DARKTRACE

Autonomous Response, Everywhere

How to Stop Cyber-Attacks, Without Disrupting your Business

Contents

A New Era of Cyber-Threat

With cyber-attacks getting faster and more disruptive, it has become clear that human security teams cannot react fast enough to modern threats. Ransomware continues to find new victims and result in large pay outs or significant disruption, as demonstrated by high-profile incidents in 2021 involving Colonial Pipeline, JBS foods and the Irish healthcare system.

These developments have highlighted the need for autonomous systems that can not only detect but *respond* to emerging attacks – and crucially this response must be targeted, containing the attack without incurring disproportionate disruption to the wider business.

As attackers continue to develop new techniques, thousands of organizations are turning to Autonomous Response to take action against novel and sophisticated cyber-attacks. This white paper explores the various applications of Autonomous Response technology, including its ability to respond in the email, cloud, endpoint, and network layers.

> "The ransomware that we are up against today moves too quickly for humans to contend with alone – the way we stay ahead is by having Darktrace AI fight back precisely and proportionately on our behalf"
>
> CIO, Ted Baker

> "Ransomware can spread across your network rapidly, so you need tools that can prevent that from occurring. AI can autonomously take control and provide split-second reactions"
>
> CIO, City of Las Vegas

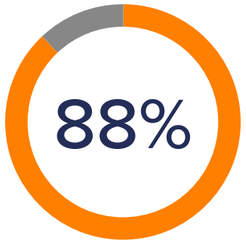
It’s a Machine Fight: AI vs AI

While security teams are already struggling to keep up with today’s threats, the challenge is only getting harder as AI-powered attacks emerge in the wild. In a report published by MIT Tech Review, ‘offensive AI’ is expected to increase the scale, speed, and sophistication of attacks, augmenting every stage of the cyber kill chain.

Deep-learning analytics will enable AI to increase the personalization of attacks, leading to greater accuracy and a higher success rate. At the same time, cyber-criminals will be better able to predict the layout and defensive strategy of victims’ digital infrastructure and data.

Today, cyber security is no longer a human-scale problem: it is a machine-on-machine fight. It is critical that organizations adopt defensive AI to protect against this next generation of automated attacks.

Autonomous Response technology is fundamental to thwarting in-progress threats – no matter how novel or sophisticated. Self-Learning AI understands how and when to respond to contain malicious activity in a targeted and proportionate manner, while sustaining normal business operations.



of cyber security professionals believe it’s inevitable for AI-driven attacks to become mainstream

Forrester

of executives have already begun to prepare for AI-powered cyber-attacks

MIT Technology Review

“Autonomous Response is the crown jewel of our security. It can trigger a broad range of actions, each targeted according to the nature of the threat”

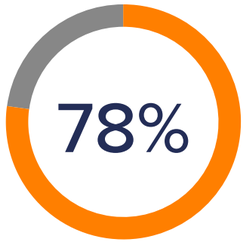
Corporate IT & Security Manager, EV Group

The Limitations of a Traditional Approach

A variety of commonly used security tools - from firewalls and antivirus, to email gateways and preventative controls - rely on the same retrospective approach to threat detection. Their reliance on pre-defined rules, signatures, and playbooks makes them unable to stop novel attacks.

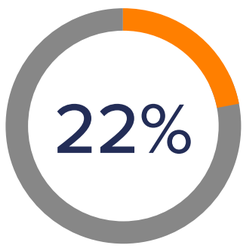
Furthermore, cyber security has evolved in silos. But, with unpredictable employee behavior cutting across a wide range of services and infrastructure, isolated point solutions lack the visibility and context needed to determine malicious from benign.

Traditional tools compensate for this lack of contextual awareness by taking increasingly aggressive actions, ultimately leading to a proliferation of ‘false positive’ alerts and destructive responses.



of IT professionals lack confidence in their company’s cyber security posture

IDG



of organizations feel they lack visibility in the cloud

Cybersecurity Insiders

Automated vs Autonomous Response

Given the speed, scale, and sophistication of modern cyber-threats, human teams alone are no longer capable of staying ahead of attackers. Organizations need a technology that can not only detect attacks but contain them – without a human ‘on call’ to authorize an action.

This has led to automated response solutions, such as SOARs, email gateways, and ‘next-gen’ IPS. While these respond to known threats, these solutions are still bound by historical attack data and pre-defined rules.

As a result, their response mechanisms are mechanical, inflexible, and heavy-handed, favoring a one-size-fits-all approach. In the case of attacks like ransomware, this translates to a choice between encrypted systems or drastic shutdowns.

To fight back, Autonomous Response is needed – stopping ongoing cyber-attacks in a highly targeted and proportionate manner.

The technology works by forming a dynamic and evolving understanding of ‘normal’ for every user and device in an organization, and all the connections between them. This enables the AI to identify the subtle signals of an attack, before taking surgical action in real time to stop the malicious activity while allowing business operations to continue as normal.

Autonomous Response

Fast and Targeted Action

Darktrace Antigena operates as an AI decision-making framework that acts in seconds to surgically neutralize both known and unknown threats in real time - enabling organizations to create self-defending businesses.

Autonomous Response technology calculates the best action to take to autonomously contain in-progress attacks at machine speed. Unlike traditional tools, Self-Learning AI does not rely on a set of pre-programmed, static actions and rules but instead dynamically reacts on the fly to unusual behavior.

It works by enforcing the normal 'patterns of life' for compromised users and devices. Only the malicious activity is interrupted, with employees and systems free to perform their roles as usual.

Darktrace Antigena's proportionate and highly targeted response is only possible through its continually evolving understanding of what 'normal' looks like at a granular level for each part of the digital ecosystem.

> "Darktrace's autonomous cyber response is necessary not only because humans alone cannot keep up with today's threat climate but also because self-driving AI attacks are approaching"
>
> CIO, Elias Neocleous

Key Takeaways

- Takes action to stop unpredictable and fast-moving attacks
- Surgical and proportionate response which prevents business disruption
- Adapts to persistent, evolving threats
- Operative across the entire digital ecosystem
- 24/7 protection

Figure 1: Autonomous Response neutralizes threats wherever and whenever they occur - without the need for human input

Stops the Full Range of Attacks

Due to its approach of learning and enforcing ‘normal’, Autonomous Response stops the full range of attacks, taking targeted action in each case according to the nature of the threat.

Ransomware

Takes action at every stage, from initial intrusion (in the email or network layer) to lateral movement through blocking anomalous connections, to the final stages through blocking unusual data transfers and unusual encryption activity

Phishing Attacks

Locks malicious links and attachments, or holds emails back in the case of a high-confidence attack

Cloud Account Takeover

Logs out a cloud account across all devices in the case of highly unusual and suspicious user behavior

Threats Targeting Remote Workers

Takes targeted action on endpoints, blocking malicious activity without fully quarantining a device

Figure 2: Antigena takes surgical and proportionate action to stop threats while maintaining normal business operations

> “We have confidence in Darktrace’s AI-enabled Autonomous Response, which has a greater capacity for action and response than a human team”
>
> CIO, Delfingen

Protecting All Digital Environments

Unifying enterprise defense in the face of evolving threats and exploding complexity has never been more critical.

Darktrace Antigena understands employees across their digital footprint. This pervasive and unified approach enables the AI to recognize that unremarkable behavior seen in isolation may point to a greater picture of malicious activity.

Cyber AI thrives in changing environments, adapting as new technologies, employees, and systems are added. This helps teams build cyber resilience, with the AI learning 'on the job' to continuously improve its understanding of 'normal' while surgically neutralizing malicious activity in real time.

Self-Learning AI leaves attackers nowhere to hide.

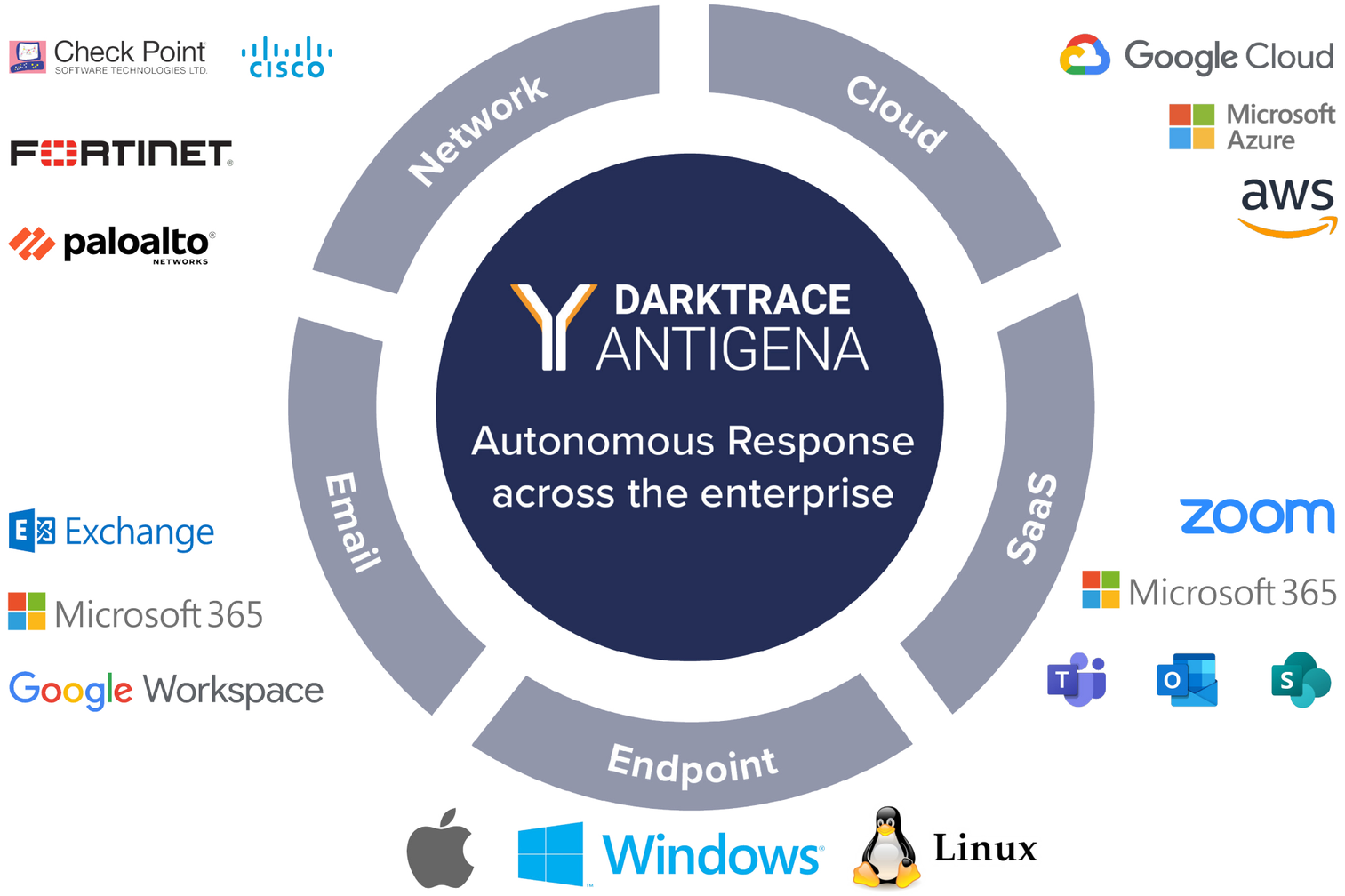


Figure 3: Darktrace autonomously protects digital infrastructure, sensitive data, and employees wherever they are

Real-World Case Studies

Ransomware

Zero-Day Ransomware

Darktrace Antigena stopped a zero-day ransomware attack targeting an electronics manufacturer, detecting and neutralizing this threat in its earliest stages.

The infected device was observed making an unusually large number of connections, writing multiple SMB files, and transferring data internally to a server it did not usually communicate with. Hundreds of Dropbox-related files were then accessed on SMB shares, with several of these files becoming encrypted, appended with a [HELP_DECRYPT] extension.

Darktrace Antigena kicked in a second later. It enforced the device's usual 'pattern of life', immediately stopping the encryption. By the time the AI took action, only four of these files had been successfully encrypted.

This strain of ransomware was not associated with any publicly known indicators of compromise. Nevertheless, Darktrace was able to detect this attack based purely on its comprehensive understanding of 'normal' for every device and user within the organization.

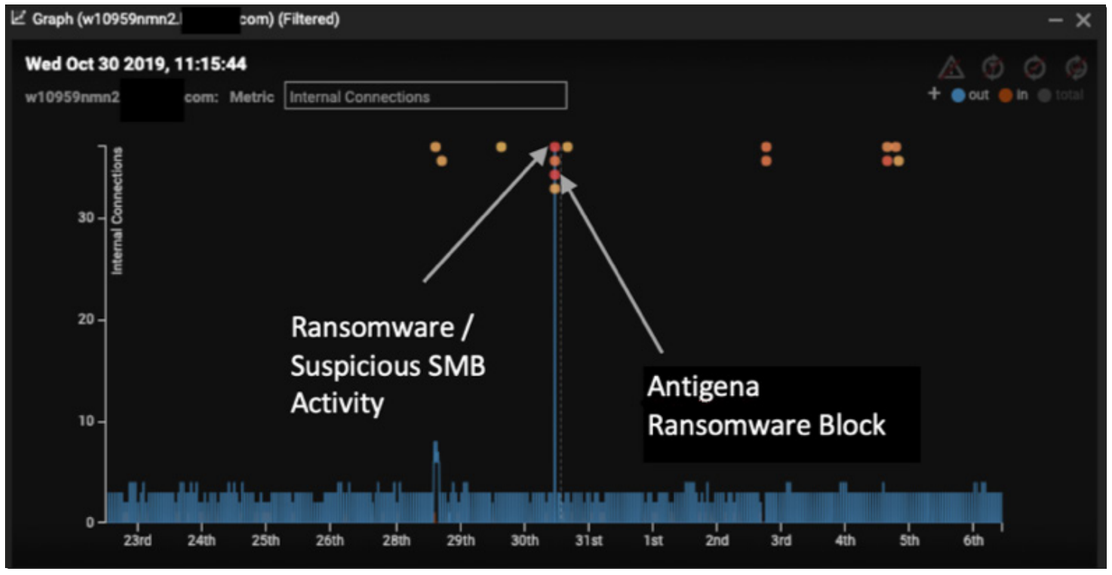


Figure 4: Four model breaches observed on October 30th and a dotted line representing Darktrace Antigena's actions

Automated Ransomware Attack

Darktrace detected and responded to an extortion campaign that occurred on a Friday night.

An employee accessed their personal emails from a corporate smartphone and was tricked into downloading a malicious file containing ransomware. Seconds later, the device began connecting to an external server on the Tor network and SMB encryption activities began.

Within just nine seconds, Darktrace had detected the threat and had raised a prioritized alert. As the behavior persisted over the next few seconds, the AI revised its judgment on the severity of the threat.

Thankfully, while the security team had left the office for the weekend, Darktrace Antigena was on and ready to defend. Self-Learning AI independently stopped the attack, interrupting all attempts to write encrypted files to network shares and preventing a single file from being encrypted.

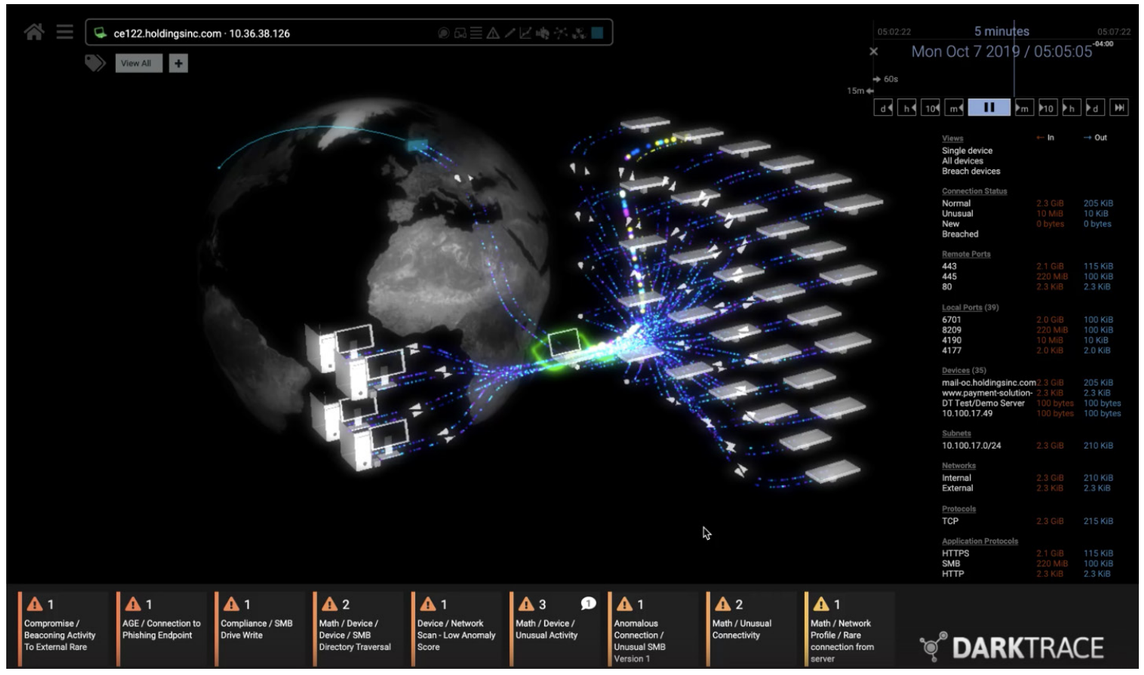


Figure 5: Self-Learning AI identifies a ransomware attack, taking action at machine speed to neutralize the threat

> “Autonomous Response technology combats the most sophisticated ransomware attacks out there and it does that within seconds of the threat emerging”
>
> Chief Security Officer, Sun Life

Email Attacks

Targeted Phishing Attack

During one of the highest stakes race weekends of the F1, a member of McLaren's C-suite was targeted with a phishing attack, 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'.

While the email was well-written and showed no obvious signs of malintent, Antigena Email recognized the latent threat. It noticed that the sender was highly unusual in the context of the organization and recipient, while the hidden URL was deemed suspicious. The AI decided to double lock the link and move the email to the executive's junk folder.

Had the executive clicked on the link, they would have been directed to a fake login page where their credentials would have been harvested, while the legitimate-looking invoice waiting beneath contained the criminals' bank details.

The threat was autonomously neutralized without the on-call cyber security team having to be alerted, so the team could keep focus on their high-stakes race.

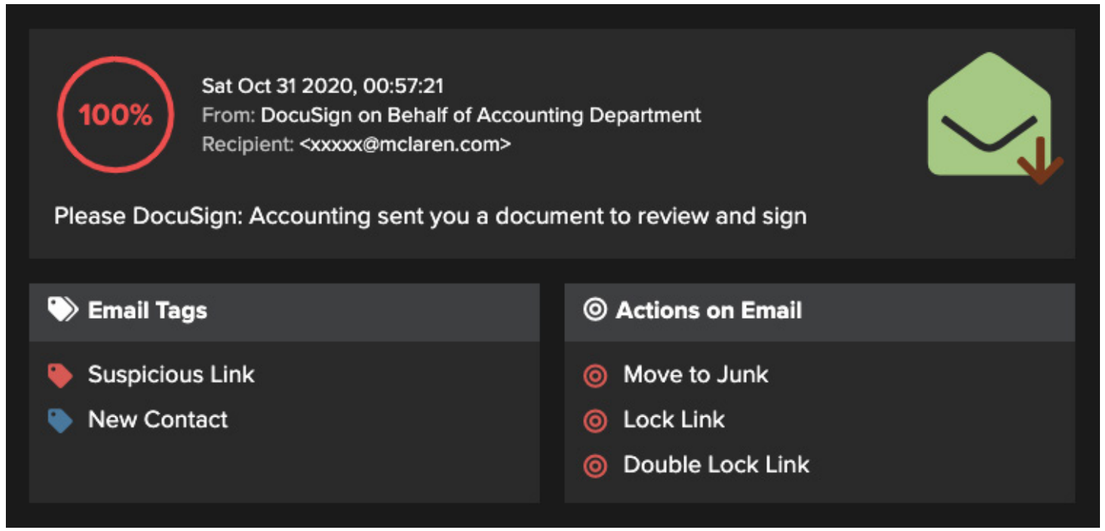


Figure 6: A snapshot of Antigena Email's user interface surfacing the email

> "Antigena Email stopped attacks that were otherwise getting through"
>
> CISO, Calligo

Fake $78,000 Invoice

At one academic organization, an attacker took over an internal Microsoft 365 account and sent a fraudulent invoice to the organization's accounts department. The invoice, which claimed to be from Siemens, contained subtly edited bank details, and the institution paid over $60,000 into an attacker's bank account.

At this point, the organization decided to deploy Antigena Email.

A week after the first attack, another employee SaaS account was compromised, with new email processing rules set up. The cyber-criminal then created an email address, pretending to be from Siemens, and exchanged communication with the hijacked employee account.

When the cyber-criminal went to loop in the organization's account department about a Siemens invoice, this time for $78,000, Darktrace was on and recognized the threat. It held the email back from delivery, protecting the accounts team. The attacker then harvested a company-wide contact list and went on to launch a more generic phishing campaign to dozens of email users across the company, hoping in turn to compromise their accounts.

Antigena Email deemed every one of these emails to be 100% anomalous and held them back in each case.

Figure 7: Antigena Email's intuitive user interface highlights threat trends over time

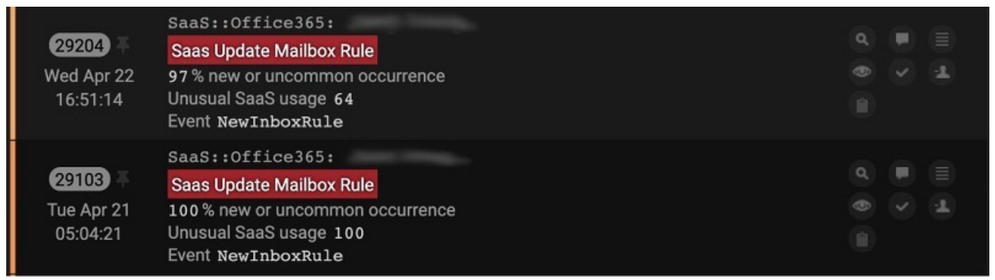


Figure 8: Darktrace detecting the anomalous mailbox rule, indicating a 97-100% anomalous action

Account Takeover

Microsoft 365 Compromise

At a leading technology firm, one employee was victim to an account compromise over the weekend. Darktrace identified the threat in its earliest stages – and had Darktrace Antigena been in Active Mode, the threat would have been stopped before the damage was done.

The attack started when an employee logged in from an unusual location. The user then progressed to setting up new inbox rules and viewed several shared, sensitive files – all outside of this employee's normal 'pattern of life'.

With Antigena Email and Antigena SaaS, the threat would have been stopped at this point. But, as the AI was in Human Confirmation Mode, the attacker proceeded to send over 200 phishing emails containing a link to a Microsoft OneDrive landing page titled 'Contract & Proposal – Customer'. The page contained a phishing link hidden under the display text 'Click to Review Fax Document'.

Less than one hour after the phishing emails were sent, Darktrace's AI detected another unusual login coming from the same IP address to a second account in the organization, indicating this account had likely also been compromised.

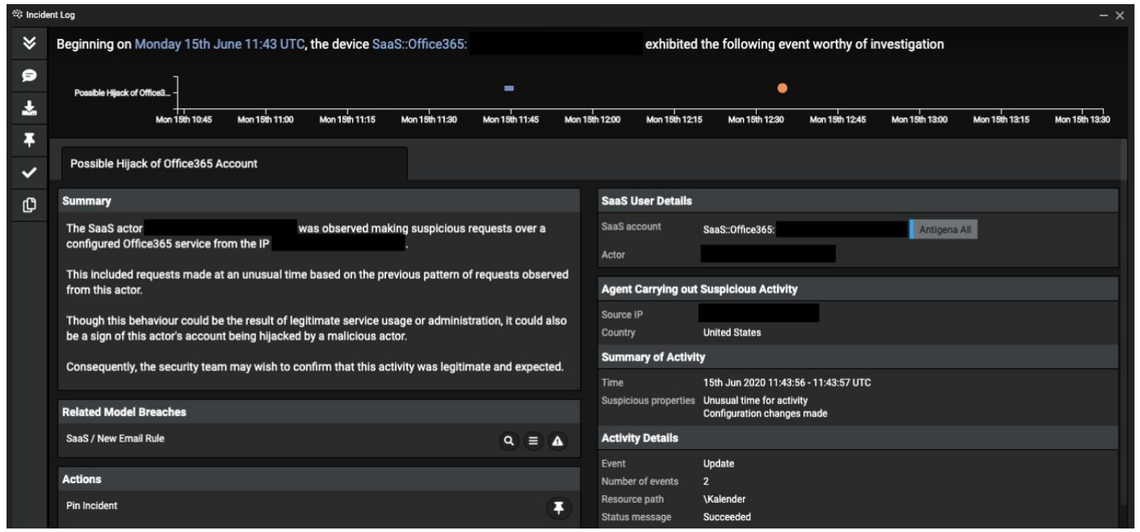


Figure 9: An excerpt of Cyber AI Analyst's report of the account hijack

Fake Request for Proposals

During a trial, Darktrace detected that a logistics company was under sustained attack. A cyber-criminal had performed account hijacks on a number of the company's trusted suppliers and partners and had sent out several tailored emails from these accounts.

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. Had Antigena Email been in Active Mode, these emails would not have made it into the employees' inboxes.

Three hours later, an anomalous employee SaaS login was detected from an IP address not seen across the business before. At this point, Antigena SaaS would have responded, locking the user's account and enforcing their 'pattern of life'.

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

Darktrace autonomously identified this anomalous behavior, graphically revealing that the attacker sent out over 1,600 tailored emails over the course of 25 minutes. Meanwhile, the Managed Security Service Provider (MSSP) running their cloud security was completely unaware of the account takeover.

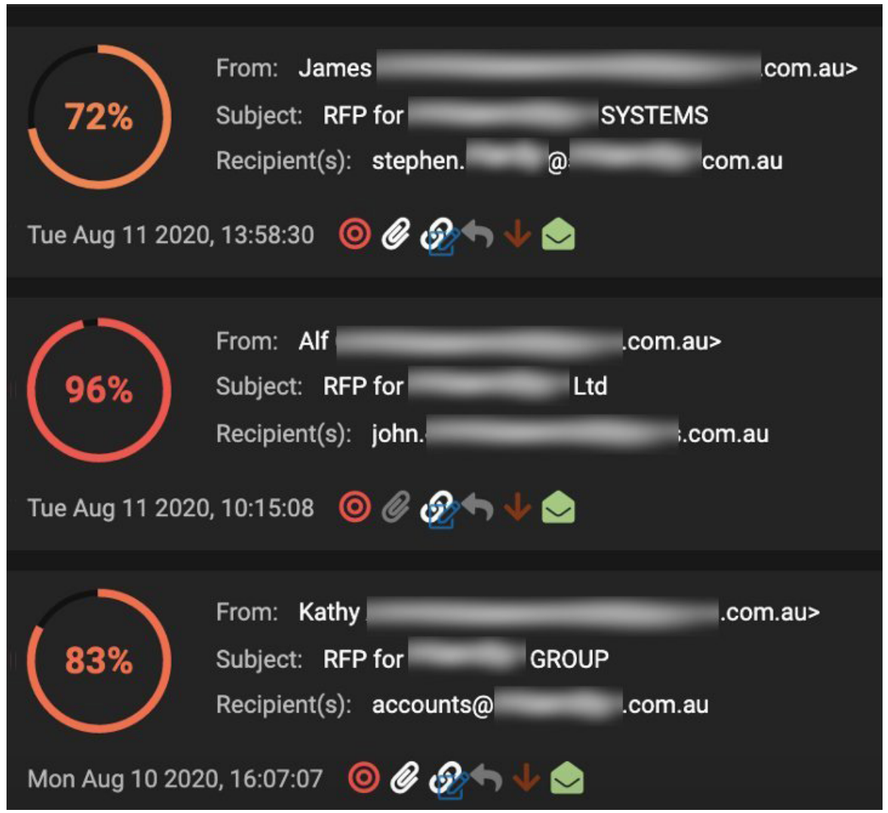


Figure 10: A sample of the malicious emails from the hijacked accounts; the red icon indicating that Antigena Email would have held these emails back

> "Darktrace AI adapts while on the job, illuminating our network and cloud infrastructure in real time, and allowing us to defend the cloud with confidence"
>
> CISO, Aptean

Data Exfiltration

Data Exfiltration Stopped at the Endpoint

Darktrace detected a case of insider threat after an employee was fired from their position as an IT Systems Administrator.

The attack started when the former IT admin logged into their SaaS account and quickly downloaded multiple sensitive files, including contact details and credit card numbers, from the customer database. They then attempted to secretly transfer these files to a home server via one of the company's regular data transfer services. The IT admin knew that this particular service was not only sanctioned by corporate policies but also cloud-based and assumed that the security team would have limited visibility in this area.

However, Darktrace immediately picked up on the unusually large file downloads and the exfiltration, with Darktrace Antigena kicking in to block the attempted upload.

Subsequent investigation revealed that when the employee's first attempt failed, they continued to try and exfiltrate the data via several other methods – first through their corporate cloud account and then through their remote endpoint off the VPN. However, Darktrace Antigena surgically interrupted these attempts at every turn.

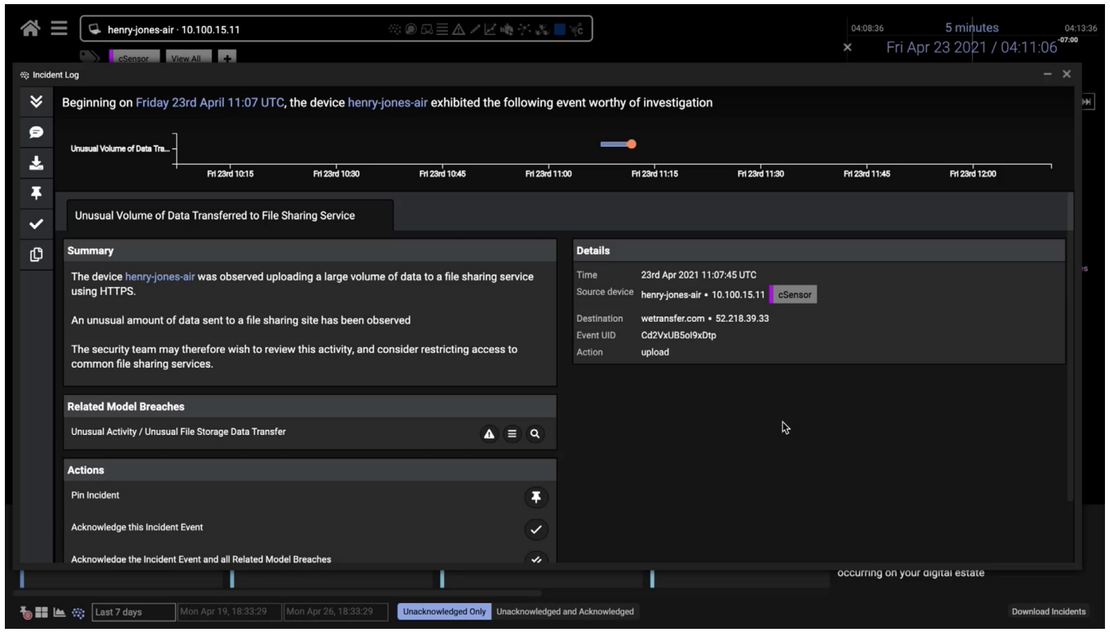


Figure 11: Cyber AI Analyst summary of the incident, including model breaches and actions taken

Industry Recognition

TIME100 Most Influential Companies 2021 — Named as one of the top 100 most influential companies

Microsoft 20/20 Award Winner — Security Trailblazer

2021 SC Awards Europe Winner — Best Security Company Highly Commended — Best Email Security Solution (Antigena Email)

BIG Innovation Awards Winner — Products (Cyber AI Analyst)

CDM Global Infosec Awards 2021 Artificial Intelligence and Machine Learning (Best Product)

The Sales and Customer Service Awards (The Stevies®) 2021 — Bronze — Artificial Intelligence/ Machine Learning Solution (Antigena Email)

Cybersecurity Excellence Awards 2021: Gold — Best Cybersecurity Company, North America

2021 Globee Awards Gold — Customer Service and Support Team of the Year (Darktrace Customer Success)

"Darktrace thrives in complex digital environments, as the technology is adaptive and continues to revise its understanding of 'normal' in light of new evidence, enabling it to detect and respond to threats that other tools miss, while providing complete visibility across the digital infrastructure"

Jonas Knudsen, Research Director, IDC

About Darktrace

Darktrace (DARK:L), a global leader in cyber security AI, delivers world-class technology that protects over 6,500 customers worldwide from advanced threats, including ransomware and cloud and SaaS attacks. Darktrace's fundamentally different approach applies Self-Learning AI to enable machines to understand the business in order to autonomously defend it. Headquartered in Cambridge, UK, the company has 1,700 employees and over 30 offices worldwide. Darktrace was named one of TIME magazine's 'Most Influential Companies' for 2021.

For More Information

- Visit darktrace.com
- Book a demo
- Visit our YouTube channel
- Follow us on Twitter
- Follow us on LinkedIn