# Antigena Email: Building Immunity for your Inbox

## At a Glance

- ✔ Self-learning: understands the human, not just the email address
- ✔ Identifies malicious emails that traditional tools let through
- ✔ Effective against all advanced email attacks, including social engineering
- ✔ Fast, virtual deployment

## Stops the Full Range of Attacks

- Spear phishing
- Social engineering & impersonation
- Business Email Compromise
- Supply chain account takeover
- External data loss
- Novel, unknown malware

## Novel Email Threats Are Getting Through

Email attacks are getting more and more sophisticated, with offensive AI threatening to supercharge email attack campaigns in the near future. It is becoming almost impossible to distinguish targeted spoof emails from genuine communications.

Novel attacks are consistently getting through traditional email security tools, which observe individual emails in isolation, and compare them against rules and signatures of known malicious attacks. With supply chains becoming more complex and employees more distributed and mobile, the need for an AI-driven, self-learning approach to email security is ever more necessary.

> "More than ever, modern email security requires innovation and a shift in mindset to combat the evolving threat landscape."
>
> **Peter Firstbrook, VP Analyst, Gartner**

> "We were shocked by the things our traditional tools didn't catch, that Antigena Email did."
>
> **CTO, Bunim/Murray Productions**

## The World's First Self-Defending Inbox

Antigena Email is the world's first Self-Learning AI solution for the inbox. By learning the normal 'pattern of life' for every user and correspondent, the technology builds an evolving understanding of the 'human' within email communications.

While traditional defenses ask whether elements of an email have been observed in historical attacks, Antigena Email is the only solution that can reliably ask whether it would be unusual for a recipient to interact with a given email, in the context of their normal 'pattern of life', as well as that of their peers and the wider organization.

This contextual knowledge enables the AI to make highly accurate decisions and neutralize the full range of email attacks, from 'clean' spoofing emails that seek to wire a fraudulent payment, to sophisticated spear phishing attempts.

## Understanding the Human in the Email

Inspired by the human immune system, Antigena Email uses Darktrace's core artificial intelligence to learn a sense of 'self' for every internal and external user, analyzing both inbound and outbound communications together with lateral, internal-to-internal communications.

By treating recipients as dynamic individuals and peers, Antigena Email uniquely spots subtle deviations from 'the norm' that reveal seemingly benign emails to be unmistakably malicious.

# Use case: Supply chain account takeover

One of the most difficult attacks to detect is an external account takeover, where a criminal hijacks the email credentials of a trusted contact, accesses historical correspondence and produces highly convincing emails – embedding a malicious link or attachment in the conversation at just the right moment. While traditional defenses assume this is a trusted user, Antigena Email analyzes each email in the context of learned patterns of life, and detects subtle deviations. By correlating the following potential indicators, Antigena Email quickly arrives at a comprehensive anomaly score, determining with confidence that the email is malicious, and neutralizing the attack before it can make an impact.

**Unusual login location –** Antigena Email can extract the geo-locatable IP address of the genuine sender and determine whether this is rare given the trusted contact's historical pattern of life. While a rare login location by itself may not trigger an alert or autonomous response, it will figure in the system's overall calculation and anomaly score.

**Unusual recipients –** Antigena Email models graph-based relationships between internal and external users and peers and understands their relationships at a granular level. If the attacker sends multiple emails to a range of recipients in the organization, Antigena Email can estimate the likelihood that this particular group would be receiving an email from the same source.

**Link rarity –** People often share links to the websites they visit and trust. By observing these links in lateral mail, Antigena Email can determine which links and domains are rare in the context of the organization. This is also useful in other threat scenarios, when determining whether a given sender's email domain has been observed in shared internal links.

**Behavioral anomalies –** Over time, Antigena Email learns how different senders construct their emails, analyzing both hidden email metadata and patterns in the body content. By applying AI to every inbound email, Darktrace identifies subtle changes that might be indicative that the email has been sent by someone other than the true account holder.

Gartner®

Gartner defines Darktrace as an Integrated Cloud Email Security (ICES) vendor, described as "Advanced email security capabilities … being deployed as integrated cloud email security solutions, rather than a gateway" Increasingly, ICES vendors are replacing the traditional secure email gateways.

"Integrated Cloud Email Security vendors go beyond simply blocking known bad content and provide in-line prompts to users that can help reinforce security awareness training, as well as providing detection of compromised internal accounts"

Gartner recommends that organizations seek out email security solutions that use ML- and AI-based anti-phishing technology maximum protection against sophisticated email attacks, including Business Email Compromise and spear-phishing attacks.