DARKTRACE

Email Security for the Legal Sector

Law firms are increasingly under threat from well-researched and targeted spear phishing campaigns, impersonation attacks, and compromised credentials. With the threat landscape widening and cyber-criminals getting more sophisticated, it becomes harder for legal practitioners – and traditional email gateways – to tell friend from foe.

At a Glance

- Protects over 850 organizations globally
- Detects and responds to the full range of emails attacks
- Self-learning AI that understands the human
- Takes a proportionate and targeted response to each threat
- Reassesses each email throughout its entire lifecycle

APPLEBY

Russell Reynolds Associates

ELIAS NEOCLEOUS & Co LLC

BRODIES LLP

cleveland scott york

Wolf Greenfield
SPECIALISTS IN INTELLECTUAL PROPERTY LAW

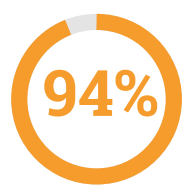
GRAY GRAY & GRAY
CERTIFIED PUBLIC ACCOUNTANTS | ADVISORS
BEYOND THE NUMBERS

Sackers

Securing Sensitive Data While Encouraging Collaboration

The unparalleled volumes of sensitive data held by law firms makes them a perfect target for threat actors. Whether it be confidential information about M&As, witness testimonies, or disclosures made under attorney-client privilege, there is no shortage of valuable material that threat actors are looking to get their hands on.

With working patterns changing, the legal sector is more reliant on email for remote collaboration and communication than ever before. For cyber-criminals, the inbox represents the front door to the valuable data held in an organization's wider digital business.



of cyber-threats start with an email

Why Legacy Tools Have a Limited Approach

Traditional email gateways rely on rules and signatures of previously recognized threats in order to determine whether a given email is 'bad', looking at metrics like the IP address, the domain, and file hashes. This 'surface level' analysis does not do justice to the wider range of characteristics of a malicious email, which can only be understood by applying advanced Cyber AI to email security.

Cyber AI: Asking the Right Questions

Leading London-based firms from Clifford Chance to Slaughter and May are turning to Darktrace's world-leading Cyber AI to protect their sensitive client data from cyber-criminals. This technology uses supervised and unsupervised machine learning to understand the normal 'pattern of life' of every person in the digital business, and then detects subtle deviations that are indicative of cyber-threat.

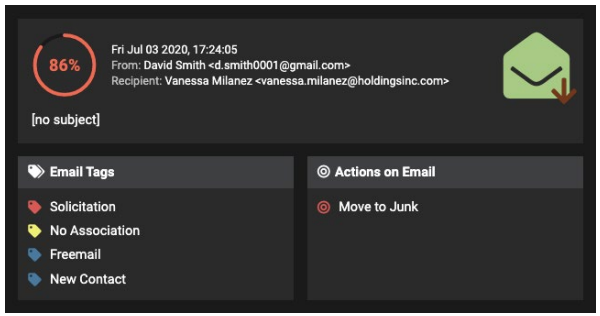
> "Overall the amount of billable hours saved will cover the amount we paid for the solution. That, plus ensuring data trust, are important ROIs."
>
> **Director of IT, Gray, Gray & Gray LLP**

Darktrace's email security technology, Antigena Email, understands the human behind email communications, learning who they typically communicate with, when and where they usually log in from, and the types of links and files that they would normally share, and continuously adapts this understanding of normal in real time.

This approach allows the AI to identify the full range of email threats, from advanced phishing and supply chain attacks, to domain spoofing and account takeover.

Catching C-Suite Impersonation Attacks

Darktrace's Cyber AI caught three related email attacks targeting high-profile individuals, each sent from three separate email accounts impersonating the CEO, the CFO, and a board member.



These emails did not appear to contain attachments or links, bypassing legacy tools that rely on access and deny lists, known attacks, rules, and signatures to spot and stop threats.

However, Darktrace recognized that these emails fell outside of the normal 'pattern of life' for the recipient, and detected the attempted solicitation contained within the email itself.

> "Having a tool that allows you to react faster and spot the threats that you wouldn't necessarily see is crucial."

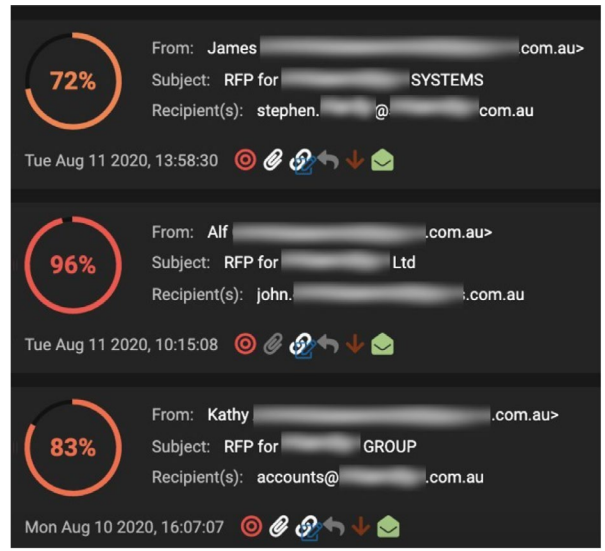
Michael Ioannou, Chief Information Officer, Elias Neocleous & Co LLC.

Detecting Malicious Links Mimecast Missed

During a trial of Antigena Email, the AI detected that an employee's credentials had been compromised after clicking on a malicious link from a trusted third-party supplier.

While Mimecast rewrote the link for further analysis, it failed to identify the threat. This led to over 1,600 malicious, tailored emails being sent from a corporate account in 25 minutes.

At the time, Antigena Email was configurated in passive mode, so while it identified every stage of the kill chain, it was unable to action the threat. Had Darktrace been in active mode, the initial email would have never reached the inbox.



[Discover how Darktrace caught two Microsoft 365 account takeovers]

For more information

- Book a demo
- Download the email threat report
- Hear from our customers
- Read the Emotet blog
- Watch our phishing video

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 4,000 organizations to protect against threats to the cloud, email, IoT, networks and industrial systems.

The company has over 1,300 employees and headquarters in San Francisco and Cambridge, UK. Every 3 seconds, Darktrace AI fights back against a cyber-threat, preventing it from causing damage.