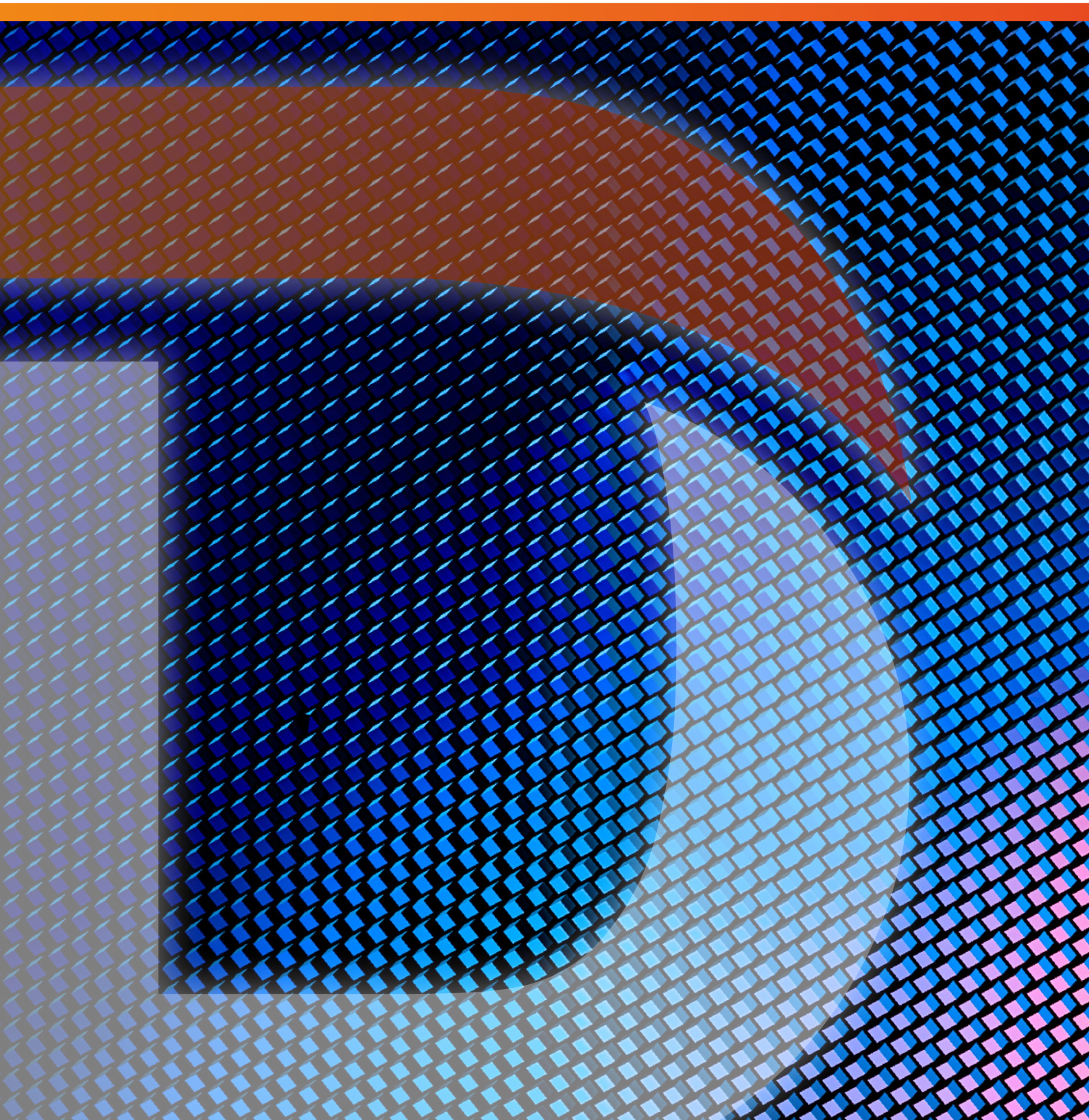
DARKTRACE
Evolving threats call for evolved thinking

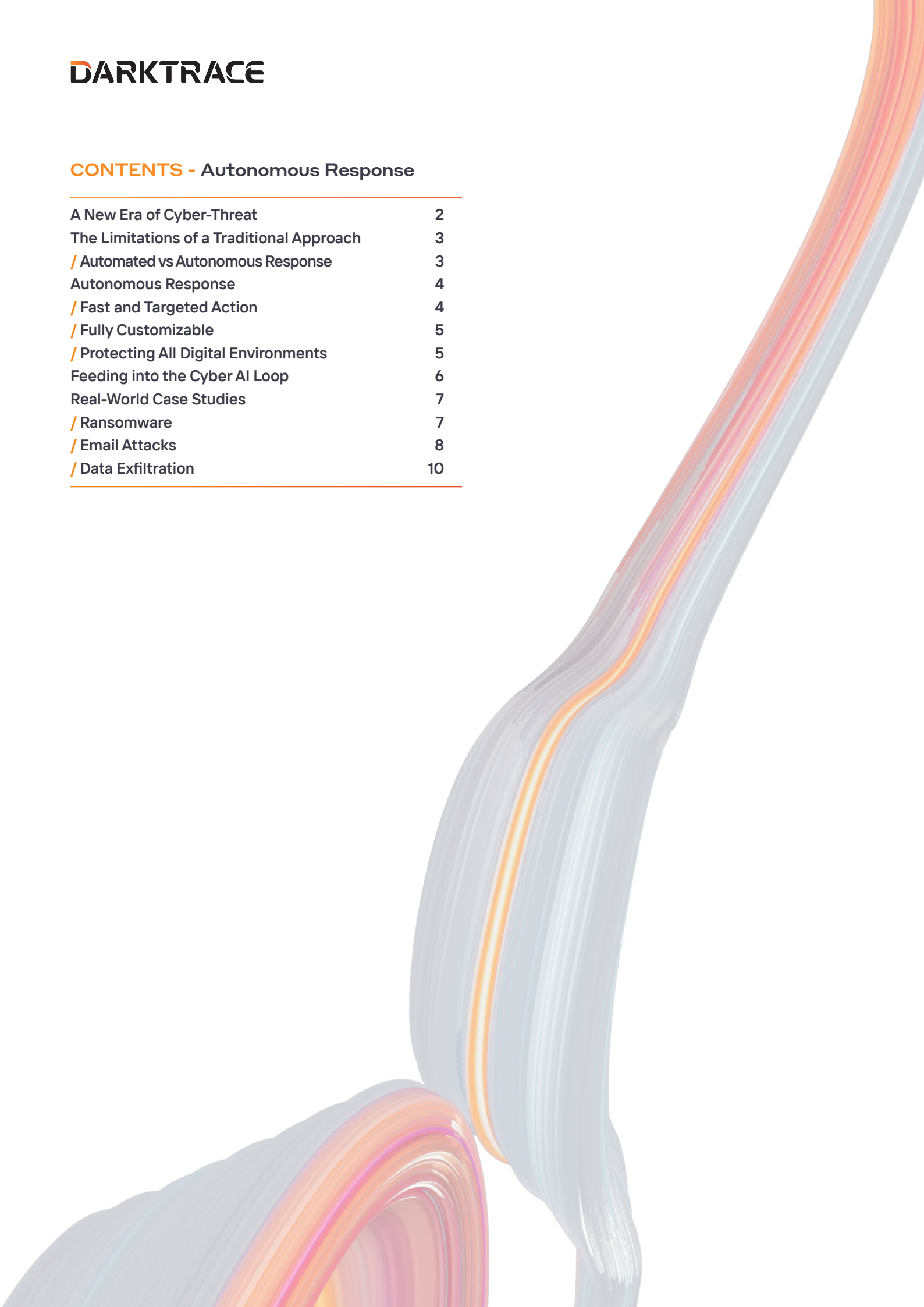
Autonomous Response

Streamlining Cyber Security and Business Operations



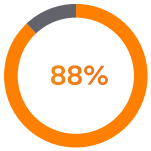
DARKTRACE

CONTENTS - Autonomous Response



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. While ransomware continues to find new victims that result in large pay outs or significant disruption to business operations, the threat landscape also includes supply chain attacks, social engineering, and phishing/smishing attempts. Human teams alone cannot always be relied on to initiate a timely response and high-profile incidents in 2021 involving Colonial Pipeline, JBS foods and the Irish healthcare system show us that human defense teams need additional support when fighting against a variety of threats.



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

These developments have highlighted the need for autonomous systems that can not only detect but respond to emerging attacks in a targeted and concise manner, containing the attack without incurring disproportionate disruption to the wider business.

For these reasons, the cyber security industry has turned to response solutions that automatically contain in-progress cyber-attacks on behalf of human teams, giving them time to catch up and investigate an incident. 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

> 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

> 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

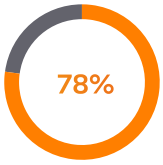
DARKTRACE

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.

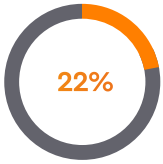
Furthermore, cyber security has evolved in silos. But, with unpredictable employee behavior cutting across a wide range of services and infrastructure, isolated point solutions lack the visibility and context needed to determine malicious from benign.

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 RESPOND enables organizations to create self-defending businesses by operating as an AI decision-making framework that surgically neutralizes both known and unknown threats in seconds.

Autonomous Response technology calculates the best action to take to 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. Instead, it dynamically reacts to unusual behavior.

Darktrace AI'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. By enforcing 'normal', Darktrace RESPOND ensures that only the malicious activity is interrupted, without disrupting regular business operations.

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

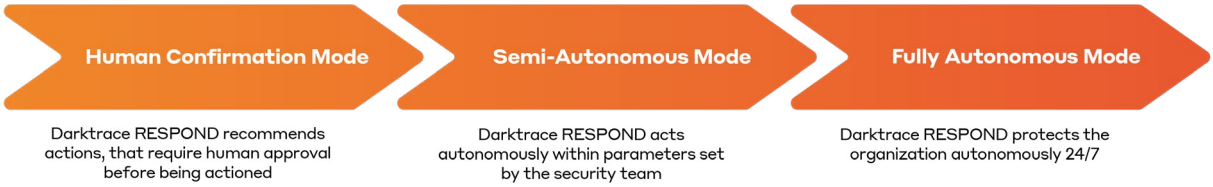
> Darktrace's autonomous cyber response is necessary not only because humans alone cannot keep up with today's threat climate but also because self-driving AI attacks are approaching
>
> / CIO, Elias Neocleous

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

DARKTRACE

/ Fully Customizable

Darktrace RESPOND runs fully autonomously, or can be set to act within guiderails decided by the security team. It can, for example, be set to operate only at certain times, on certain devices, or in response to certain events. As organizations build trust in the autonomous decision-making, many switch to fully autonomous mode within weeks.



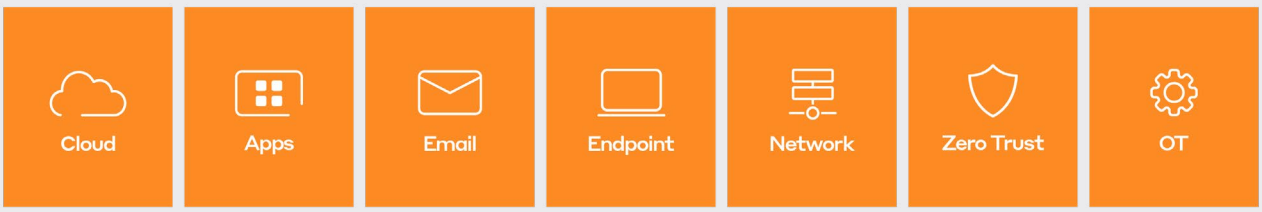
/ Protecting All Digital Environments

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

Darktrace RESPOND 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.

Comprehensive Protection Wherever You Need It

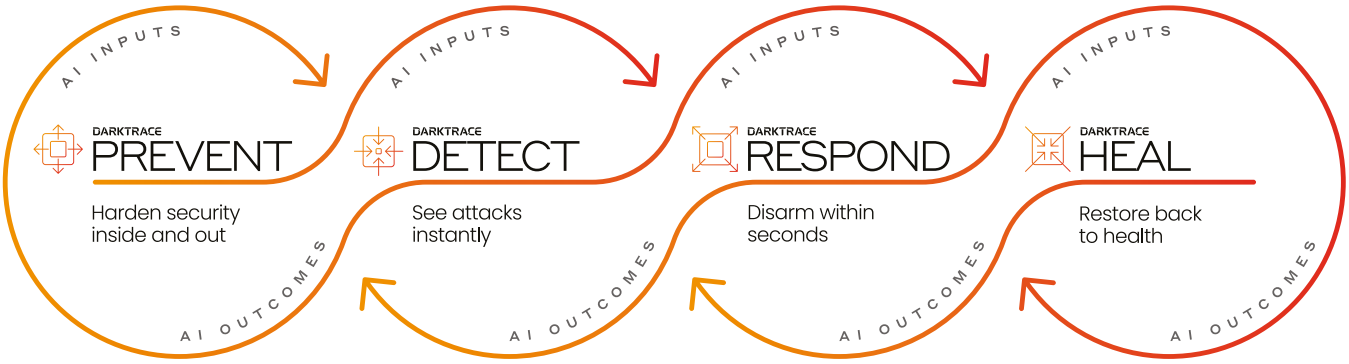


For every major partner and service including:

Google Cloud · Dropbox · slack · Windows · Microsoft 365 · box · aws · Microsoft Azure · Linux · zoom · salesforce

Feeding into the Cyber AI Loop

Darktrace RESPOND forms part of Darktrace's technology vision of a Cyber AI Loop, which empowers defenders to reduce cyber risk and disruption at every stage of the attack life cycle – from proactive measures taken to harden security before an attack gets in, to detecting and containing an attack, through to ultimately healing in the aftermath of a breach.



At each of these stages, it is vital that insights are shared with the wider technology ecosystem, continuously improving the state of cyber security for the organization. But it is equally important for a human operator to understand, at every step, what the AI found, what action (if any) it chose to take, and why. To this end, Explainable AI is hugely valuable in generating natural-language reports that can be quickly and easily understood by anyone – from a new IT starter to a board member.

Real-World Case Studies

/ Ransomware

Zero-Day Ransomware

Darktrace 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 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.

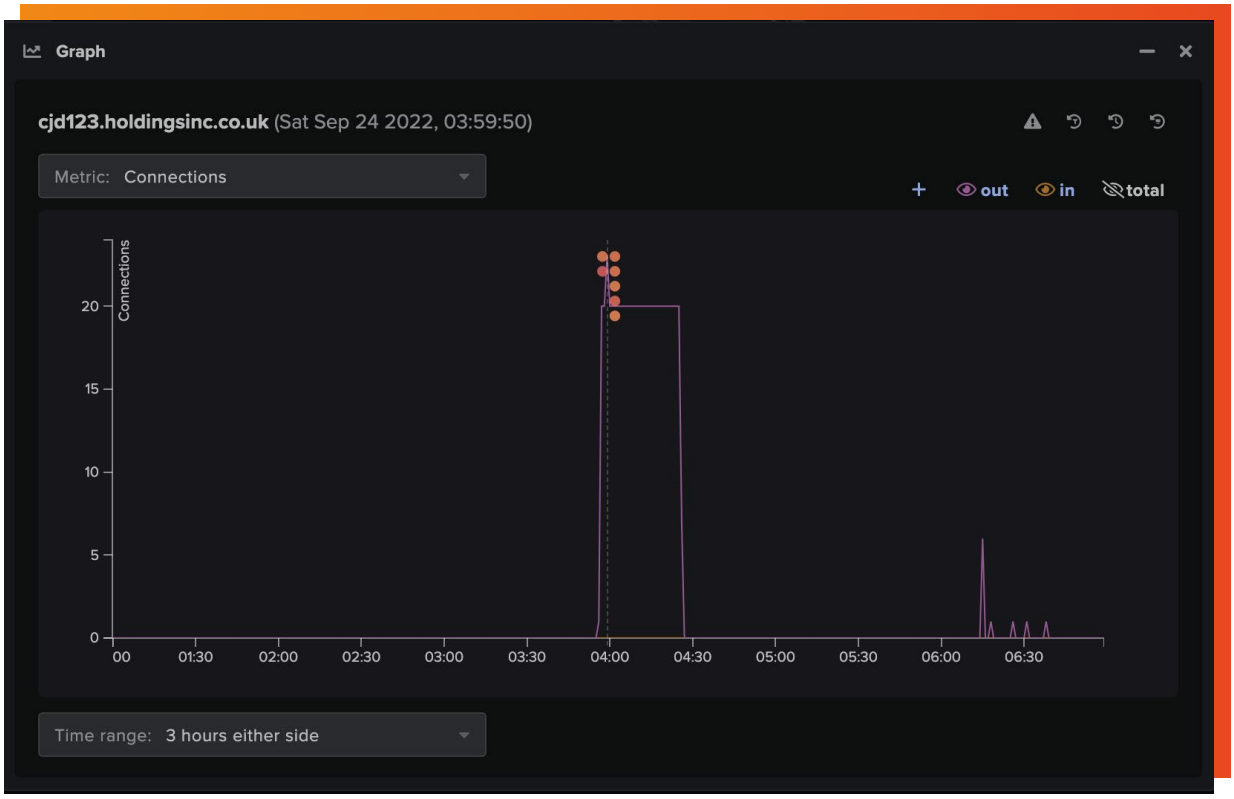


Figure 2: Darktrace displays the spike in connections from the infected device

/ 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, Darktrace/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.

> Darktrace/Email stopped attacks that were otherwise getting through
>
> / CISO, Calligo

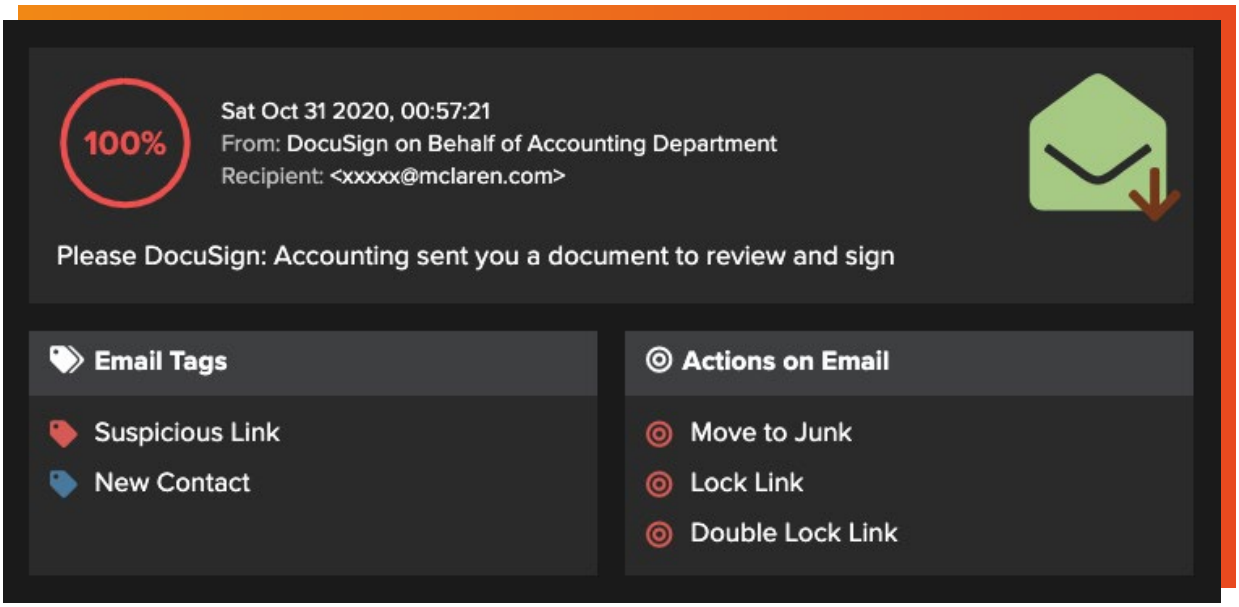


Figure 3: A snapshot of Darktrace/Email's user interface surfacing the email

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 Darktrace/Email been in Active Mode, these emails wouldnnot have made it into the employees' inboxes.

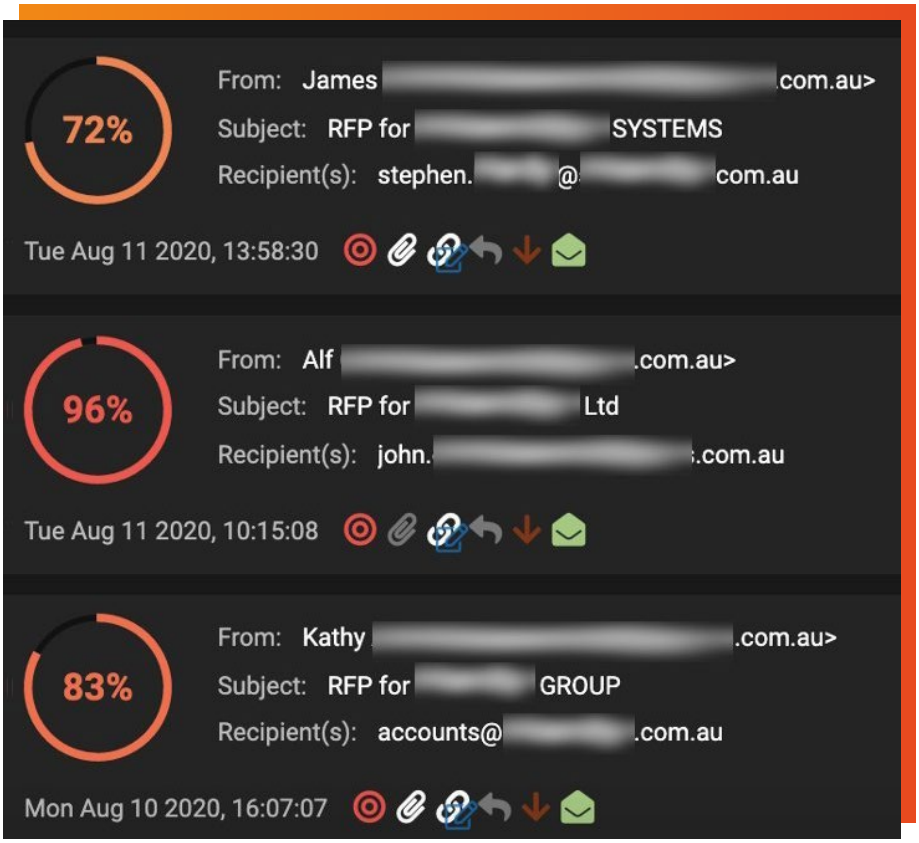


Figure 4: A sample of the malicious emails from the hijacked accounts; the red icon indicating that Darktrace/Email would have held these emails back

Three hours later, an anomalous employee SaaS login was detected from an IP address not seen across the business before. At this point, Darktrace/Apps 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.

/ 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 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 surgically interrupted these attempts at every turn.

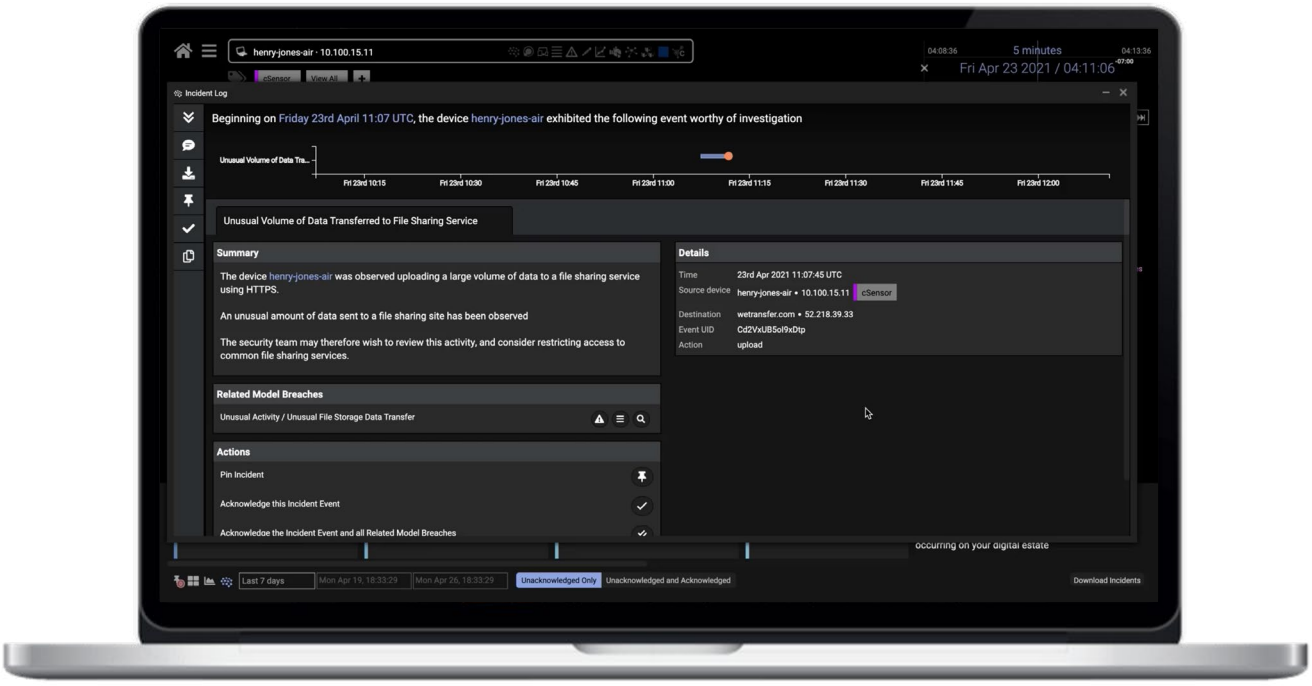


Figure 5: Cyber AI Analyst summary of the incident, including model breaches and actions taken

About Darktrace

Darktrace (DARK.L), a global leader in cyber security AI, delivers complete AI-powered solutions in our mission to free the world of cyber disruption. We protect more than 7,400 customers from the world's most complex threats, including ransomware, cloud, and SaaS attacks. Darktrace is delivering the first-ever Cyber AI Loop, fuelling a continuous security capability that can autonomously spot and respond to novel in-progress threats within seconds. Darktrace has 115+ patent applications filed. Darktrace was named one of TIME magazine's "Most Influential Companies" in 2021.

Scan to LEARN MORE

DARKTRACE
Evolving threats call for evolved thinking

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
Latin America: +55 11 97242 2011
info@darktrace.com
darktrace.com