

Antigena Email: Customer Testimonials

Getting Started

Darktrace offers a complimentary 30-day 'Proof of Value', allowing you to discover the power of Cyber AI in your own environment, free of charge. Upon installation, Antigena Email will immediately begin learning the 'pattern of life' of every email user across your organization. Darktrace's AI self-learns by passively analyzing real-time data, without using historical attack training data, rules or signatures.

You will benefit from:

- ✓ 5-minute installation
- ✓ Executive Summary Reports
- ✓ Weekly meetings to discuss results
- ✓ Access to exclusive training videos and customer portal

The Self-Defending Inbox

Antigena Email is a self-learning email security technology that understands the human behind email interactions to detect and neutralize sophisticated attacks that other tools miss.

While point solutions work by analyzing a given email in isolation and at a single point in time, correlating it against signatures, black-lists, and pre-definitions of bad, Antigena Email uses AI to learn the normal 'patterns of life' for internal and external email users. By leveraging its rich understanding of normal activity across inbound, outbound and internal email traffic, Antigena can neutralize malicious emails that deviate from the normal 'pattern of life' for a given user in relation to their past, their peer group, and the wider organization.

"Our experience with Antigena Email has been positive since the day we installed it."

– **Manager of IT, Entegrus**

"These are exactly the results we were looking for. We are blown away and have nothing but praise for this product."

– **CIO, City of Las Vegas**

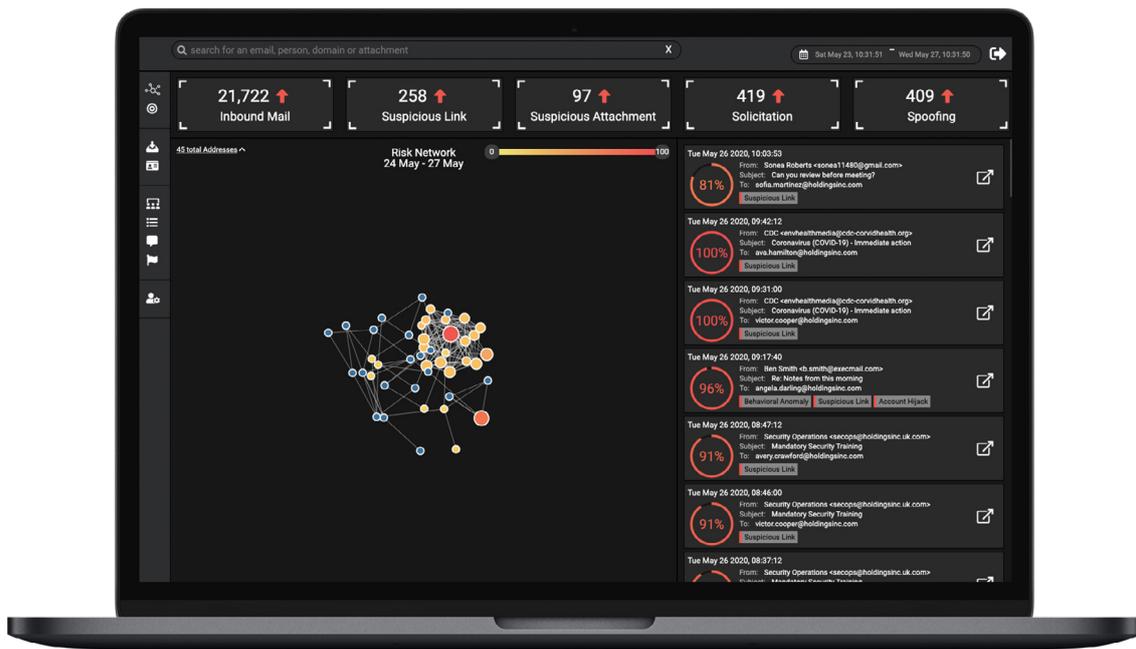


Figure 1: Antigena Email's user interface showing an overview of email attacks caught by Darktrace's AI

Stopping Advanced Threats

Once inside your environment, the technology dynamically analyzes every internal and external user, forming a 'pattern of life' and recognizing the subtle signs of threatening behavior. This allows it to catch the full range of threats targeting the inbox, including spear phishing, supply chain account takeover, and solicitation.

"When Antigena Email caught a spear phishing campaign that the Leader in the Gartner Magic Quadrant missed, we were convinced. The trial was over."

– CIO, Numeris

"We rely on Darktrace's AI to fight back against email attacks with complete autonomy and lightning speed – before damage is done."

– CIO, McLaren

"We were shocked by the things our legacy tools didn't catch that Antigena Email did."

– CTO, Bunim/Murray Productions



"Using AI, Darktrace can detect and respond to email-borne threats and cloud-based attacks that other tools miss."

– CIO, City of Las Vegas

"We deployed Antigena Email and a malicious email hasn't gotten through since. Before, at least one or two very serious malicious emails were getting through per month."

– Director of IT, CTC Global

"AI that has the ability to actually understand a user and how they use their email is a huge step forward from systems using whitelists and blacklists."

– Head of IT, Terra Firma



Freeing Up your Team

Darktrace's AI autonomously neutralizes the threatening activity missed by legacy gateway solutions. Antigena Email will contain the threat either by locking malicious links or flattening attachments, or even preventing an incoming email from reaching the inbox entirely. This allows your security team to focus their time on high-value tasks.

"When the Cyber AI Analyst came to life, I have begun leaving the individual security events with a low anomalous score. I leave the whole security overwatch to AI at this point."

– Lead IT Infrastructure Architect,
Pizza Hut Restaurants UK

"Antigena Email does the tough decision-making so the user doesn't have to."

– CTO, Bunim/Murray Productions

"Overall the amount of billable hours saved will cover the amount we paid for the solution. That, plus ensuring data trust, are important ROIs."

– Director of IT, Gray, Gray & Gray LLP

"Darktrace's AI has been able to spot the most subtle indicators of attack as soon as they emerge"

– IT Manager, Primafrio