Bank One

At a Glance

- Antigena Email has augmented Bank One's email security posture, protecting prized assets.
- Stops impersonation attacks and novel malware.
- Organization will be trialling Darktrace's AI in the network after seeing success.

Bank One Limited is a top-tier banking institution founded in 2008 following a joint venture between Mauritian conglomerate CIEL Ltd and Kenya-based I&M Group PLC.

Email Security Challenges

Before turning to Darktrace, Bank One already had well-tuned traditional email security tools firmly in place, which were successful in dealing with spam and known attacks. However, with the pace of attacker innovation, they sought to extend their security stack with technology that analyzed each email in context and protected against the most sophisticated threats which often evade traditional email tools on the marketplace. Darktrace's Antigena Email has provided an additional layer of defense against:

Advanced impersonation attacks: Modern impersonation attacks involve the attacker inserting themselves in existing conversations between the bank and its customers, using spoofing techniques and sending fraudulent transaction requests.

Advanced spear phishing using cloud services: Phishing attacks in which the email does not contain any direct phishing link or malicious content, but the recipient is directed to a genuine page which in turn contains the phishing link or malware.

Novel malware: Newly released malware for which there is no Threat Intelligence available.

"Antigena Email has helped us address a major security concern," explains Sanjeev Jhurry, Head of Information Security at Bank One. "It is like having one additional resource on the team; we are very impressed."

"Darktrace's AI complements our traditional email security systems as it adds another protection layer on top of predefined rules," said Mathieu Mariole, Information Security Manager at Bank One. "The number of threats is increasing every day and it's clear that traditional defenses are not bulletproof. Darktrace's AI helps us detect novel and sophisticated attacks that evade traditional tools".

Bank One

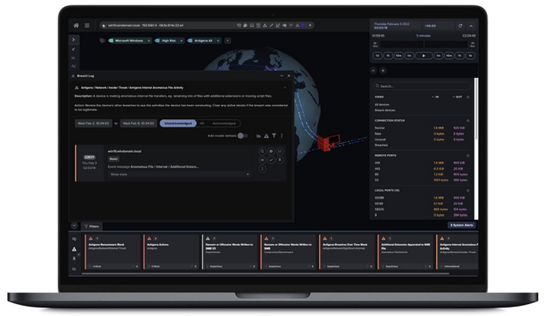
Quick and Seamless Installation from Grove and Darktrace

The team undertook a 30-day trial to see the results of Antigena Email in its own environment, and were impressed with the level of support from both Darktrace and Grove, Darktrace's Partner of the Year in 2020 and 2021.

"The deployment process was simple since the team that helped with installation were very capable," said Sanjeev. Antigena Email was set up in hours and immediately started learning 'self' for every email user in Bank One's digital environment.

"The results were immediate," added Mathieu "We saw a rapid decrease in the number of malicious emails that previously went through undetected by our existing defenses. These threats were successfully addressed by Darktrace. This was the selling point for us, and we were extremely happy with the results."

The team evaluated two other solutions alongside Antigena Email, both were highly rated direct competitors. "During our evaluation, Darktrace clearly took the lead and demonstrated its strength using its highly advanced AI and machine learning capabilities," said Mathieu.



Darktrace's findings and autonomous actions are shown in the Threat Visualizer

Stopping a Targeted Supply Chain Attack

Antigena Email proved its value after it stopped a supply chain attack targeted Bank One, in which a trusted partner's account was taken over and emails were sent to Bank One disguised as legitimate RFPs but containing malicious links. Antigena recognized these emails were unusual in the context of prior correspondence and locked the links, effectively containing the attack.

"It has been almost perfect in stopping malicious emails," explained Sanjeev. "We have started producing metrics on its capabilities and I must say it's impressive. I find it impossible now to imagine life without having this system protecting our emails."

The technology also frees up the team, allowing them to spend their time on more strategic work. As Mathieu explains, "as a small team, we could not afford to be constantly triaging emails or to look through logs and make sure that everything is working as intended." Antigena Email has been a set-and-forget solution, requiring next-to-no manual configuration as it constantly learns about new threats and malicious behaviors by itself.

After seeing the power of Darktrace's AI in the email layer, Bank One is now trialing Darktrace's Enterprise Immune System to detect network-based threats. The technology uses the same underlying approach as Antigena Email, learning normal behavior and spotting subtle anomalies that indicate a cyber-threat. Having different areas of their digital infrastructure protected by a single approach will further improve the ability of the AI to detect and respond to emerging threats across the network and email layers.

> "We saw a rapid decrease in the number of malicious emails that previously went through undetected... I find it impossible now to imagine life without having this system protecting our emails."
>
> Mathieu Mariole, Information Security Manager, Bank One