Cyber AI Platform

Darktrace Antigena

Powered by Darktrace's world-leading AI, Darktrace Antigena is an award-winning Autonomous Response solution that responds to cyber-threats in real time. Working in conjunction with the Enterprise Immune System, it generates actions that are proportionate to the threat level detected and effectively counters the attack, allowing business operations to continue as usual.

Key Benefits

- ✔ Stops an attack spreading in real time
- ✔ Surgical response
- ✔ No disruption to your business
- ✔ Customizable
- ✔ Buys you time to catch up

Neutralizes Threats in Seconds

Thousands of new threats are halted each day, including:

- ○ Hacked IoT devices
- ○ Compromised credentials
- ○ Advanced spear phishing attacks
- ○ ICS and SCADA compromises
- ○ Zero-day attacks
- ○ Cloud misconfigurations

Building Trust with the Mobile App

The Darktrace Mobile App allows you to build trust in Antigena at a pace that suits you. Available in two customizable modes, you can tailor Antigena to your risk appetite, and stay informed on the move.

Human Confirmation Mode – gives users the option to confirm Antigena's recommended actions to build trust.

Active Mode – acts autonomously within its defined operating parameters, without the need for the security team to log on.

Autonomous Response: The Machine Fights Back

As cyber-attacks get faster and more advanced, security teams are overwhelmed and outpaced. Autonomous Response technology changes the stakes for defenders by giving you the ability to contain fast-moving threats, even when you are not in the office and cannot respond fast enough.

Darktrace Antigena works like a digital antibody, intelligently generating surgical responses to cyber-attacks across your digital environments. It does this by mathematically calculating the best action to take in the shortest period of time, to effectively stop an attack from spreading.

Whether a ransomware attack hits out of hours or an insider is exfiltrating sensitive data, Darktrace Antigena is able to enforce the normal 'pattern of life' of the digital environment, stopping the threats without interrupting the business. With Darktrace Antigena prepared to defend 24/7, security teams gain the precious time they need to catch up.

Darktrace Antigena Modules

Antigena for Cloud

Provides 24/7 autonomous protection of your crown jewels and sensitive data in the cloud. It stops insider threats, account takeovers, critical misconfigurations and more, wherever they occur, in real time.

Antigena for Email

Neutralizes spear phishing and impersonation attacks in Office 365. By analyzing each email in the context of a bespoke understanding of 'normal' across network, email, and cloud, Antigena Email defends the network against malicious emails that evade the email gateway.

Antigena for Network

Delivers Autonomous Response AI across the enterprise and Internet of Things. Like a digital antibody, it generates measured and proportionate responses when a significantly threatening incident arises. Within seconds of detecting a threat, Antigena surgically enforces a device's normal 'pattern of life'. It can also integrate with your firewalls or network devices if appropriate.

Real-World Use Case: Antigena Fights Back

At a Japanese consultancy, Darktrace discovered that an internet-connected CCTV system, which monitored the entire office space, had been infiltrated by unknown attackers who had begun watching all the cameras' video recordings.

Darktrace's AI quickly detected that massive volumes of data were moving between the unencrypted CCTV server, indicative of the attackers preparing to exfiltrate sensitive information. At this point, Antigena took rapid and precise defensive action. The technology's autonomous decision-making blocked data movement from the device to an external server – while still allowing the CCTV to operate in its intended capacity.

Darktrace Antigena fought back at machine speed, preventing a serious breach of market-sensitive information. By taking proportionate action to isolate and neutralize the attack at an early stage, Antigena created an important time buffer, allowing the security team to further investigate and remediate the threat, avoiding critical damage.

What Our Customers Say

"
Darktrace's ability to detect and contain attacks in real time enables us to feel confident our business is secure 24/7 "

- Director of IT, Country Life Vitamins

"
Antigena has been a revelation, it's so easy to stop anything on our network, even when our security team is away from their desks "

- Head of IT Operations, PPS Insurance

"
Antigena can autonomously and precisely contain in-progress attacks far quicker than our human team can "

- Information Systems Manager, Layton Construction

For more information

Book a demo now	Antigena threat report	Hear from our customers