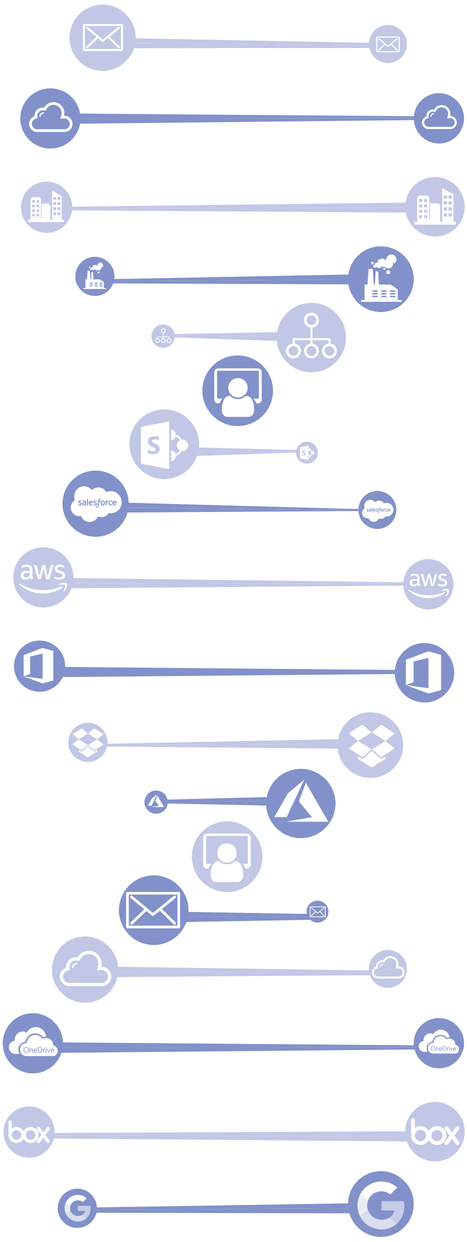
Why Antigena Email?

94% of cyber-threats originate via email, and legacy defenses at the border continue to fall short. Yet whenever Antigena Email and legacy defenses are deployed in the same environment, Antigena consistently neutralizes external threats and data loss that evade email defenses at the border.



Why?

1. AI that learns 'self'

Antigena Email is the only solution that analyzes individual emails in the context of a bespoke understanding of 'self' (what is 'normal') for your entire digital business – not just email:

- Because Antigena understands the normal 'pattern of life' of your employees across cloud, SaaS, email, and the network, it can detect sophisticated threats by spotting subtle deviations
- Antigena treats recipients as dynamic individuals and peers, not mere email addresses, and understands the full scope of their normal behaviors
- By contrast, legacy defenses analyze each email in isolation and correlate it against static rules and signatures, which are based on historical attacks
- Rules and signatures are blind to sophisticated, novel attacks, which are becoming increasingly common

In short, Darktrace knows your entire digital business in a way that other tools do not, and this allows it to catch advanced email-borne threats that would otherwise go unnoticed, while allowing legitimate business email to pass uninterrupted.

2. Decisions that evolve over time

Antigena Email is the only solution that operates as a layered, unified system that updates its decisions in light of new evidence:

- Antigena's decision-making is operative throughout the entire lifetime of an email – from delivery, through to click and execution
- Antigena's unique knowledge of network, cloud, email, and SaaS events allows it to adjust its appraisal of a given email's level of threat in light of new evidence, and vice versa
- Legacy email defenses only operate at the border and are blind to past, present, and future network and cloud events that would greatly enhance its decision-making
- Threats that might be benign at the point of delivery can be neutralized if they present a later threat evinced in the context of the network

3. Accurate & precise action against the full range of targeted email attacks

Together, (1) and (2) drastically improve Antigena Email's accuracy when deciding whether a given email is malicious or benign, which means that more malicious emails are stopped, and far fewer desirable emails are held back than with other solutions that do not have this context.

Thanks to this unique approach, Antigena Email will not only stop less advanced, 'known' threats that legacy defenses would, but it is also best-in-class at stopping the sophisticated threats that evade legacy defenses by design:

Social Engineering Attacks

- Traditional email defenses often fail to stop social engineering attacks, especially when they do not include links or attachments (i.e. 'clean' emails) that could be used to correlate against blacklists and signatures. Since Antigena Email 'knows your network' in a way that other tools do not, it can spot subtle deviations in the metadata that reveal seemingly benign emails to be unmistakably malicious.

Unknown Malware & Impersonation Attacks

- If an email does include a malicious link or attachment but the domain is unknown, Antigena Email will still catch it when others do not because the system does not rely on blacklists or signatures. The same logic applies to newly registered spoof domains used in subtle impersonation attacks.

External Account Hijacks

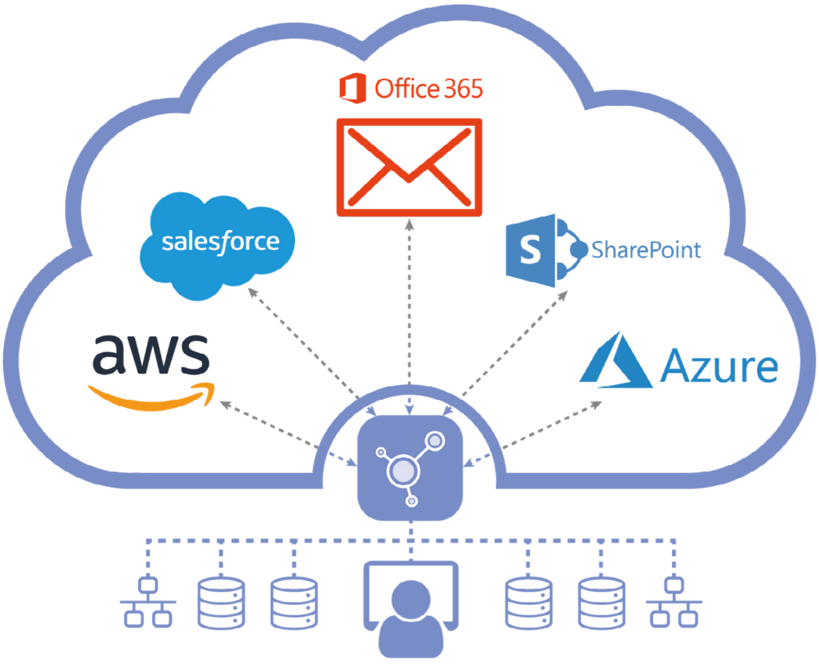
- Since Darktrace analyzes and understands your organization's and users' relationships with trusted external contacts, Antigena Email can pick up on subtle inconsistencies that point to a compromised account, and it can take autonomous action to protect against this. Legacy email defenses assume trust, which means that account hijack attacks often go completely unnoticed.

Inbound and Outbound Data Loss Protection

- Because Antigena Email understands the full scope of your users' 'pattern of life' in every corner of the business, it knows which files they should and should not have access to and where they should or should not send them. Antigena is not only neutralizing malicious inbound emails, but also alerting on malicious outbound emails – this could be an insider threat or bad leaver emailing files to themselves to send to a competitor or use in their next role, or simply a naive employee sending work home against corporate policy.

All email tools will require a holistic view of the entire environment, not just email data, to identify increasingly sophisticated email threats in the years to come.

Antigena Email is the first and only solution that does this.



Antigena Email is the only solution that analyzes data across the digital business and in light of new evidence – whether that evidence is made manifest in email, or in emerging behaviors in the network.

Additional Benefits / Use Cases

Learning from Patient Zero

By correlating Darktrace's understanding of the infrastructure, SaaS, and email environment, Antigena Email can uniquely detect an infection in the network (Patient Zero), and automatically 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.

From an operations perspective, someone still needs to clean up the laptop of the first victim, but that's much better than cleaning up 200 or worse. By contrast, other email security tools can only provide preemptive protection against a given attack campaign if dozens, hundreds, or even thousands of victims have already been affected across their client base.

Auto-Prioritization of Key Individuals

Antigena Email understands who your users are, which means it can automatically 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.

Surgical Response

Antigena Email was designed with the IT and security team, as well as your busy employees and executives, in mind. It allows email delivery in marginal cases whenever possible by only removing the malicious aspect of the mail – rather than the actual content – thereby greatly reducing or directly off-setting admin workload. Legacy email defenses will often hold such emails back, costing the business time and money.

Because Antigena Email learns on the job, if an email is actioned more or less severely than desired, it will automatically learn to treat a similar email more appropriately in future, meaning the email administrator does not have to create complex rules each time they wish to treat an email differently.

Visibility, Forensics, & Auditing

Organizations that trial Antigena Email and legacy email defenses side-by-side invariably report that Antigena has far superior functionality around email visibility, forensics, and auditing.

This includes the ability in the interface to see which users have clicked on links in an email, whether or not a message has been read, who else has received certain emails, who users normally communicate with, breakdowns of email headers, and more.

Antigena also allows security teams to remove live emails from inboxes if needed, which is not possible with many other tools.

Works with Default Office 365 Controls

When organizations deploy email gateways at the border, they are often forced to disable Microsoft's default security controls in Office 365. This often allows malicious emails that Microsoft would have stopped to evade the entire security stack. Antigena Email and Microsoft's native controls can be deployed at the same time, which means that they can work together to provide meaningful defense-in-depth.

Incognito Email Defense

Email gateways also require organizations to change their 'MX record', which means that any attacker can immediately see which tools are being used and can craft their attacks accordingly. Because Antigena Email does not sit in line, attackers have less intel on your security stack and will be less likely to target your organization.