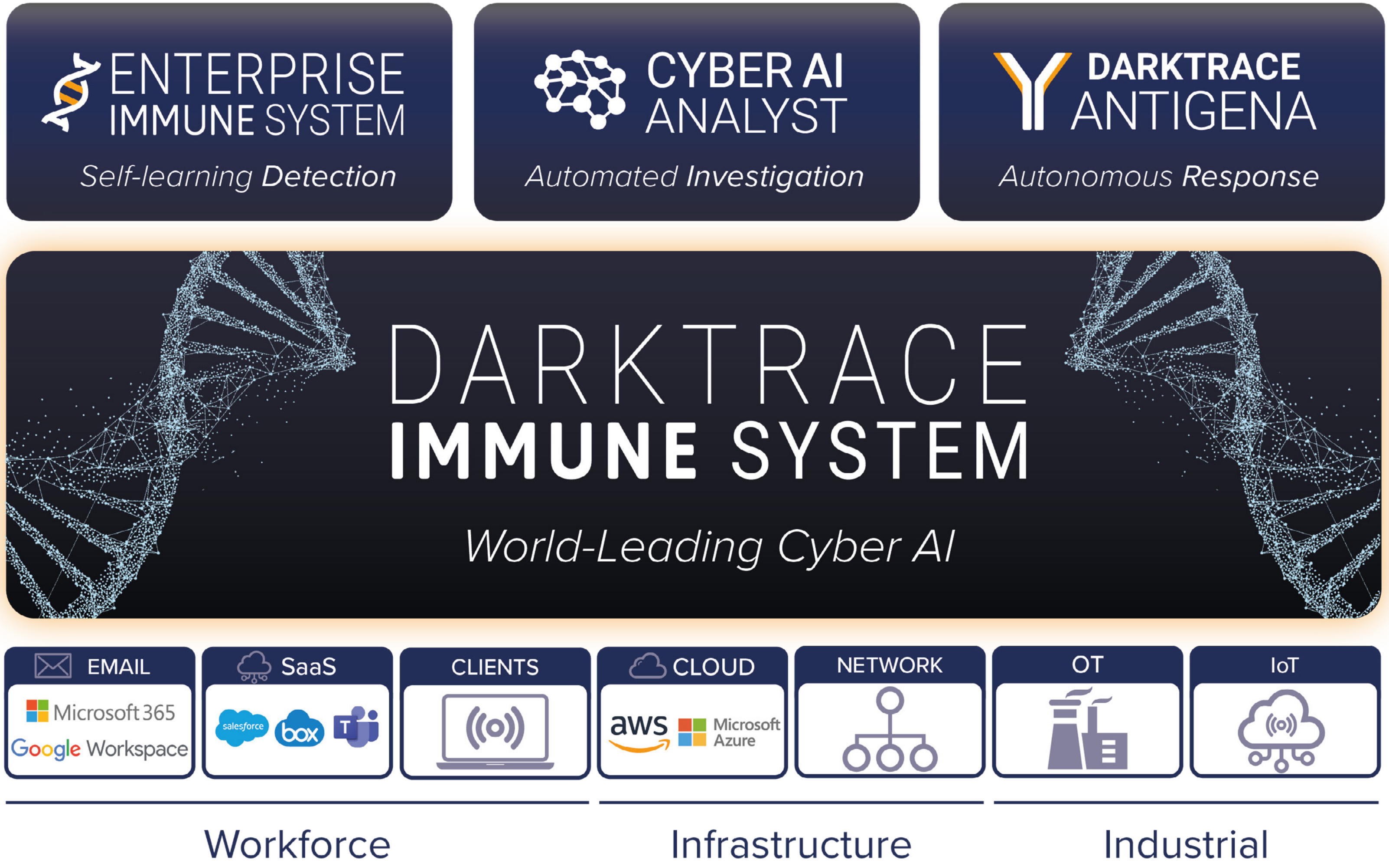
Antigena actions displayed in the SaaS Console.

Microsoft 365 OneDrive zoom

Microsoft Dynamics 365

Darktrace Immune System Platform

Darktrace Antigena operates as an Autonomous Response framework embedded in a wider self-learning platform. The Darktrace Immune System serves as the core self-learning technology that powers early threat detection, Cyber AI Analyst investigations, and Antigena actions to protect an organization's dynamic workforce and diverse digital infrastructure.


ENTERPRISE IMMUNE SYSTEM
Self-learning Detection
CYBER AI ANALYST
Automated Investigation
DARKTRACE ANTIGENA
Autonomous Response
DARKTRACE IMMUNE SYSTEM
World-Leading Cyber AI
EMAIL
Microsoft 365
Google Workspace
SaaS
salesforce
box
CLIENTS
CLOUD
aws
Microsoft Azure
NETWORK
OT
IoT
Workforce
Infrastructure
Industrial