Darktrace Antigena

Fight Back: Autonomous Response AI

Powered by Darktrace's world-leading AI, Darktrace Antigena is an autonomous response solution that takes targeted action against in-progress cyber-threats in real time.

The technology works like a digital antibody, intelligently generating surgical and proportionate responses when a highly threatening incident arises. By enforcing the normal 'pattern of life' for a given user or device, the system interrupts malicious activity while sustaining normal operations. This ability to contain emerging threats using proven AI is a game-changer for security teams, who benefit from the critical time needed to catch up and avoid major damage.

With over 8,000 deployments across 105 countries worldwide, Darktrace's cyber AI is being harnessed to transform even the most complex and vulnerable organization into a resilient, self-defending digital business, neutralizing advanced attacks before they have time to escalate into a crisis.

> " Darktrace Antigena acts faster than any security practitioner could to prevent damage from attacks such as ransomware. "
>
> 451 Research

Proven to Protect

Hundreds of organizations rely on Darktrace Antigena to take targeted, real-time actions in response to significant cyber-threats.

By enforcing the normal 'pattern of life' for a given user or device, Darktrace Antigena generates and executes actions to stop in-progress ransomware and insider threat, compliance breaches, malware, email-borne attack campaigns, and other threats, saving the security team valuable time in triaging and responding to threat alerts.

Antigena Key Benefits

Highly Targeted

Darktrace Antigena is highly targeted and surgical in its actions, neutralizing threats by enforcing the normal 'pattern of life' for a given user or device. This means that it does not disrupt day-to-day business activity, instead working behind the scenes to proactively protect your business.

Buys Your Team Time to Catch Up

Darktrace Antigena's ability to contain in-progress attacks at an early stage, before they have time to cause damage, keeps the business protected even when security teams are between shifts or out of office. On average, Antigena responds to threats within 2 seconds.

Self-Defending Digital Business

Darktrace Antigena is the technology that powers the self-defending digital business, working across IT and OT environments, third-party cloud services, SaaS applications, and email. Antigena's autonomous actions save an average of 10 hours a week per security analyst.

Antigena Network

Antigena Network is an autonomous response module that takes action within the network, including in virtualized and cloud environments. It requires no additional hardware and can be activated within minutes.

The autonomous response module is customizable, allowing customers to stay in the driving seat, and transition to a fuller use of AI in their enterprise. The system can be configured in one of two modes:

○ **Trust-Building Mode: Human Confirmation**
In this mode, Antigena Network generates responses which must be validated by the security team before action is taken. This allows you to build confidence in Antigena's decision-making before switching to Active Mode.

○ **Active Mode: Self-Defending Digital Business**
In Active Mode, Antigena Network is fully autonomous, meaning that a serious threat may be instantly contained without a security analyst needing to log on. The system acts within the operating parameters that you define, and an alert is generated to indicate the action taken.

> "
> ## No matter what the attacker does, Darktrace recognizes the risk and then Antigena shuts it off. "
>
> **Yorck Reuber, CTO North Europe, AXA IT**

Fast
Responds within 2 Seconds

Targeted
Stops high severity threats

Efficient
10 hours a week saved per security analyst

Antigena Integration
Antigena Network can also take action by integrating with your existing security infrastructure, including network defenses and leading firewalls.

Antigena Email

Antigena Email is an autonomous response module that works with Darktrace AI in the network to neutralize malicious emails, and deliver preemptive protection against targeted, email-borne attack campaigns in real time. Deployed as an extra 'hop' in mail routing rules, Antigena Email is cloud-based and requires minimal configuration.

With Antigena Email, Darktrace AI can detect and contain an infection in the network, recognize that the infection had an email as its source, and identify and neutralize similar malicious emails targeting the business – stopping the spread of an emerging attack campaign, and giving human responders the crucial time needed to catch up.