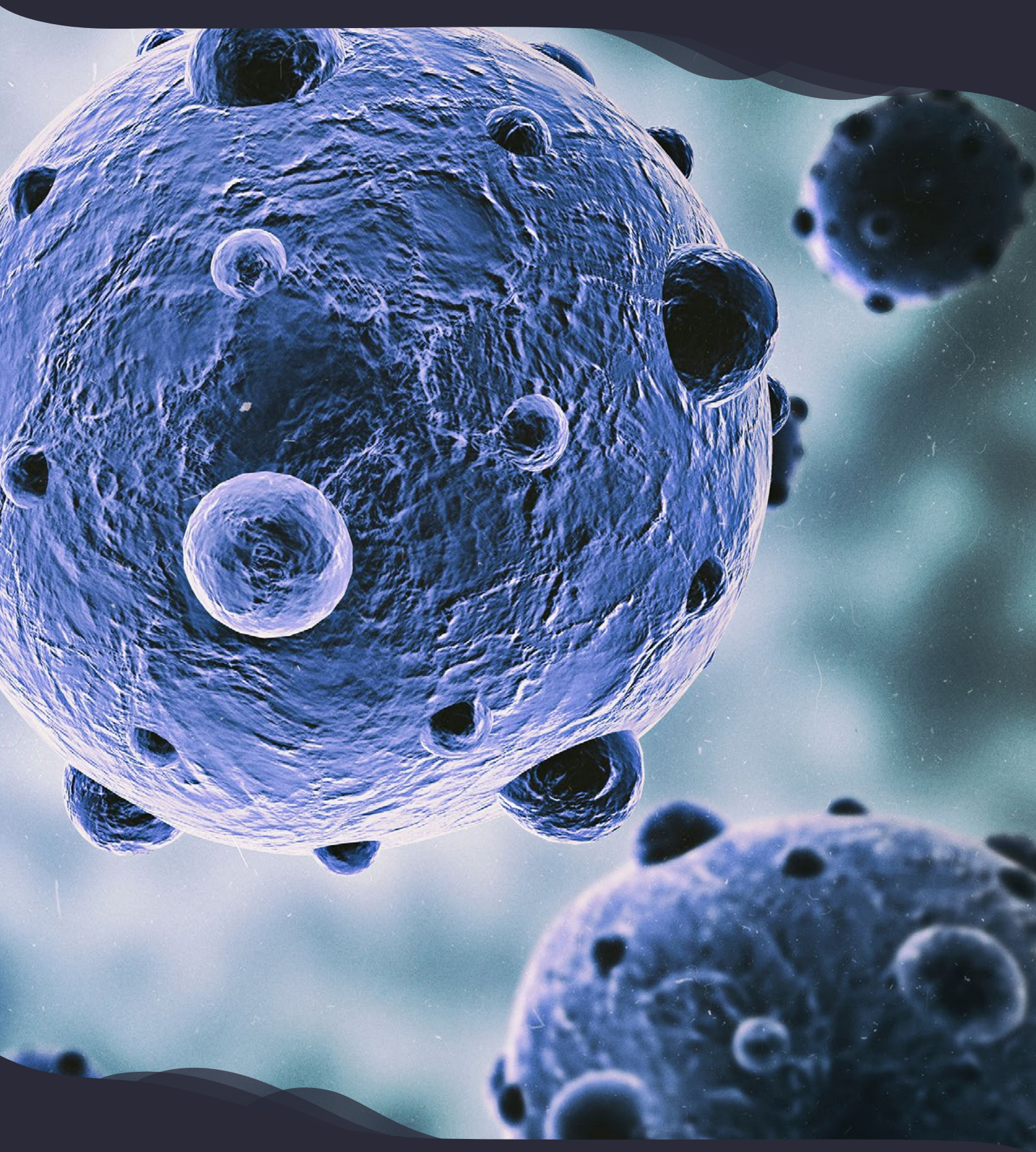


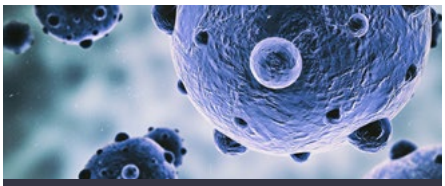
DARKTRACE

Darktrace Antigena

Autonomous Response to Cyber-threats

PRODUCT OVERVIEW

The Machine Fights Back



Key Benefits

- Takes automated, measured, and targeted action
- Responds faster than any security team can
- Human Confirmation Mode available
- No rules, no signatures
- Fully configurable
- Does not disrupt day-to-day activity

"Darktrace is the clear leader in anomaly detection...well ahead of peers."

451 Research

"Darktrace is one of the few cases where talk about use of AI in cybersecurity has turned into action."

Ovum
TMT intelligence | informa

In this new era of cyber-threats, attackers are fast and stealthy. Automated attacks like ransomware spread in seconds, and employees may jeopardize security with a few clicks, whether deliberately or not. It has become impossible for security teams to keep up with the pace of threats, amid dynamic enterprise environments.

Darktrace's Enterprise Immune System was the first application of artificial intelligence (AI) for cyber security, proving the efficacy of using machine learning for finding in-progress cyber-threats, including novel, stealthy and insider threats that have never before been identified. Darktrace Antigena completes the Enterprise Immune System by autonomously reacting against those threats detected, in real time.

The technology works like a digital antibody, intelligently generating measured and proportionate responses when a threatening incident arises, without impacting normal business operations. This ability to contain threats as they happen using proven AI is a game-changer for security teams, who benefit from the critical time they need to catch up and avoid major damage.

Bridging the gap between automated threat detection and a security team's response, Darktrace Antigena represents a new era of cyber defense that autonomously fights back.

How Does Darktrace Antigena Work?

Modeled after the human immune system, Darktrace's Enterprise Immune System leverages advances in machine learning and AI algorithms to build a deep understanding of the normal 'pattern of life' for every user and device in a network.

Darktrace Antigena then uses that understanding to autonomously respond to serious threats by taking precise, defensive action designed to neutralize threats and allow the security team precious time to catch up.

Darktrace Antigena is fully configurable, allowing for varying degrees of automation according to your organization's needs. For example, users may choose to 'validate' Antigena's responses before they are put into effect, thus allowing users to gain confidence in Darktrace Antigena, while saving time on the investigation and contextualization of the threat.

Autonomous Response

Darktrace Antigena is a response capability that takes action within the network where Darktrace's Enterprise Immune System has been deployed. The module can be activated on your existing appliance or a stand-alone appliance can be deployed. Once deployed, Darktrace Antigena performs defensive actions designed to maintain a normal 'pattern of life'. It highlights devices engaged in anomalous activity and takes action to return them to normal operations.

Darktrace's unique understanding of 'normal' communication between machines is constantly evolving, so the more information it sees, the better understanding it has of what is anomalous.

If a device within an organization is seen to be displaying significant levels of abnormality, Darktrace Antigena may elect to terminate connections deemed to be highly unusual for the device and its peer group in that specific context. However, the immediate action is specific enough that, while the abnormal connection is slowed or terminated, other processes can continue, allowing business proceedings to continue uninterrupted.

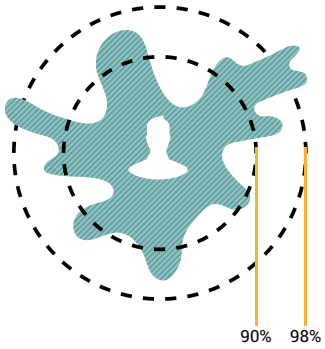
Many customers choose to initially deploy Darktrace Antigena in Human Confirmation Mode. In this mode, Antigena automatically generates recommendations of response actions, based on its judgement of what a threat is, however a human operator is required to validate the action. This mode allows your security team time to understand and gain confidence in Darktrace Antigena's decision-making. When you are ready, you may switch to Active Mode, which allows the responses to be performed automatically.

All actions taken by Darktrace Antigena are reported to you within the Threat Visualiser. Actions may be edited or revoked by your security or infrastructure team at any point.

"Darktrace Antigena is the only automated cyber defense technology on the market that is capable of fighting the most important battles for us. Using Darktrace's AI, we can now stop never-before-seen threats in their tracks, allowing us to remain uniquely proactive in the face of a rapidly-changing threat landscape."

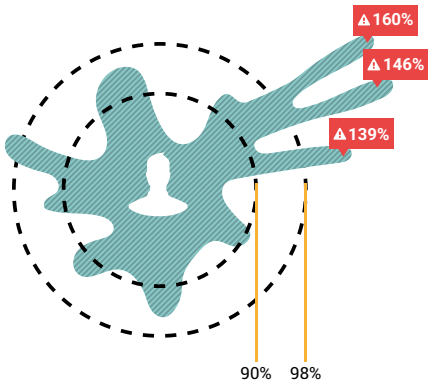
Michael Sherwood, CIO, City of Las Vegas

Intelligent, Real-time Response



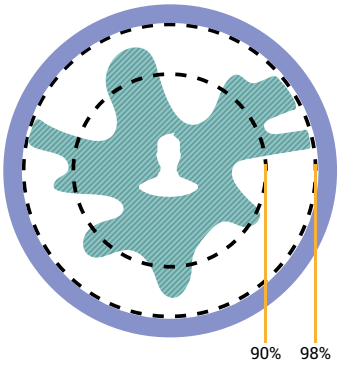
Normal 'Pattern of Life'

Darktrace uses unsupervised machine learning to build a deep understanding of the normal 'pattern of life' of devices and users



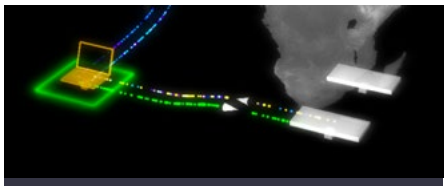
Anomalous Activity

Darktrace identifies highly anomalous activity associated with a rare file download from an unusual source. This is a major deviation from normal activity.



Autonomous Response

Antigena enforces the device's 'pattern of life'. All connections outside of its normal behavior are terminated. Normal activity from the machine remains unaffected.



Darktrace Antigena

- Actions are performed by the administrative interface of the Darktrace appliance
- Creates dynamic boundary for inter-machine networking
- Slows transfer of anomalous data, giving the security team time to investigate
- Available for a four-week Proof of Value trial

"Protecting our systems and data from the ever-increasing cyber-threat is now a fundamental requirement. After a period of learning, the Antigena logic demonstrated its ability to detect and contain potential ransomware attacks by blocking unusual traffic instantaneously."

Steve Drury, COO,
The Family Building Society

Threat scenarios where Darktrace Antigena has taken action include:

- An external attacker infiltrated an internal device and conducted malicious reconnaissance with the goal of appropriating sensitive client information. Darktrace Antigena generated an automatic response and blocked malicious connections.
- A device was infected by a Trojan and was discovered scanning hundreds of devices for open channels of communication in a suspected attempt to exploit vulnerabilities. Darktrace Antigena blocked outgoing connections from the device, allowing it to be isolated and cleaned before the infection could develop further.
- An employee inadvertently executed a malicious file received in an email, the malware immediately started to encrypt data on the employee's computer. Within a minute, Darktrace Antigena had isolated the device and stopped the ransomware attack before it spread across the network.

Conclusion

Today's fast-moving threats routinely outpace human security teams, regardless of their size or experience. Automated, real time responses are quickly becoming an indispensable tool to buy valuable time, proactively neutralize threats, and enforce normal network activity.

Darktrace Antigena represents the first automated, self-defending cyber security system that allows the Enterprise Immune System to take direct action against specific threats, without disrupting normal business operations.

With Darktrace Antigena, the Enterprise Immune System delivers both real-time threat detection and real-time responses, performing intelligent and targeted actions to neutralize threats before they can escalate into a crisis.

About Darktrace

Darktrace is the world's leading machine learning company for cyber security. Created by mathematicians from the University of Cambridge, the Enterprise Immune System uses AI algorithms to automatically detect and take action against cyber-threats within all types of networks, including physical, cloud and virtualized networks, as well as IoT and industrial control systems. A self-configuring platform, Darktrace requires no prior set-up, identifying advanced threats in real time, including zero-days, insiders and stealthy, silent attackers. Headquartered in San Francisco and Cambridge, UK, Darktrace has 24 offices worldwide.

Contact Us

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
info@darktrace.com
darktrace.com
@darktrace