Antigena Endpoint

- ✔ Protects employees without disrupting business
- ✔ Surgical, proportionate response
- ✔ Covers insider threat, ransomware, DLP and other use cases
- ✔ Easy to set up with lightweight agents
- ✔ Fully configurable

"Self-Learning AI investigates behavior on the endpoint alongside behavior in Microsoft 365 and across our entire cloud environment."

Head of IT Infrastructure,
Scope Markets

Protecting employees, wherever they are

The shift to remote and hybrid working has taken many employees out of firewalled offices, and created new security risks. With employees working from offices and homes, hotels and coffee shops, endpoint devices face a myriad of cyber-threats. Meanwhile, cyber-criminals are constantly developing new techniques to exfiltrate and encrypt the information these devices hold.

Surgical response at the endpoint: powered by Self-Learning AI

Darktrace's core technology, Self-Learning AI, understands the 'pattern of life' of every user and device in your organization, building up a sense of what is normal, across the entire digital estate. This enables it to identify subtly unusual behaviors and threats, including threats that have never been encountered before.

Antigena Endpoint harnesses this knowledge of what is normal to protect endpoints in your organization proactively, taking targeted and proportionate response within seconds, where necessary. Critically, its actions are appropriate to the threat, and do not overstep the mark – ensuring that normal operations are not negatively impacted.

The right action, at the right time

Using Darktrace's proprietary agents, Antigena Endpoint takes action in seconds to contain cyber-threats – and without relying on pre-programmed response mechanisms. Instead, Darktrace's AI makes micro-decisions from hundreds of data points, and can tailor its actions according to the precise nature of the threat and your organization's preference.

Antigena Endpoint's 'Autonomous Response' actions may include:

- Blocking anomalous connections for a given length of time
- Enforcing 'pattern of life' for a given length of time
- Preventing anomalous data upload and downloads
- Quarantining device (with configurable allow-lists, e.g. VPN, anti-virus)

Autonomous Response has become critical for security teams given developments in the cyber-threat landscape:

Attacker innovation: an increasing number of novel attacks cannot, by definition, be thwarted with pre-programmed responses.

Speed of attacks: shrinking dwell times and a preference for 'smash & grab' tactics have meant human response times are too slow.

Overstretched teams: threat investigation is manual and human-intensive; by the time a threat is understood it is often too late – the damage is done.

Rapid cloud deployment

Antigena Endpoint installs in minutes, and immediately starts to learn your unique digital estate, without reliance on manual rules and signature lists that need constant updating and maintenance.

The technology is easily deployed using lightweight Darktrace agents, and can also be used in conjunction with third-party EDR agents.

Darktrace's serverless architecture enables automatic deployment and scaling within AWS.

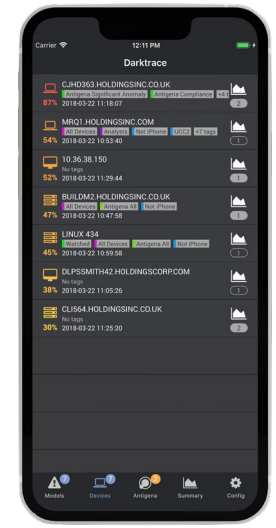
Tailors to your needs

It's also easy to customize Antigena Endpoint, restricting Autonomous Response actions to specific devices, or particular threat use cases, for example.

Thanks to the technology's rapid learning period, customers can switch to 'Autonomous Mode' soon after initial deployment, or whenever desired.

Bringing the human into the loop

Full oversight is provided through Darktrace's Threat Visualizer interface, and via the Darktrace Mobile App. You can configure your alerts to ensure your team get instantly informed when Autonomous Response actions have been generated, and how incidents have been handled.



Notifications of Darktrace's findings and actions can be delivered by the Mobile App

Attack scenario: Data exfiltration via employee error

An employee browsing the internet clicks on a malicious link containing novel malware. The threat is not caught by anti-virus and EDR tools that are in place.

Darktrace's understanding of this employee's normal behavior allows it to recognize that this file download is highly unusual, and Antigena blocks the anomalous file download, without interrupting the rest of the employee's activity.

If the attack continues...

C2 communication begins. The attacker is using entirely new infrastructure, meaning this stage is again missed by conventional tools.

Darktrace recognizes this communication as anomalous, since the employee has never communicated with this endpoint in this way. Antigena interrupts the command-and-control traffic in seconds.

If the attack still persists...

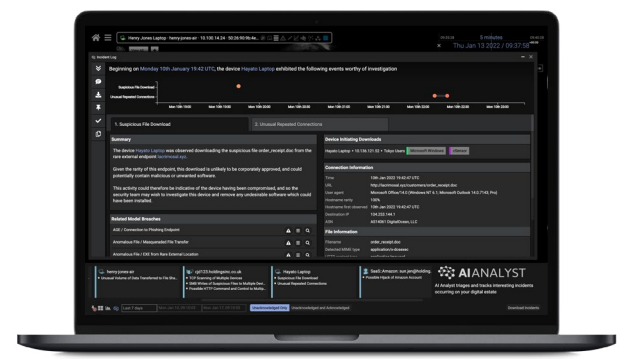
The attacker uploads sensitive documents to OneDrive. Since the employee uses OneDrive regularly, the activity – which is encrypted – blends in and goes undetected by traditional endpoint tools.

Darktrace's nuanced understanding of the employee and business allows it to discern that, whilst the employee regularly connects with OneDrive, they have never before uploaded this amount of data, using these methods, at this time of day. Hundreds of data points combine to reveal deeply unusual activity. Targeted action is taken to stop this particular data upload, without interrupting legitimate OneDrive activity.

The threat is automatically investigated, and the full scope of the incident summarized

Darktrace's Cyber AI Analyst investigates in the background, connecting the dots between these events, in conjunction with events across email, SaaS, cloud and the corporate network. The AI works at machine speed, investigating hundreds of threads in parallel.

A single, detailed incident report is generated, allowing the security team to fully understand what occurred and take any further action necessary.



Example of a Cyber AI Analyst investigation