DARKTRACE

Self-Learning Email Security

The Email Threat Landscape

- Email Threat Landscape
- Traditional Email Security
- Antigena Email
- Use Cases
- Immune System Platform
- Gartner Reviews
- Industry Recognition

Email is the primary connective tissue for the majority of businesses. Nearly 300 billion emails are sent every day, many of them containing private information, confidential plans, and financial transactions.

Considering this overwhelming reliance on email, it is a worrying fact that 94% of all cyber-attacks still originate in the inbox.

Spear phishing, impersonation attacks, and account takeovers are slipping past traditional email security tools with alarming frequency. Furthermore, cyber-criminals have exploited global uncertainty around the pandemic to lure users into clicking malicious attachments or links in a tactic called 'fearware', as well as targeting the weakest links in supply chains to launch mass-scale fraud campaigns across multiple organizations.

In this era of sophisticated threats, it is critical for organizations to embrace new technologies which can adapt to attackers' tactics and techniques, and autonomously defend their email environment. A self-learning approach to email security has become critical in the face of increasingly advanced and fast-changing threats.

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

CIO, McLaren Technology Group

> "Antigena Email has been incredibly valuable in catching threats with its understanding of 'normal' for email traffic."

Head of IT, Entegrus

The Traditional Approach to Email Security

Legacy security tools look at emails 'in isolation', without the context of an organization's wider email patterns. These controls rely on historical knowledge of previously encountered attacks in order to spot the threats of today and tomorrow.

These 'reputation checks' cross-reference every email with a series of lists containing known 'bad' IPs, domains, and file hashes, and if there is a match the email is held back. In addition, security teams often create static rules and policies to tailor these controls to their organization. This involves spending a lot of time scrolling through Indicators of Compromise (IoCs) and updating their infrastructure to defend against known attacks.

Such an approach invariably results in playing 'catch-up' with cyber-criminals and is becoming increasingly antiquated as attackers increase the speed and scale of their campaigns. By the time an IoC has been created and a rule updated, the cyber-criminal has usually moved on. Attackers are constantly renewing their attack infrastructure by purchasing thousands of new email domains, usually for just a few pennies each, that don't have a reputation, and their attacks therefore bypass legacy tools with ease.

Furthermore, this approach is blind to cases of account takeover where a legitimate user's account is compromised and malicious emails are sent out. Since these emails come from a trusted contact they are judged both by the recipient and traditional email security to be benign. These tools therefore suffer from high-miss rates with new attacks and often overcompensate for this by holding back legitimate mail.

Key Takeaways

- ○ Reliant on rules and deny lists
- ○ False positives disrupt business
- ○ Deployment type leads to outages
- ○ Fails to catch novel or sophisticated threats

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

Antigena Email: Asking the Right Questions

Email Threat Landscape

Traditional Email Security

Antigena Email

Use Cases

Immune System Platform

Gartner Reviews

Industry Recognition

Antigena Email is the world's first self-learning email security technology. Powered by AI, it represents a fundamentally new approach to email security in moving away from static rules and playbooks that seek to answer the question of 'Is this email bad?'. Rather than looking at the data of an email alone and running it through pre-existing deny lists, Antigena Email looks at emails in their full context and instead asks: 'Does this email belong?'.

The technology analyzes thousands of data points for every email in the context of the sender, the recipient, and wider email traffic, looking at metrics including: previous interactions, login locations, similar-looking domains, and behavioral anomalies.

In this way, Antigena Email learns the normal 'pattern of life' for every user, building an evolving understanding of the human behind the email. With this more complete description of an email and the wider organization, Antigena can start questioning the data in order to understand if it belongs, given the wider context.

This allows the AI technology to spot subtle deviations and anomalous behavior, detecting all threat types regardless of whether they have been seen before. Antigena Email then responds accordingly, locking links, neutralizing attachments, or preemptively pulling the email from the inbox, depending on the precise nature of the incident.

Key Takeaways

- Learns an evolving sense of 'self'
- Analyzes inbound, outbound, and lateral (internal) emails
- Continuously evaluates as the organization evolves
- Responds proportionately
- Can be enriched with other data sources across the business, such as network data, cloud, and SaaS

Email Threat Landscape
Traditional Email Security
Antigena Email
Use Cases
Immune System Platform
Gartner Reviews
Industry Recognition

AI-Native Email Security

Innovations in AI have fundamentally changed the email security landscape in recent years, but it can often be hard to determine what makes one system different to the next. One approach involves harnessing an extremely large data set with thousands or millions of emails. Once these emails have come through, the AI is trained to look for common patterns in malicious emails. The system then updates its models, rules set, and deny lists based on that data.

This method certainly represents an improvement to traditional rules and signatures, but it does not escape the fact that it is still reactive and unable to stop new attack infrastructure and new types of email threats. It is simply automating that limited, traditional approach, only instead of having a human update the rules and signatures, a machine is updating them instead.

Antigena Email uses this approach for one specific use which is futureproof and not prone to change over time: to analyze grammar and tone in an email in order to identify intention: asking questions like 'Does this look like an attempt at inducement? Is the sender trying to solicit some sensitive information? Is this extortion?'. By training a system on an extremely large data set collected over a period of time, you can start to understand what, for instance, inducement looks like. This then enables the system to easily spot future scenarios of inducement based on a common set of characteristics.

In addition, Antigena Email uses unsupervised machine learning to extract and extrapolate thousands of data points from every email. Only after having a more comprehensive set of indicators, with a more complete description of that email, can the data be fed into an unsupervised, topic-indifferent machine learning engine to start questioning the data in millions of ways, asking for instance:

- Does this person usually receive Zip files?
- Does this supplier usually send links to Dropbox?
- Has this sender ever logged in from China?
- Do these recipients usually get the same emails together?

The technology identifies patterns across an entire organization and gains a continuously evolving sense of 'self' as the organization grows and changes. It is this innate understanding of what is and isn't 'normal' that allows the AI to spot the truly 'unknown unknowns' instead of just 'new variations of known bads.'

Auto-Prioritization of Key Individuals

Antigena Email understands the human behind email communications, which means it can autonomously detect which users are high priority, which users are more likely to be targeted, and which users have access to sensitive material. It will therefore take an appropriate response to different users, rather than a single response across the board.

Cloud Delivered

Advancements in cloud computing have given rise to fast, resilient, dependable services hosted without hardware maintenance. Microsoft 365 has continued to thrive as organizations shift away from hosting their own mail servers.

Antigena Email is built for cloud solutions like Microsoft 365 and Google Workspace, and is highly agile, scalable, and robust. It can be hosted on-premises or deployed in 5 minutes in the cloud.

Antigena Email uses journaling to receive a copy of each email. Journaling reliably sends a copy to additional, pre-configured destinations. It takes only a few minutes to set up and requires no MX record changes, meaning there is no risk of operational outages. The technology then processes every email in real time, leveraging email providers' APIs to take action if necessary.

> "Antigena Email is as close to 'set it and forget it' as you can find in the email security market. We've been using the product for a few months now and we have seen zero phishing attempts make it into our organization."
>
> CIO, Transportation

Use Cases: Spear Phishing and Payload Delivery

Email Threat Landscape
Traditional Email Security
Antigena Email
Use Cases
Immune System Platform
Gartner Reviews
Industry Recognition

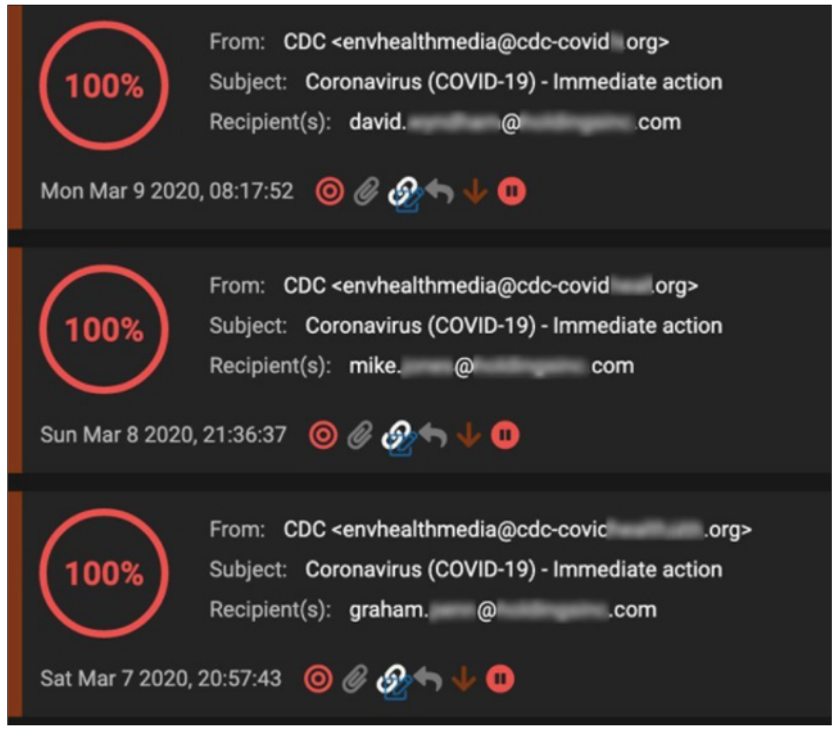
The majority of phishing attempts aim to deceive employees into clicking malicious links or attachments in an email in order to harvest credentials or deploy malware into an organization. These emails can be launched as mass 'drive by' campaigns or as carefully crafted 'spear phishing' attacks that are targeted towards the recipient.

'Fearware' Attacks Neutralized by Darktrace AI

With the onset of the pandemic, Darktrace caught several emails purporting to be from the Center for Disease Control (CDC). This was the latest in a new trend of 'fearware': attacks that play into Fear, Uncertainty, and Doubt (FUD) by impersonating officials with pertinent information about current global issues.

The emails claimed to offer urgent information on the spread of the pandemic. Darktrace, however, detected that these emails contained malicious links and held them back from the recipients' inboxes, protecting the organization from harm.

> "Using AI, Darktrace can detect and respond to email-borne threats and cloud-based attacks that other tools miss."
>
> CIO, City of Las Vegas

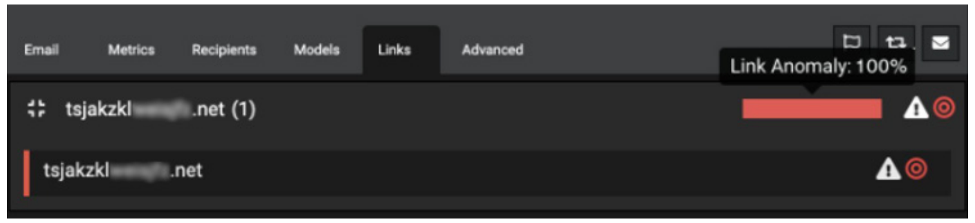


100%
From: CDC <envhealthmedia@cdc-covid[redacted]org>
Subject: Coronavirus (COVID-19) - Immediate action
Recipient(s): david.[redacted]@[redacted].com
Mon Mar 9 2020, 08:17:52

100%
From: CDC <envhealthmedia@cdc-covid[redacted].org>
Subject: Coronavirus (COVID-19) - Immediate action
Recipient(s): mike.[redacted]@[redacted] com
Sun Mar 8 2020, 21:36:37

100%
From: CDC <envhealthmedia@cdc-covic[redacted].org>
Subject: Coronavirus (COVID-19) - Immediate action
Recipient(s): graham.[redacted]@[redacted].com
Sat Mar 7 2020, 20:57:43

Figure 1: The CDC spoof emails that evaded gateways but were stopped by Antigena Email



tsjakzkl[redacted].net (1)
tsjakzkl[redacted].net

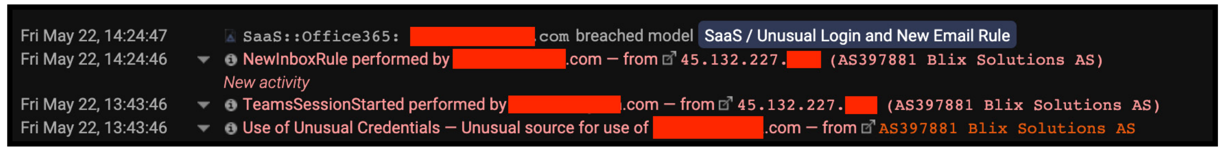
Figure 2: The 100% anomalous link surfaced by Darktrace

Use Cases: Compromised Credentials and Account Takeover

Attackers may steal email credentials using a variety of methods, including brute force attempts, exchanges on the Dark Web, or using software that records keystrokes on compromised devices. Once in an account, attackers can pillage the inbox for valuable data or use the account as a launching point for the next stages of an attack.

Compromise Across Microsoft 365 and Teams

Darktrace picked up on several anomalies at a public accounting firm, including a sudden surge in outbound email traffic, as well as an unusual login location: while the company was located in Wisconsin, an IP address located in Kansas was used to log in to both Outlook and Microsoft Teams accounts.



```
Fri May 22, 14:24:47      SaaS::Office365: [redacted].com breached model SaaS / Unusual Login and New Email Rule
Fri May 22, 14:24:46      NewInboxRule performed by [redacted].com — from 45.132.227.[redacted] (AS397881 Blix Solutions AS)
                          New activity
Fri May 22, 13:43:46      TeamsSessionStarted performed by [redacted].com — from 45.132.227.[redacted] (AS397881 Blix Solutions AS)
Fri May 22, 13:43:46      Use of Unusual Credentials — Unusual source for use of [redacted].com — from AS397881 Blix Solutions AS
```

Figure 3: Darktrace detected a Microsoft Teams login from a 100% rare destination

‘Impossible travel’ rules alone would have missed these anomalies, but an understanding of activity and behavior across different SaaS applications allowed Darktrace’s AI to recognize these events as one systematic case of credential theft. When the threat-actor subsequently created a new email rule, Darktrace was able to connect this event with the other anomalous behavior and understand its malicious nature.

Five minutes later, Antigena Email alerted on 220 outbound emails containing a generic subject line and an attached PDF. The technology detected there was a clear spike in outbound emails from this user and flagged each of these emails with the “Out of Character” tag.

The unusual login behavior detected by Darktrace’s SaaS Module could be connected to the anomalous outbound email behavior flagged by Antigena Email, allowing the security team to see the extent of the attack and neutralize it as it emerged. The security team therefore immediately disabled the compromised account.

> “Antigena Email has the ability to suspend all activity it deems malicious”
>
> General Manager, Global Travel

Use Cases: Supply Chain Account Takeover

Email Threat Landscape

Traditional Email Security

Antigena Email

Use Cases

Immune System Platform

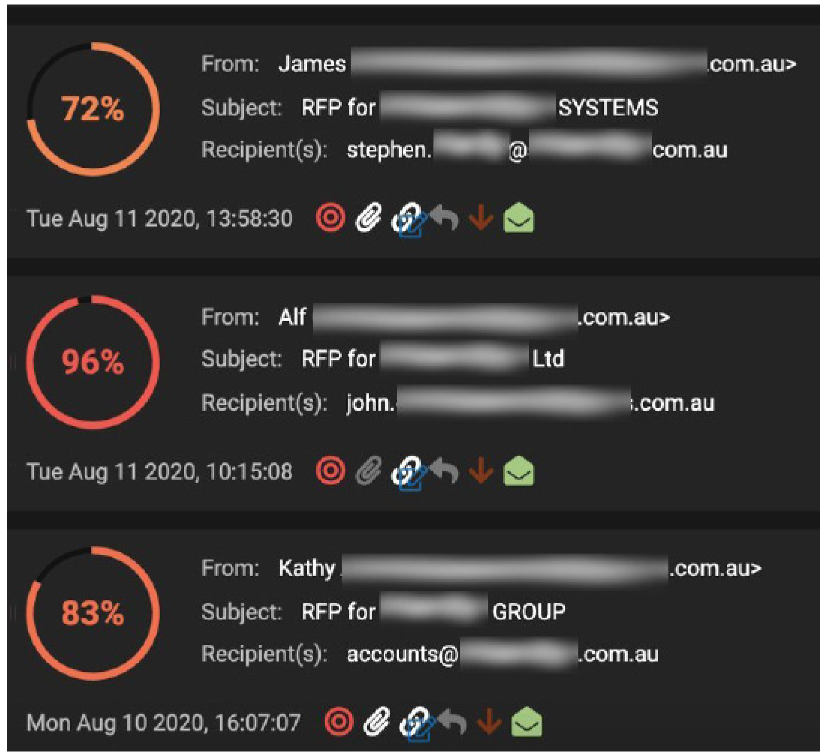
Gartner Reviews

Industry Recognition

By hijacking the account details of a trusted contract in an organization's supply chain, threat actors can gain the trust of a recipient and coax them into clicking a malicious link or transferring money from the business.

Phishing Attack Leads to Microsoft 365 Compromise

Antigena Email detected that a logistics company was under sustained attack. The cyber-criminal had already performed account hijacks on a number of their trusted suppliers and partners, and had sent out several tailored emails from these accounts to the company which slipped through the gateway.



72%

From: James [redacted].com.au>

Subject: RFP for [redacted] SYSTEMS

Recipient(s): stephen.[redacted]@[redacted]com.au

Tue Aug 11 2020, 13:58:30

96%

From: Alf [redacted].com.au>

Subject: RFP for [redacted] Ltd

Recipient(s): john.[redacted].com.au

Tue Aug 11 2020, 10:15:08

83%

From: Kathy [redacted].com.au>

Subject: RFP for [redacted] GROUP

Recipient(s): accounts@[redacted].com.au

Mon Aug 10 2020, 16:07:07

Figure 4: A sample of the malicious emails from the hijacked accounts; the red icon indicating that Antigena Email would have held these emails back

Antigena Email was being trialed in passive mode, so the attack was not shut down in its initial phases. Fifteen of these emails were opened, and one employee clicked on a malicious link, which led them to a fake Microsoft login page for credential harvesting. Three hours later, an anomalous SaaS login was detected from an IP address not seen across the business before. Shortly afterwards, Darktrace detected an anonymous sharing link being created for a password file.

The following day, the attacker sent out further malicious emails from this account to trusted business associates using the same methodology as before – sending fake and targeted RFPs in an attempt to compromise credentials.

Darktrace's SaaS Module identified this anomalous behavior, graphically revealing that the attacker sent out over 1,600 tailored emails over the course of 25 minutes.

The Managed Security Service Provider (MSSP) running their cloud security was completely unaware of the account takeover. However, with Darktrace's SaaS Module working alongside Antigena Email, Cyber AI autonomously stitched these disparate events together into a single incident and gave the security team full visibility of the account takeover.

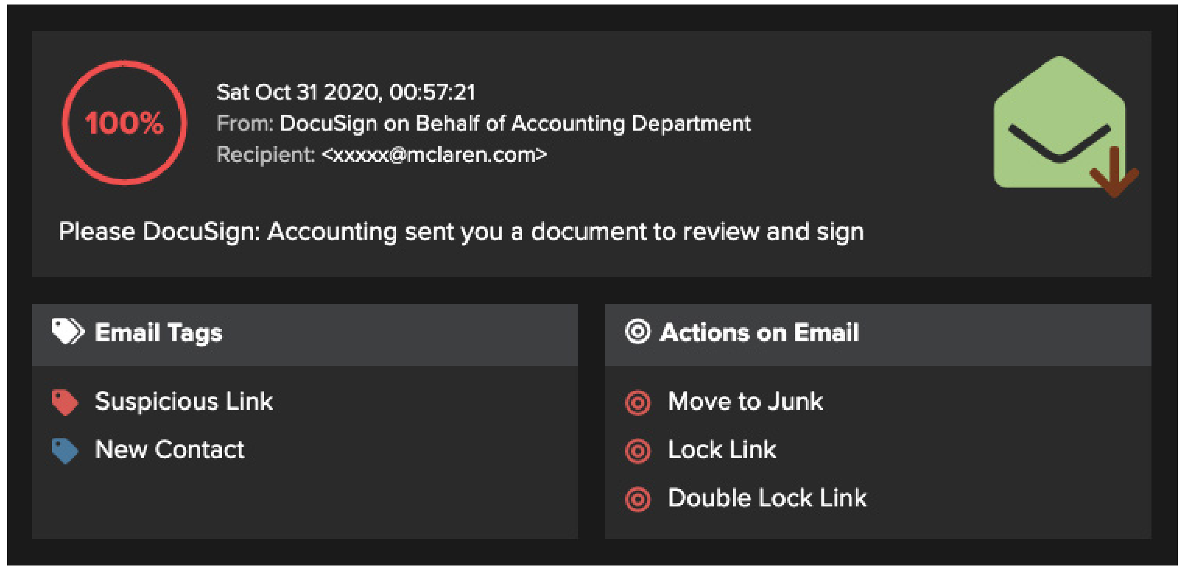
Use Cases: Social Engineering and Solicitation

Email Threat Landscape
Traditional Email Security
Antigena Email
Use Cases
Immune System Platform
Gartner Reviews
Industry Recognition

Attackers can impersonate a trusted colleague, contact, or executive to gain a foothold in an organization. These attacks often exploit the assumption of trust and may come in the form of 'clean' emails, with no malicious links or payloads, which make them difficult to detect.

Stopping a Targeted Credential-Grabbing Attack on McLaren

Antigena Email recently detected an email sent to one of McLaren's executives, prompting them to sign a financial document. The email appeared to come from DocuSign and contained a malicious link hidden behind the text 'Review Document'.



100%

Sat Oct 31 2020, 00:57:21
From: DocuSign on Behalf of Accounting Department
Recipient: <xxxxx@mclaren.com>

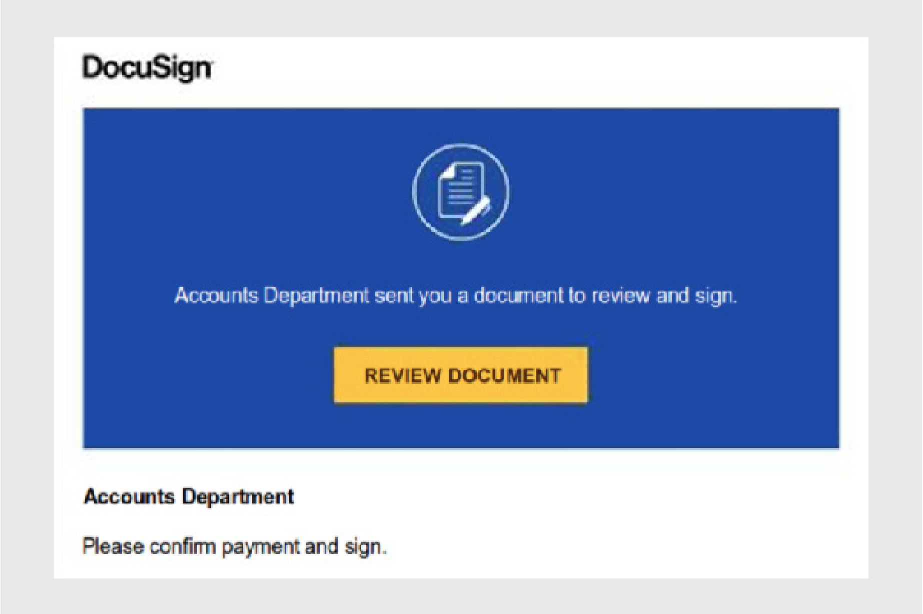
Please DocuSign: Accounting sent you a document to review and sign

Email Tags	Actions on Email
Suspicious Link	Move to Junk
New Contact	Lock Link
	Double Lock Link

Figure 5: An interactive snapshot of Antigena Email's user interface surfacing the email

Had the executive clicked on the link and attempted to log in, they would unknowingly have sent their credentials to the attacker.

The malicious email was sent over the Imola GP race weekend, which was a high-pressured 48 hours for the McLaren team. Antigena Email recognized the sender as a new contact and deemed the link to be suspicious. As a result, it double locked the link and automatically moved the email to the executive's Junk folder, all without having to alert the on-call cyber security team over the weekend.



DocuSign

Accounts Department sent you a document to review and sign.

REVIEW DOCUMENT

Accounts Department

Please confirm payment and sign.

Figure 6: A screenshot of the email in question

Immune System Platform

Email Threat Landscape
Traditional Email Security
Antigena Email
Use Cases
Immune System Platform
Gartner Reviews
Industry Recognition

Antigena Email can be enriched with additional data sources when used as part of Darktrace's Immune System Platform. This allows it to incorporate behavior and insights from other parts of the organization, adjusting an email's threat level in light of network, cloud, and SaaS events across the digital business.

The core of Darktrace's Immune System Platform consists of three tightly integrated autonomous AI systems: the Enterprise Immune System, which detects threats as they emerge, Cyber AI Analyst, which investigates, triages, and reports on security incidents, and Darktrace Antigena, which surgically responds to threats to neutralize malicious activity.

Darktrace's Microsoft 365 SaaS Module adds visibility and protection across Outlook, Microsoft Teams, SharePoint, OneDrive, and more. An equivalent SaaS Module exists for Google Workspace.

When installed alongside Darktrace's Immune System, Antigena Email can uniquely detect an infection in the network (Patient Zero) and perform root cause analysis to see if it originated via email. If so, it will instantly protect the business by stopping all other emails that are part of the same campaign.

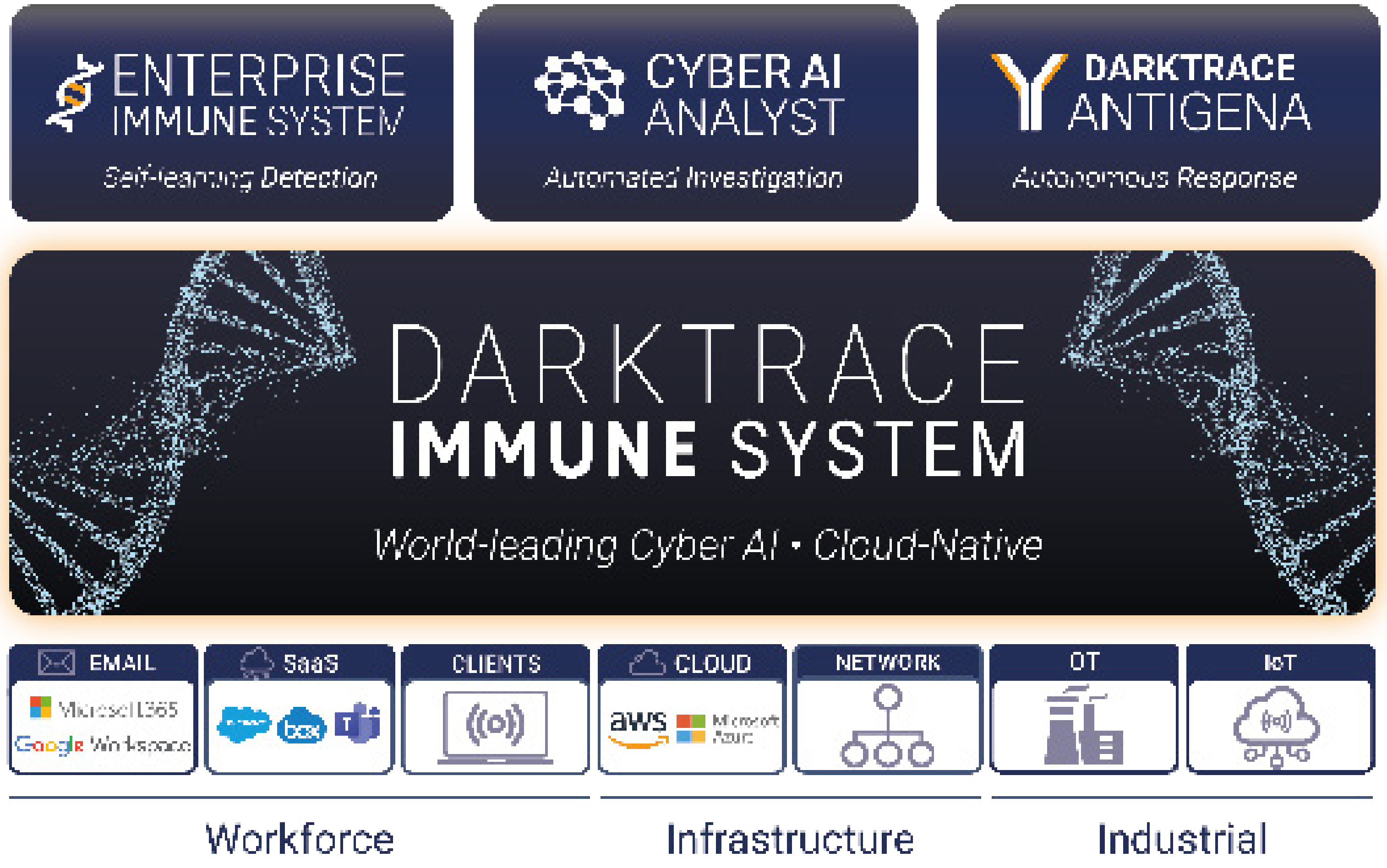


Figure 7: Darktrace's Immune System Platform

> "With Antigena Email we're able to granularly address all of the email issues and see where our emails are really coming from"

Director of Technology, Gallagher-Kaiser

Gartner Reviews: Darktrace Antigena Email

Gartner peerinsights

Email Threat Landscape
Traditional Email Security
Antigena Email
Use Cases
Immune System Platform
Gartner Reviews
Industry Recognition

"Antigena Email is light years ahead of any other email security system."

Cyber Security Vice President, Miscellaneous

★★★★★

"Antigena Email is a gamechanger in the email threat detection landscape."

Director of Business Solutions & IT, Transportation

★★★★★

"Darktrace Antigena Email has proved an extremely reliable and effective solution."

CIO, Services

★★★★★

"An advanced email security solution that does what others can't."

Director Of Information Systems, Transportation

★★★★★

"Fantastic product, easy to use and hugely effective, backed up by a great support team."

CISO, Services

★★★★★

"Truly autonomous security control with an impressive detection rate."

Cyber Security Operations Manager, Manufacturing

★★★★★

"Email protection for the next generation of threats."

CIO, Finance

★★★★★

"Easy to integrate, painless to manage."

IT Director, Manufacturing

★★★★★

Industry Recognition

Email Threat Landscape
Traditional Email Security
Antigena Email
Use Cases
Immune System Platform
Gartner Reviews
Industry Recognition

Computing Technology Product Awards 2020: Winner — Best AI/ Machine Learning Provider

Computing Security Excellence Awards 2020: Winner — Email Security Award

2020 Golden Bridge Awards: Silver — Email Security Innovation

2020 Fortress Cyber Security Awards: Winner — Application Security

The AIconics® 2020: Winner — Best Enterprise AI Solution

UK IT Industry Awards 2020: Winner — Security Innovation of the Year

Marsh Cyber Catalyst Designated Solutions 2020: Cyber Catalyst Designation (Enterprise Immune System and Antigena Email)

Antigena Email has been designated as a Marsh Cyber Catalyst solution for 2020. Evaluated by leading cyber insurers, Marsh has recognized that Antigena Email plays crucial role in reducing cyber risk.

About Darktrace

Darktrace is the world's leading cyber AI company and the creator of Autonomous Response technology. Its self-learning AI is modeled on the human immune system and used by over 4,500 organizations to protect against threats to the cloud, email, IoT, networks and industrial systems.

The company has over 1,500 employees and is headquartered in Cambridge, UK. Every 3 seconds, Darktrace AI fights back against a cyber-threat, preventing it from causing damage.

For More Information

Visit darktrace.com

Book a demo

Visit our YouTube channel

Follow us on Twitter

Follow us on LinkedIn