DARKTRACE

DATA SHEET

Darktrace Antigena

Product Overview

Introduction

As cyber-attackers use increasingly sophisticated technologies to penetrate and propagate within networks, the need for automated response to combat these fast-moving adversaries has grown. Security teams cannot keep up with a threat landscape that is evolving 24/7, and which includes automated attacks, like ransomware, that can seriously jeopardize an organization's infrastructure within as little as 20 minutes.

Darktrace Antigena is an automated response capability, which allows organizations to 'fight back' against cyber-threats – without disruption to their day-to-day business activity. Working in conjunction with Darktrace's core detection technology, Antigena replicates the functions of antibodies in the human immune system by intelligently locating and neutralizing threats.

As a 'digital antibody', Antigena completes the end-to-end functionality of the Enterprise Immune System by automatically detecting and responding to threats that have been uniquely detected. Thanks to the nuanced understanding of what are 'normal' and 'abnormal' behaviors, it is capable of taking measured and targeted responses, disrupting threats without interrupting normal business processes and allowing security teams time to catch up and perform further investigations.

Benefits

- Respond to threats faster than any security team can
- Take automated, measured, and targeted action
- No rules, no signatures
- Does not disrupt day-to-day business
- Frees up resources and people
- Fully configurable

> "It is our belief that [Antigena's] ability to drive security actions based on observed behavior is critical to protecting organizations against sophisticated threats. For businesses where alerting operations staff is too passive and slow, the Antigena API allows security teams to automate responses via firewalls, endpoint software and management consoles."
>
> **Eric Ogren, 451 Research Senior Analyst**

451 Research

How Does Antigena Work?

Antigena works in conjunction with Darktrace (Core), which lies at the heart of the Enterprise Immune System approach, and is powered by Darktrace's proprietary mathematics and machine learning. As a result, organizations must have a core Darktrace appliance or appliances installed within the network before activating Antigena.

When Darktrace has identified activity that has been deemed threatening or highly anomalous, Darktrace Antigena is triggered and generates a response to that activity in real time, which depends on the severity of the incident.

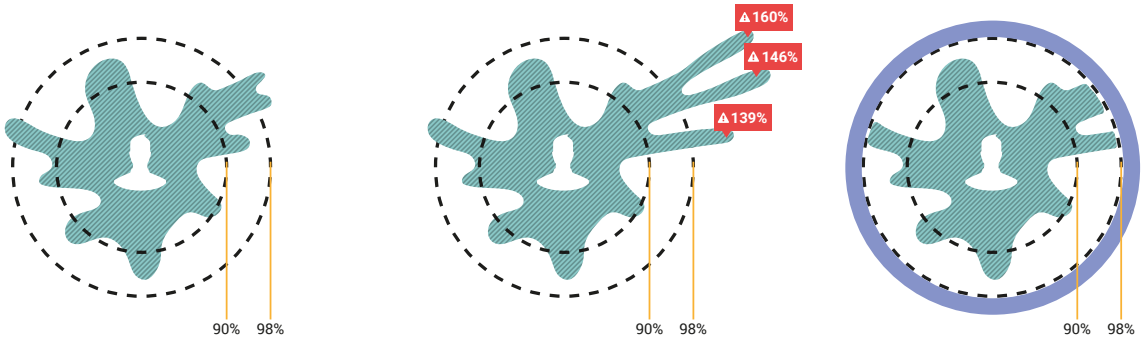
Examples of actions taken by Antigena may include:

- Stopping or slowing down activity related to a specific threat
- Quarantining or semi-quarantining users, systems, and/or devices
- Marking specific pieces of content, such as email, for further investigation or tracking

The precision with which Antigena operates means that interruption to normal business processes is avoided. Instead, Antigena's self-learning capability allows it to enforce the normal 'pattern of life' by slowing and mitigating threats, giving security teams time to investigate the evolving situation and take further action.

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

Illustrative example of Antigena response



Normal 'Pattern of Life'

The normal 'pattern of life' of devices and users are known to Darktrace. The historical actions of a device or user, and those of its peers, are calculated and used to determine a level of normality for every connection made.

Anomalous Activity

Darktrace identifies highly anomalous activity associated with a rare file download from an unusual source and subsequent beaconing to an external machine. Unknown malware has been downloaded and is reporting back to a control center.

Enforced Containment

Antigena enforces the device's 'pattern of life'. All connections outside of its normal behavior are terminated. Normal activity from the machine is left unaffected and the user continues to work unaware that preventative action has been placed on their device.

Darktrace Antigena Framework

The Darktrace Antigena Framework provides a layer of intelligent decision-making and response, according to the known 'pattern of life' of the enterprise. Darktrace's Enterprise Immune System upstreams the subtle changes in behavior witnessed in anomalous activity to the Framework, enabling it to make targeted decisions about the most appropriate way to respond to identified threats. Antigena is therefore capable of making precise decisions that will return an anomalous user or device back to its normal behavior profile.

This methodology ensures that normal working activity is permitted, while potentially malicious actions are prevented, effectively eliminating false positives. Antigena creates a dynamic boundary, which is automatically personalized to each user and device on a network.

The Antigena Framework interacts with your network via one or more modular elements that can communicate with aspects of your existing infrastructure. The Framework is self-aware, constructing its decision-making process around its existing capabilities. In this way, Antigena is fully modularized and can be expanded with new abilities as your architecture develops.

Dynamic Boundary

Many traditional proactive security devices fail because they rely on static restrictions of behavior that apply to large groups of users and devices.

Security professionals are forced into making these restrictions widely permissive to accommodate a few individual users within the group. The administrative overhead, cost, and time involved in tailoring policies means that it is often easier to open permissions to far more users than is required.

Antigena solves this problem by providing a dynamic boundary to a user's behavior. Just as no single user is alike, no behavior profile is alike either.

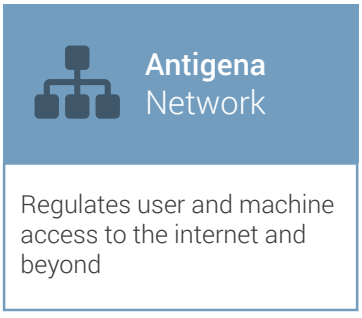
Feedback Loop

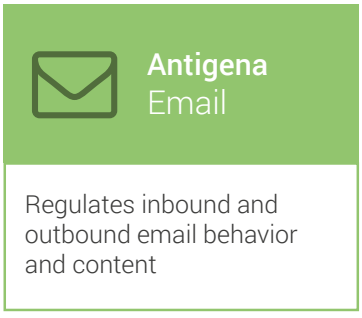
Antigena monitors the actions that it produces to better understand an organization's threat surface area. Determined attackers or insider elements will not stop at the first attempt. Malicious software often has many fall back routines to run in the event that it is prevented from functioning.

Antigena and its modules will send the results of failed attempts back into the Darktrace Enterprise Immune system, producing further insight into anomalous activity. It enables Darktrace to learn, not just from normal activity, but from activity that has already been prevented. In this way, undesirable behavior learned in one part of the network can better inform the choices made across the entirety of the network.

Darktrace Antigena Modules

The Antigena Framework interacts with your network via one or more modular elements that can communicate with aspects of your existing infrastructure. These modules are Antigena Network, Antigena Internet, and Antigena Email.





Antigena Internet

Antigena Internet regulates and controls user and device internet connectivity in accordance with the Antigena Framework and Darktrace's behavioral awareness of your network, users, and devices.

The Antigena Internet module exists as one or more physical appliances that sits in-line with an internet egress gateway or an element in an existing web proxy infrastructure. Devices required to access the internet can have their internet-bound traffic transparently observed or be explicitly configured to browse via Antigena Internet.

Darktrace will upstream detected anomalous behaviors to the Antigena Framework, which may instruct the Internet module to automatically provide intelligent preventative actions on internet-bound activity. The reactions can be produced based on an internal machine's general behavior – not just its internet activity.

Use Cases:

- Stop malware from being accidentally or intentionally downloaded from the internet
- Prevent the upload of sensitive data to the internet
- Block users from visiting dangerous or suspicious websites

Key Benefits

- Actions are performed by the administrative interface of an existing Darktrace appliance or optionally by a dedicated appliance
- Connections can be terminated from internal-to-internal and internal-to-external communications
- Creates Dynamic Boundary for inter-machine networking
- Network layer interactions frequently require no integration within an organization's infrastructure
- Available for a four-week Proof of Value trial

Antigena Network

Antigena Network is a software component that permits interaction between the core Antigena Framework and elements within a protected network. It is available for installation on existing Darktrace devices and requires no additional hardware.

From the main Darktrace appliance, the Antigena Network module provides the ability to connect to internal systems to perform defensive actions, designed to maintain a normal 'pattern of life' on devices with a high level of anomalous activity and protect the network at large.

Darktrace's 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 sufficient levels of abnormality, Antigena may elect to emit signals to that device that terminate connections deemed as 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 for business proceedings to continue uninterrupted.

The actions that Antigena performs are all reported in Darktrace's Threat Visualizer and can be revoked at any point by your security team or infrastructure.

Use Cases:

- Triggered by a suspicious connection to foreign IP address (detected by Darktrace)
- Slow a known device downloading large amounts of data it does not normally access
- Prevent a device ' communicating' to an unknown location
- Stop the transfer of secure files to an unauthorized user

Key Benefits

- Actions are performed by the administrative interface of an existing Darktrace appliance or optionally by a dedicated appliance
- Connections can be terminated from internal-to-internal and internal-to-external communications
- Creates Dynamic Boundary for inter-machine networking
- Network layer interactions frequently require no integration within an organization's infrastructure
- Available for a four-week Proof of Value trial

Antigena Email

Antigena Email is an appliance that sits at the border of your email infrastructure. As such, it is capable of interacting with inbound and outbound mail transit and message content.

By progressive learning techniques, the Email module will work with Darktrace's Enterprise Immune System to build up an understanding of patterns of email communication and develop a complex mesh of 'likelihood of correspondence' that identifies the fingerprints of legitimate email. Each inbound email is compared against known and frequent correspondence to establish a level of trust. The Antigena Framework has the ability to flag suspicious emails, as well as sanitize attachments and links as they pass through the Antigena Email module, neutralizing any harmful content.

Use Cases:

- Prevent phishing or spear-phishing campaigns by preventing harmful links from reaching the target
- Stop confidential information from being intentionally shared to recipients without clearance
- Block employees from sending sensitive information to a personal account

Key Benefits

- Dynamic boundary enforced for communications
- Stop phishing based on mathematical correspondent profiling
- Feedback loop provides Darktrace with a dynamic threat surface area unique to your organization
- Highly anomalous email can be blocked before they reach the end user
- Sanitation of mail-borne content
- Works in conjunction with your existing mail server

Conclusion

It is becoming impossible to manually keep up with this new era of computer-speed threats, irrespective of how large your security team is. Automated response is the next step in ensuring that cyber defense keeps pace with these new attackers, and take preventative actions as threats develop.

By using unique machine learning and mathematics, Darktrace can detect in-progress threats without requiring rules and signatures, which are proven to fail when faced with machine-on-machine attacks and sophisticated hackers.

Antigena represents the first automated, self-defending system that allows the Enterprise Immune System to take direct action against specific threats – without disrupting your organization. It buys you time, reduces response time and enables better, more efficient risk mitigation, irrespective of the type of threat encountered.

> "We believe [Antigena] represents an important step in behavior analytics evolving to an active defense that traditional systems cannot match."
>
> **Eric Ogren, 451 Senior Analyst**

About Darktrace

Winner of the Queen's Award for Enterprise in Innovation 2016, Darktrace is one of the world's leading cyber threat defense companies. Its Enterprise Immune System technology detects and responds to previously unidentified threats, powered by machine learning and mathematics developed by specialists from the University of Cambridge. Without using rules or signatures, Darktrace is uniquely capable of understanding the 'pattern of life' of every device, user and network within an organization, and defends against evolving threats that bypass all other systems. Some of the world's largest corporations rely on Darktrace's self-learning technology in sectors including energy and utilities, financial services, telecommunications, healthcare, manufacturing, retail and transportation. Darktrace is headquartered in Cambridge, UK and San Francisco, with 20 global offices including Auckland, Johannesburg, Lima, London, Milan, Mumbai, Paris, Seoul, Singapore, Sydney, Tokyo, Toronto and Washington D.C.

info@darktrace.com US: +1 (415) 243 3940 Europe: +44 (0) 1223 324 114 APAC: +65 6248 4516 www.darktrace.com