DARKTRACE

The Evolution of Autonomous Response

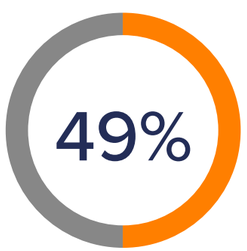
Fighting Back in a New Era of Cyber-Threat

A New Era of Cyber-Threat

Cyber-attacks are ranked by the World Economic Forum as the fourth clearest and most present danger to humanity. As threat actors step up their campaigns and organizations rely on increasingly fragmented digital ecosystems, traditional security tools have proven either too slow or siloed to meaningfully fight back.

Hybrid working has undoubtedly complicated the challenge facing defenders, with sensitive data now spread across a diverse patchwork of cloud services, SaaS platforms, corporate networks, and employee devices. And cyber-criminals have been quick to capitalize on this ever-expanding attack surface.

Spear phishing and ransomware remain top concerns for security professionals, and with cyber-criminals adopting new techniques and updating their attacks faster than ever before, the world has entered a new era of cyber-threat.



of respondents to the World Economic Risk Report 2021 forecast that cyber security failure will become a critical threat to the world in 3-5 years.

World Economic Forum

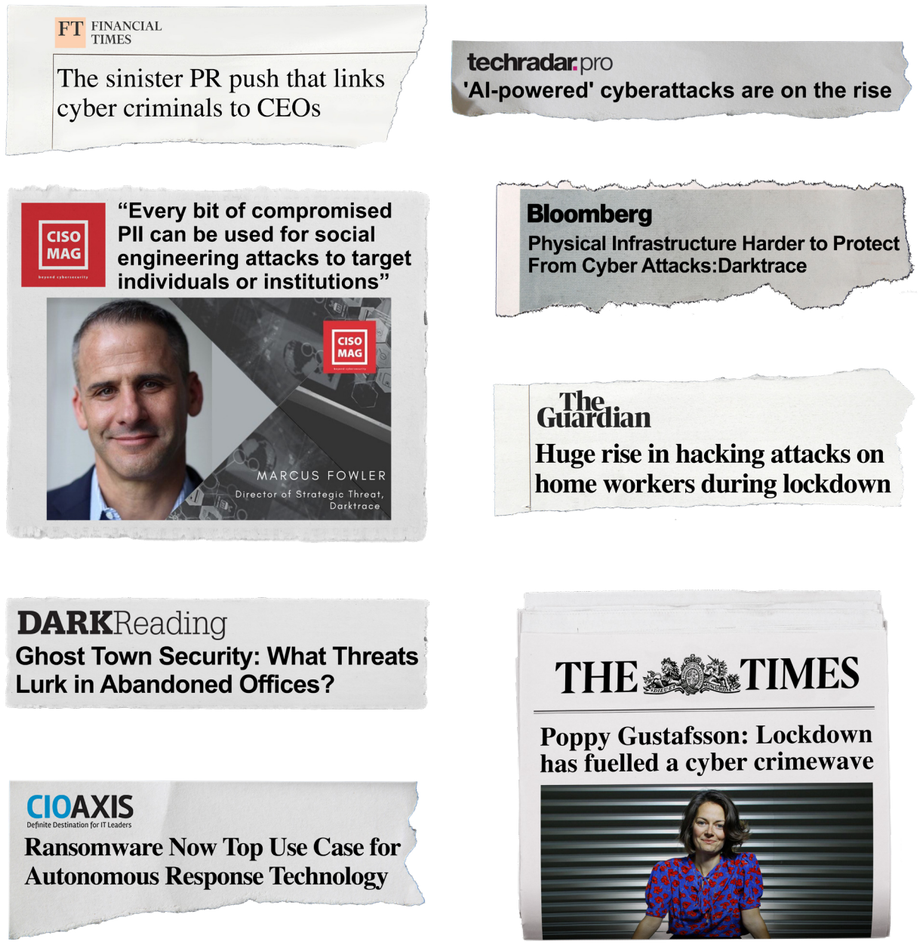


Figure 1: Cyber-attacks are repeatedly front page news, from the Colonial Pipeline attack to SolarWinds

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.

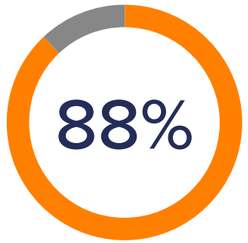
Deep-learning analytics will enable AI to increase the personalization of attacks, leading to greater accuracy and a higher success rate. At the same time, cyber-criminals will be better able to predict the layout and defensive strategy of victims' digital infrastructure and data.

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

MIT Tech Review Report



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

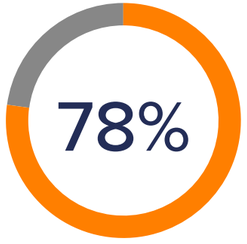
Forrester

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.

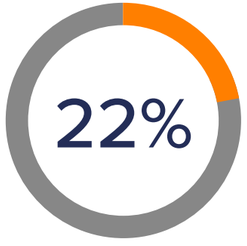
Furthermore, cyber security has evolved in silos. But, with unpredictable employee behavior cutting across a wide range of services and infrastructure, isolated point solutions lack the visibility and context needed to determine malicious from benign.

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, they are 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 subtlest signals of threat, before taking surgical action in real time to stop the malicious activity while allowing business operations to continue as normal.

Autonomous Cyber AI

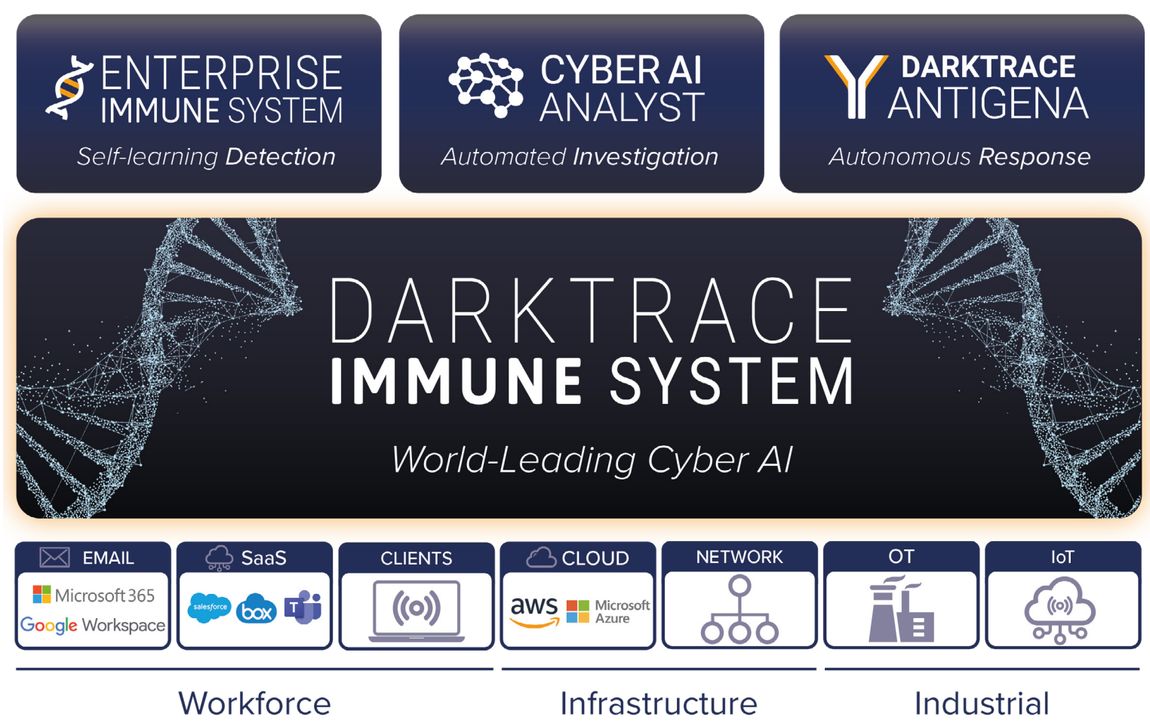


Figure 2: Darktrace's Immune System platform

"We had all the traditional countermeasures in place but we were looking for something different because they don't protect against zero-day exploits. You're always a day behind."

Head of Information Security, British Land

Autonomous Cyber AI thwarts in-progress cyber-attacks seconds after they emerge, without the need for human input.

While traditional solutions pre-define 'bad' or 'benign', Autonomous Cyber AI understands an organization's digital DNA to identify and stop the targeted attacks that inevitably get inside. Powered by unsupervised machine learning, this dynamic and adaptive technology stops threats that static security tools are blind to.

Darktrace Antigena takes action against cyber-threats across the entire digital estate, from the corportate network to email and cloud applications.

Autonomous Response: Proportionate Action to Stop Attacks at Machine Speed

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 Cyber 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 – even on the weekend and at night

Figure 3: Autonomous Response neutralizes threats wherever and whenever they occur - without the need for human input

Around the Clock Protection

Autonomous Response technology is used by thousands of organizations globally to stop threats seconds after they emerge. Providing 24/7 autonomous defense, Darktrace Antigena safeguards critical data and systems when teams are overwhelmed, unprepared, or simply unavailable – at night, on the weekends, and on holiday.

Darktrace Antigena defends against the full range of threats, including:

- Ransomware
- Data exfiltration
- Spear phishing
- Malware
- Crypto-jacking
- Compromised SaaS credentials

Around the world, Darktrace Antigena neutralizes a threat every second – buying back critical time and freeing employees to prioritize strategic tasks.

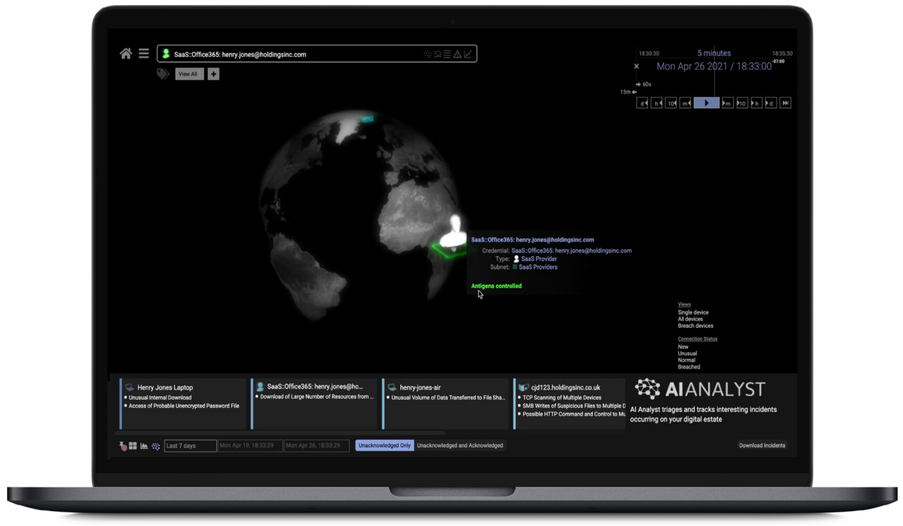


Figure 4: Antigena takes surgical and proportionate action to stop threats while maintaining normal business operations

> "Using AI to autonomously block attacks within seconds, we can feel confident that our data is protected from cyber-criminals – despite our industry becoming more vulnerable by the day."
>
> General Manager, Global Travel

Self-Learning AI Across The Enterprise: Building Cyber Resilience

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.

Autonomous Cyber AI leaves attackers nowhere to hide.

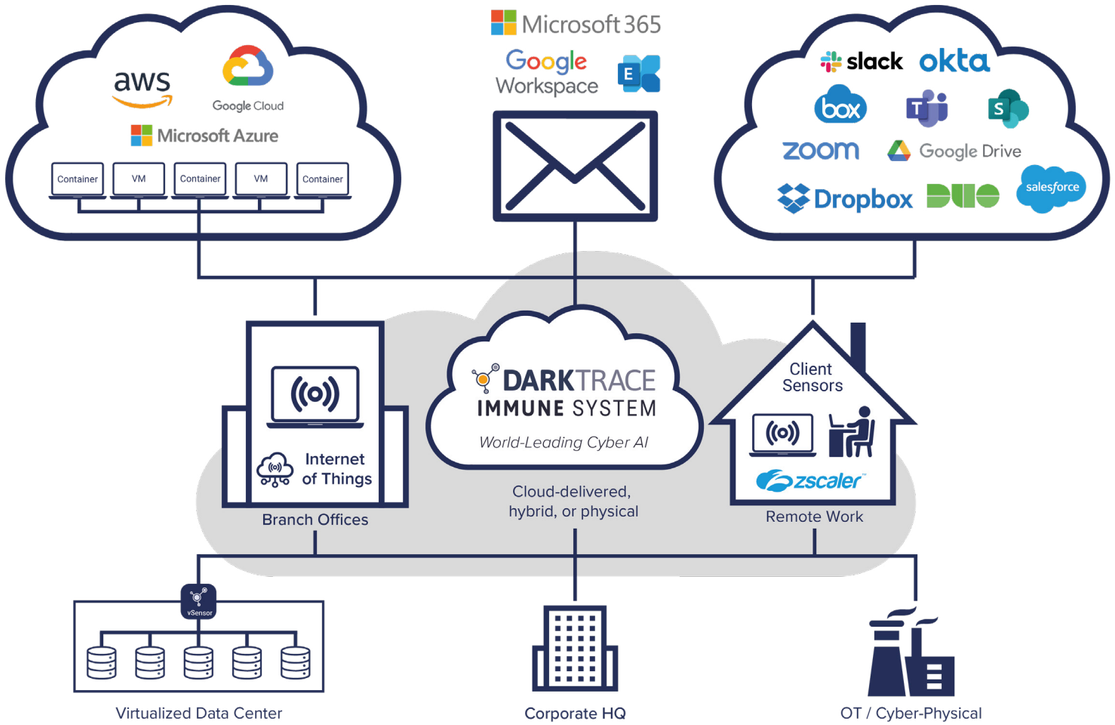


Figure 5: Darktrace autonomously protects digital infrastructure, sensitive data, and employees wherever they are

Stopping Evolving Threats At Every Turn

Darktrace Antigena adapts to threats as they unfold and stops attacks at every stage of the kill chain in real time, wherever they arise. Powered by unsupervised machine learning, Autonomous Response technology is able to scale alongside organizations without requiring manual configuration or fine tuning – even through times of drastic change.

Thwarting Ransomware at Machine Speed

Antigena Network neutralizes the full range of threats across the corporate network and Internet of Things - from fast-moving ransomware, to 'low and slow' attacks and zero-day exploits.

Antigena Network's decisions are informed by an ever-evolving understanding of what 'normal' looks like, which is enriched by its visibility across cloud, SaaS, employee devices, and email services.

In this way, self-learning AI delivers a categorically different response for each threat by understanding how, when, and where to neutralize malicious activity, while allowing the business to operate as usual.

> "Darktrace is helping us stay abreast of the changes that are happening in the digital space."
>
> CIO, McLaren Group

Fighting Back Against Spear Phishing

Antigena Email neutralizes targeted spear phishing campaigns and impersonation attacks that evade traditional tools. By understanding the 'patterns of life' of every user and correspondent, Darktrace is the only technology that truly understands the human behind email communications.

This enables the AI to intelligently determine whether a given email meaningfully deviates from the normal interactions between sender, recipient, and the wider organization - and to stop the threat at the source.

Antigena Email autonomously locks links, converts attachments to harmless file types, and holds emails back to protect the dynamic workforce from the full range of threats.

Defending Cloud and SaaS Environments

From accidental insiders in SharePoint and compromised Microsoft Teams' credentials, to misconfiguration errors in OneDrive and Zoom, Antigena SaaS is singularly equipped to autonomously detect and respond to emerging, cloud-based threats in their earliest stages.

The AI works by correlating on-prem and off the VPN activity with traffic across hybrid and multi-cloud environments in real time, revealing seemingly benign actions to be malicious in the wider context of the enterprise.

Protecting Endpoint Devices On and Off the VPN

Darktrace Antigena delivers autonomous protection for remote workers on and off the VPN, spotting known and unknown threats including insiders, latent strains of malware, downloads of unauthorized applications and software, and compliance issues.

The AI analyzes real-time traffic of users, correlating a web of connections to develop an evolving understanding of 'normal'. This enables Darktrace to not only detect cyber-threats on the endpoint but take surgical and proportionate action to stop them.

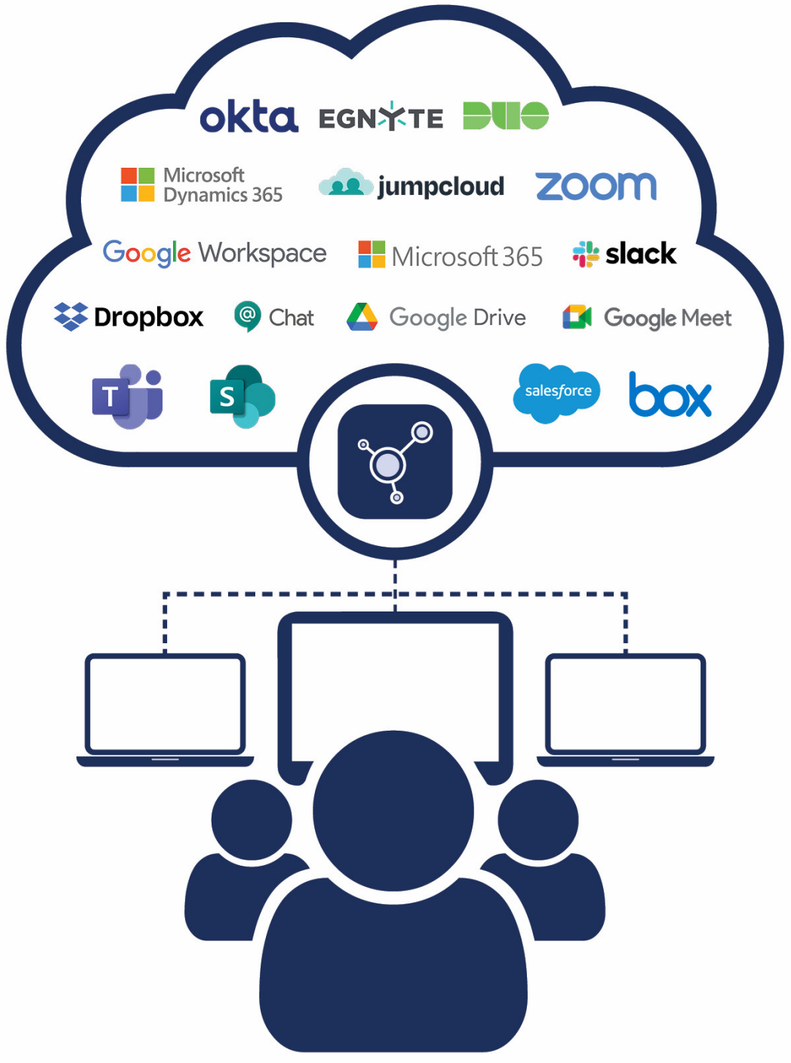


Figure 6: Darktrace seamlessly integrates with a wide range of cloud and SaaS technologies

AI Decision-Making: An Intelligent Response Framework

When faced with malicious activity, Darktrace Antigena can either take self-directed steps or hand off incident insights to existing, third-party security systems. In each case, Darktrace Antigena intelligently judges for itself what course of action is best. The range of measures Darktrace Antigena can take broadly falls into two categories:

Tactical Response

With Tactical Response, Darktrace generates self-directed actions that neutralize attacks in seconds.

Each response is surgical and anchored in the system's granular understanding of 'normal' for every user, device, and peer group, as well as the organization as a whole. This enables Darktrace Antigena to decide which events require Autonomous Response, while maintaining normal business activity during incidents.

"The Darktrace integration with our SIEM was the easiest our team has ever done, and tying the Immune System into all these various integration points has unlocked so much potential in our SOC."

Security Engineer, A&M

Strategic Response

With Strategic Response, Darktrace acts as the 'AI brain' of the entire security stack.

This means that Darktrace takes the AI's high confidence detections and passes them over to third-party systems as a mechanism for response.

Through active integrations, Antigena Network can seamlessly plug into organizations' existing security stacks, informing firewalls, network devices, zero trust technologies, and Lambda functions about attacks that have gotten through.

Darktrace can even direct third-parties' actions as based on system operators' specifications.

Threat Finds: Ransomware

The last stage of the attack kill chain, ransomware is one of the fastest and most deadly threats. Darktrace's self-learning AI detects novel and sophisticated ransomware, and with Autonomous Response, it surgically interrupts the threat in seconds.

Autonomously Neutralizing 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 Cyber 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.

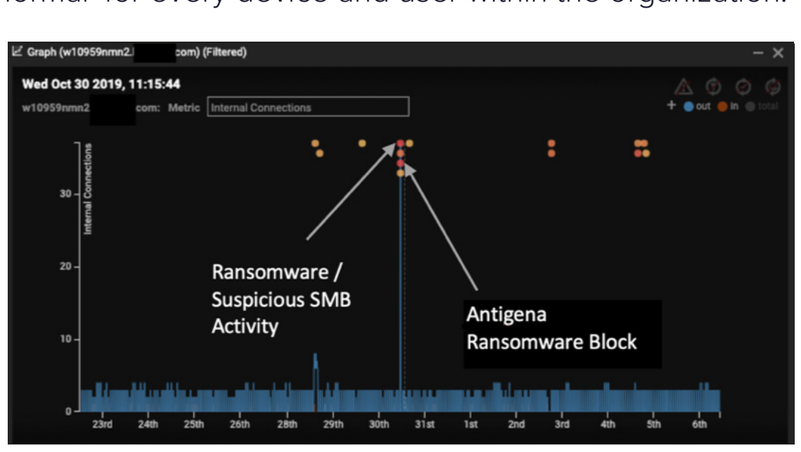


Figure 7: Four model breaches observed on October 30th and a dotted line representing Darktrace Antigena's actions

Stopping Automated Extortion Before Encryption

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. Cyber AI independently stopped the attack, interrupting all attempts to write encrypted files to network shares and preventing a single file from being encrypted.

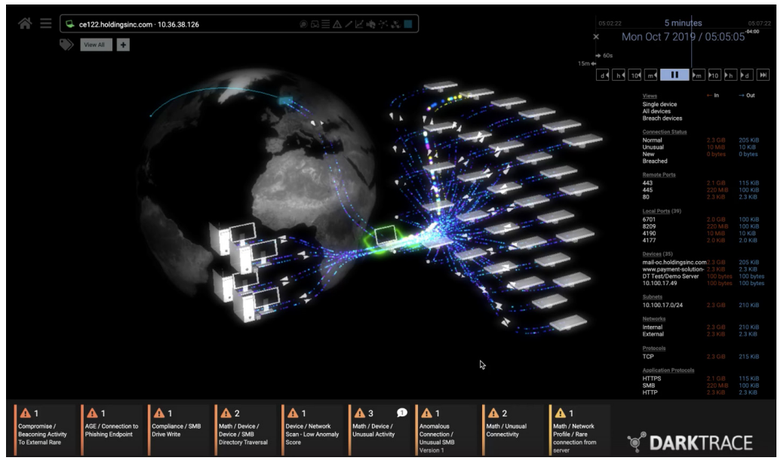


Figure 8: Cyber AI identifies a ransomware attack, taking action at machine speed to neutralize the threat

> "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

Threat Finds: Email Attacks

While traditional gateways measure individual emails against lists of previously encountered attacks, Cyber AI understands 'normal' patterns of an email communication and recognizes the subtle deviations indicative of a threat.

Preventing a Credential-Grabbing 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.

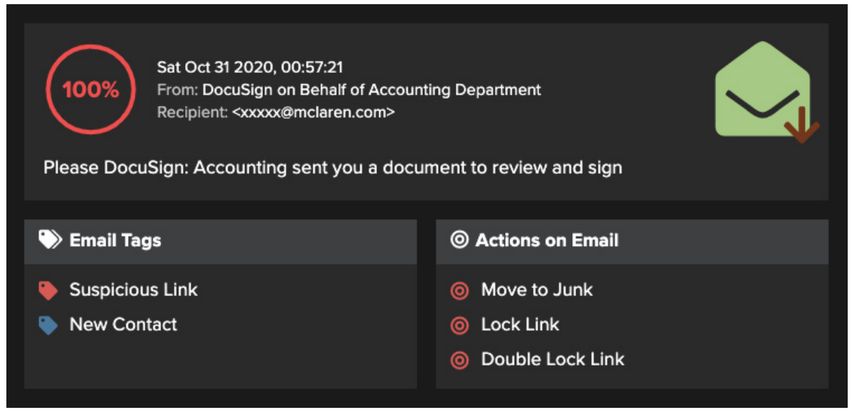


Figure 9: A snapshot of Antigena Email's user interface surfacing the email

"Antigena Email stopped attacks that were otherwise getting through."

CISO, Calligo

Thwarting a $78,000 Siemens Impersonation Attack

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

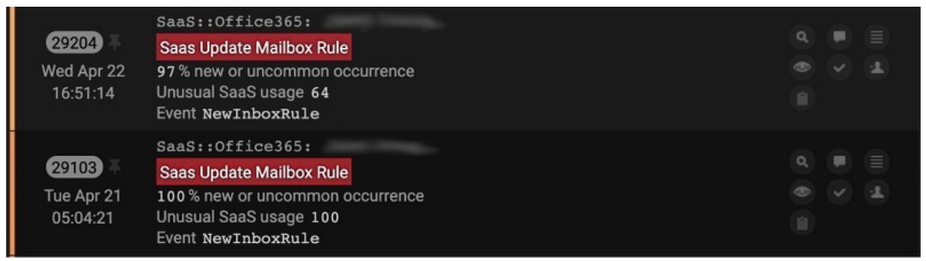


Figure 11: Darktrace detecting the anomalous mailbox rule, indicating a 97-100% anomalous action

Threat Finds: Account Takeovers

Cyber-criminals can hijack corporate accounts in a variety of ways, from email attacks to exchanges on the Dark Web. The endgame is to either steal data or pivot to users' email accounts to launch a malicious campaign en masse. While traditional tools are often blind to this threat vector, Darktrace detects and responds to account takeovers based on its contextual understanding of 'self' for each user.

Microsoft 365 Account Compromise Across SharePoint and Outlook

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.

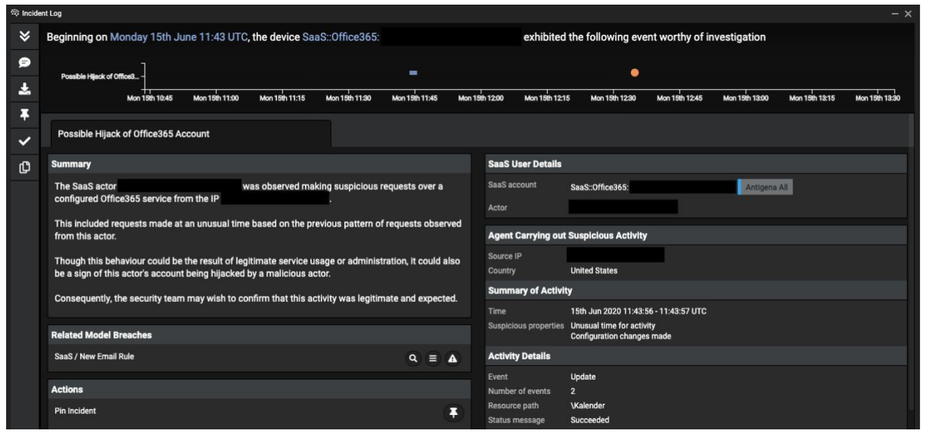


Figure 12: An excerpt of Cyber AI Analyst's report of the account hijack

Phishing Email Leads to Microsoft 365 Account Compromise

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.

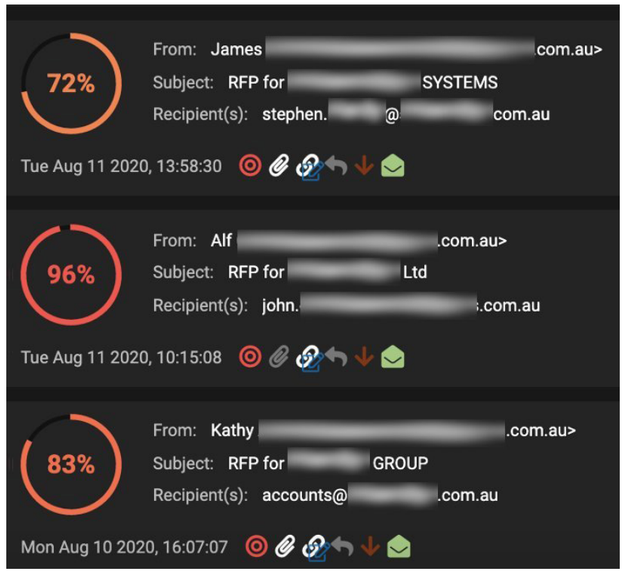


Figure 13: A sample of the malicious emails from the hijacked accounts; the red icon indicating that Antigena Email would have held these emails back

"My Darktrace SaaS Connector notified me of a compromised Microsoft account. Because of this alert I was able to lock the bad guys out and reset the users passwords within 7 minutes of the first improper access."

IT Manager, Hydrotech

Threat Finds: Data Exfiltration

Data exfiltration attacks come in many forms, from insider threats to malware deployment. While traditional tools lack the enterprise-wide visibility to spot overarching patterns that point to a threat, Darktrace's enterprise-wide understanding enables it to stop the subtle signals of an attack.

Disgruntled IT Administrator Attempts to Exfiltrate Data

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.

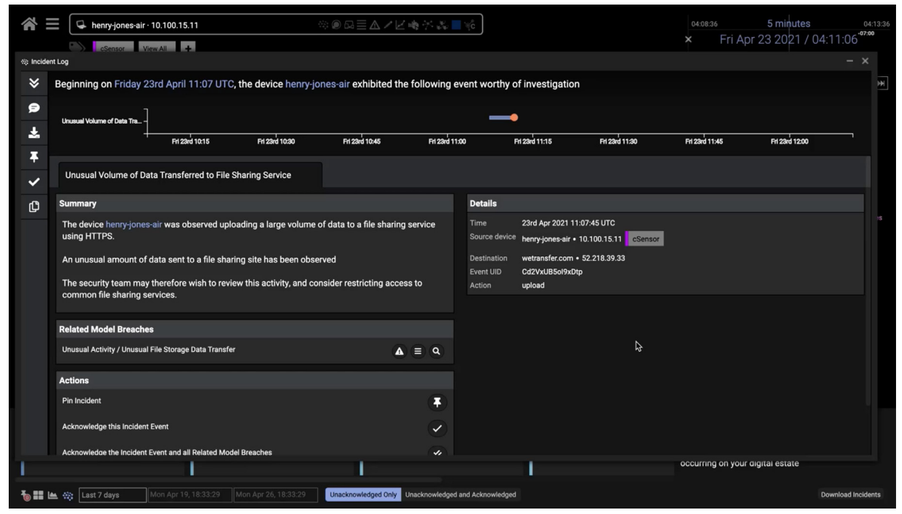


Figure 14: Cyber AI Analyst summary of the incident, including model breaches and actions taken

Stopping a Cerberus Banking Trojan

At a Canadian organization, an employee's device was compromised following a malicious email. The attacker was able to get into the corporate network by deploying malware and posing as a legitimate user. They then moved laterally through the company – looking at sensitive files and data.

Darktrace observed unusual file downloads for the infected device, followed by an attempt at command and control traffic. The attacker was likely trying to exfiltrate the data they had gathered, but Darktrace Antigena blocked this instantly.

Once the AI had stepped in, the organization disconnected the device in question, scanned it, and removed the malware.

The malware in question was the Cerberus banking trojan. Released as free malware on underground hacking forums, it is used to conduct covert surveillance, intercept communication, tamper with device functionality, and exfiltrate sensitive data – including banking details.

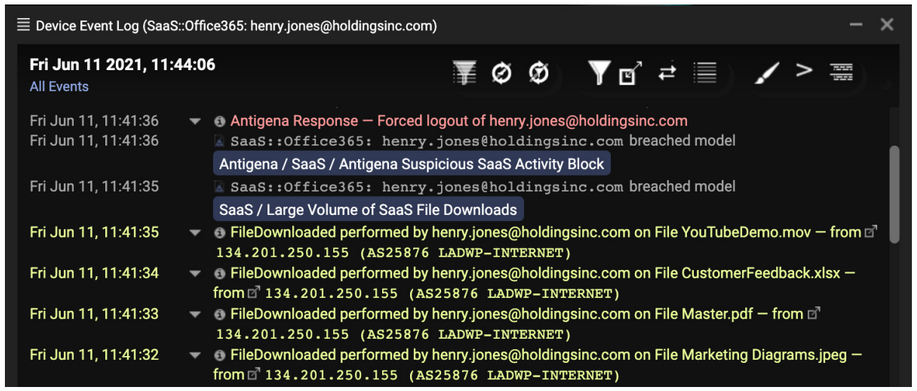


Figure 15: Darktrace Antigena kicks in to block the unusual file downloads

> "Darktrace's Autonomous Response solution Antigena takes action against in-progress cyber-threats."
>
> Jamie Snowdon, Principal Analyst, HFS Research

Threat Finds: IoT Threats

The increasing connectivity of everyday devices has introduced a significant blind spot for enterprises. While traditional solutions lack visibility and struggle to identify novel attacks, Darktrace's holistic coverage allows for protection across the entire digital ecosystem.

CCTV Camera Hack

At a Japanese investment consultancy, Darktrace discovered that an internet-connected CCTV system had been infiltrated by unknown attackers. The perpetrators had used the device to gain a foothold into the network and could watch all of the camera's video recordings from there.

Darktrace's AI quickly detected that something was amiss. Massive volumes of data were observed moving to and from the unencrypted CCTV server, as the attacker gathered data in preparation to exfiltrate sensitive information.

At the point when the attacker tried to exfiltrate the data, Darktrace Antigena took rapid and precise defensive action. The AI surgically blocked data movement from the device to an external server, preventing a serious breach of market-sensitive information, while still allowing the CCTV system to operate in its intended capacity.

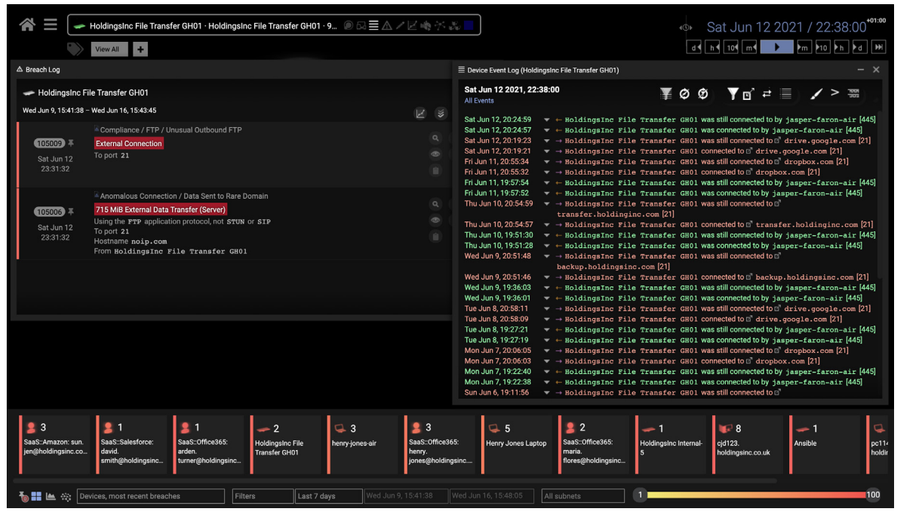


Figure 16: Example of Darktrace detecting and stopping external data transfer attempts – ensuring sensitive data is protected

Data Exfiltration via a Smart Locker

At an amusement park in North America, a threat actor attempted to steal sensitive customer data via a vulnerable IoT device: a 'smart' locker used by visitors to store personal belongings.

Darktrace's AI spotted the attack shortly after the locker started sending an unusual quantity of unencrypted data to a rare external site. The connections were timed in accordance with the device's regular communications with the supplier's platform, suggesting that this was a 'low and slow' attack specifically designed to evade rules-based security defenses.

Within seconds of the threat emerging, Darktrace Antigena took action, intelligently blocking all outgoing connections from the compromised device and giving the security team time to remediate the threat.

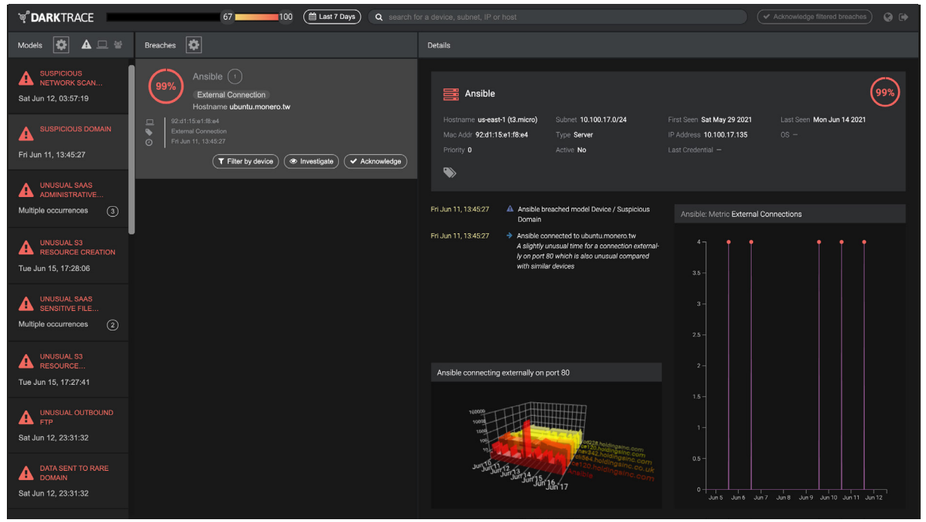


Figure 17: Example of Darktrace spotting and stopping anomalous external connections

> "Whether a targeted campaign or an accidental compromise, I know that Darktrace's AI will catch in-progress threats, safeguarding our corporate and industrial systems before the horse has bolted."

IT Manager, Berry Gardens

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)

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 5,000 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