Insider Threats

Challenges of Identifying Insider Threat

Insider attacks are difficult to spot, yet they often have the greatest impact on business operations. Malicious or compromised insiders can be difficult to identify due to their privileged access and knowledge of company workings, enabling them to easily evade detection.

Despite the risk posed by malicious insiders, firms struggle to monitor employees and respond to these threats. 72% of organizations reported an increase in insider attacks last year, according to Cybersecurity Insiders' 2020 Insider Threat Report.

Recent changes to infrastructure and workforce habits have complicated the situation. The same report notes that more than half of IT professionals say migration to the cloud has made it more difficult to identify insider threats. When it comes to monitoring critical users, only 61% of organizations have visibility over privileged accounts.

On top of this, personal mobile devices have become a particularly common point of exfiltration for both malicious and accidental insiders. Only 13% of organizations state that they can detect insider attacks that start with these devices.

This clear lack of visibility points to the failure of traditional security tools to respond to the needs of today's dynamic workforce. As employees become increasingly mobile and behave unpredictably, organizations require a nuanced, self-learning approach to cyber security, one which does not rely on rules and can detect the subtle anomalies which point to an insider acting maliciously.

> "Insiders don't necessarily have to be malicious. Every employee or contractor is a potential threat."
>
> Director of Threat Hunting, Darktrace

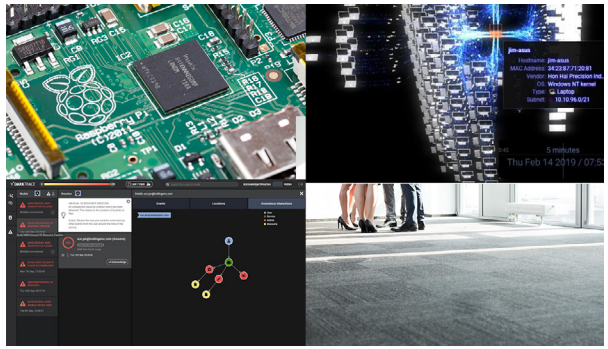


Figure 1: Insider threats can come in multiple forms, as this paper will explore

Threats by Numbers

$11.45 million — total cost of insider threat attacks in 2020.

47% — increase in the number of insider threat attacks attacks between 2018 and 2020.

33% — of breaches are the result of internal incidents.

Darktrace Immune System

Cyber AI: Understanding 'Normal' to Identify Insider Threat

Traditional security tools rely on signatures and pre-defined lists to keep the 'bad' out. This static idea of what is 'good' and what is not becomes untenable against threats which originate from within. As such, they leave companies wide open to insider attacks.

Instead, Darktrace works like a human immune system, detecting and responding to anomalies across the enterprise, no matter when or where they emerge. Cyber AI learns the digital DNA of every user and device in an organization, and all the contections between them, continually revising this understanding 'on the job'. Such a contextual approach enables Darktrace to detect subtle deviations in behavior, applying advanced AI to thwart the targeted attacks which inevitably originate inside the business.

When Cyber AI detects an insider threat, Darktrace Antigena responds autonomously to disrupt the attack in seconds. In addition, Cyber AI Analyst launches investigations into these anomalous incidents, combining the intuition of a human analyst with the speed and scalability of AI, delivering a 92% time-saving in time to triage.

Figure 2: The Darktrace Immune System platform covers the entire digital ecosystem

> "I can sleep again at night. We are confident that if something comes in Darktrace will pick it up immediately, Antigena will isolate it, and we can then take our time to resolve it."
>
> Head of IT Operations, PPS Insurance

Case Study: Threats From The Inside

Hydrotech, Inc.: Contractor's Laptop Compromised

On a normal Thursday morning, a contracted instructor turned on their computer and connected to Hydrotech's Wi-Fi network, as they had every morning that week to prepare for their upcoming class.

Figure 3: Device connects to the network

18 seconds later, Darktrace's AI detected that the laptop was behaving in an extremely unusual way, initiating a scan and making anomalous connections to other devices in the organization.

> "Before Darktrace, we lacked the power to detect if an authorized network user had gone rogue or if a novel threat had bypassed our legacy security systems."

Information Services Manager, Lockyer Valley Regional Council

Figure 4: Device begins network scanning

With its unique understanding of 'normal' for every device, Darktrace recognized this as highly anomalous behavior and alerted the security team to the incident. The Darktrace user interface, the Threat Visualizer, marked the device in yellow and notified the customer via email of the potential breach.

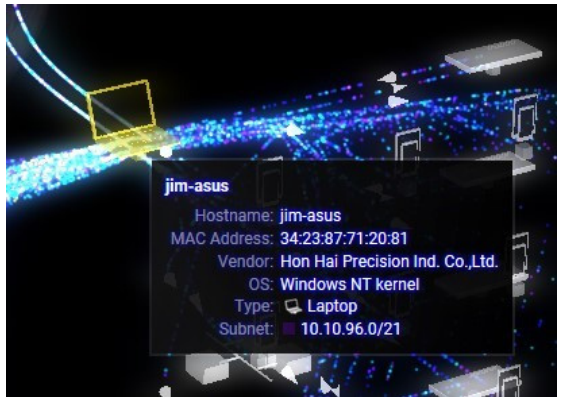


Figure 5: The anomalous behavior is highlighted

As the scanning activity continued and escalated, the Darktrace Immune System increased its anomaly score, with the color of the offending device below indicating the severity of the threat.

Figure 6: Threat severity is raised as the attack progresses

In under two minutes, the instructor's laptop had attempted connections to every device on the network which prompted the following image on the Threat Visualizer interface, leaving no doubt that there was a problem with the laptop.

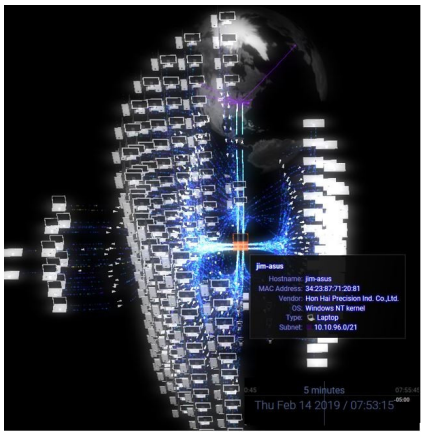
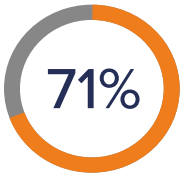


Figure 7: Device attempts total connectivity

The offending device was promptly taken offline, stopping the threat before it had a chance to develop. After investigation, it was concluded that the breach had likely originated from a USB drive which was shared with the contracted instructor by one of his students the night before.



of companies are worried most about accidental data breaches.

"Given the prevalence of never-seen-before attacks and insider threats, we were looking for a technology that could swiftly identify and alert us to anomalies as they emerge, inoculating our network from within."

IT and Infrastructure Manager, Shook Lin & Bok LLP

"Intellectual property is the bedrock on which pharmaceuticals' development and manufacturing is built. Darktrace's AI empowers us to defend that highly sensitive data."

IT Systems and Network Administrator, CordenPharma

Threat Finds: Self-Learning AI in Action

IoT Compromised by a Third-Party Vendor

In January 2021, a North American company suffered a supply chain attack when a technician came in to perform scheduled maintenance on a smart door. As soon as their laptop had connected to the control unit, the IoT device was seen making highly unusual connections to rare external IP addresses.

Darktrace then detected that the control unit was attempting to download trojans and other payloads, as well as mining cryptocurrency with a Monero (XMR) CPU miner. The device was using a SMB exploit to make external connections on port 445 while searching for vulnerable internal devices using the outdated SMBv1 protocol.

One hour later, the device connected to an endpoint related to the third-party remote access tool TeamViewer. After a few minutes, the device was seen uploading over 15 MB to a 100% rare external IP.

The attack managed to bypass the rest of the organization's security stack because it was introduced directly from a trusted external laptop, and the IoT device itself was managed by the third-party vendor, so the customer had little visibility over it.

Darktrace's Cyber AI Analyst reported on every stage of the attack, including the download of the first malicious executable file. The customer was also alerted via a Proactive Threat Notification following a high scoring model breach at 16:59, just seven minutes after the attack had commenced.

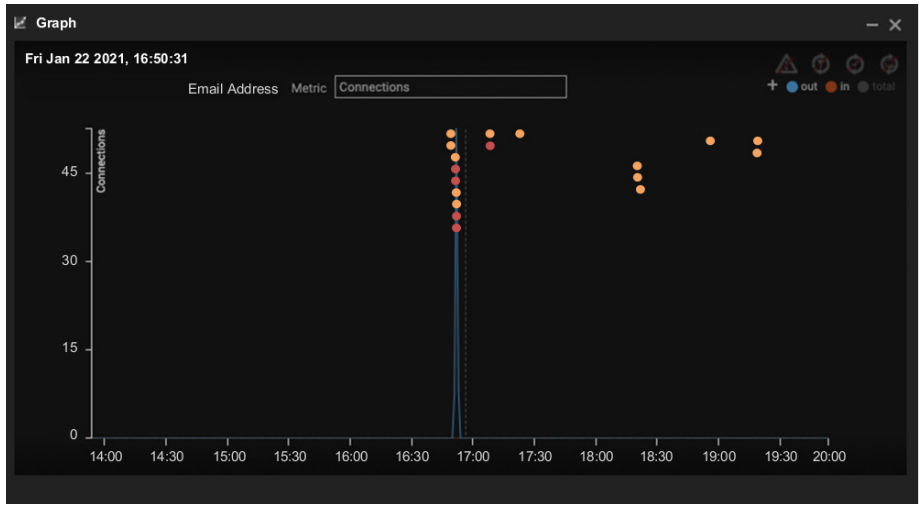


Figure 8: The connections associated with the compromise are a significant deviation from the device's normal 'pattern of life' and results in multiple unusual activity events and repeated model breaches (orange).

Disgruntled IT Administrator

When a retail organization in the UK was forced to make a series of redundancies over the course of a single week, they neglected to take a fired IT administrator's laptop or to delete their corporate account.

The former IT admin logged into one of their SaaS accounts and quickly downloaded many sensitive files – including contact details and credit card numbers from the customer database. They then attempted to secretly transfer the stolen files to a home server via one of the company's regular data transfer services.

Because Darktrace dynamically analyzes logins and file access events across SaaS services, the AI immediately picked up on on the unusually large file downloads and the exfiltration. Even though the disgruntled employee was still in the system as a legitimate administrator and used a familiar transfer service, Darktrace Cyber AI understood that the user's behavior within the SaaS platform was highly unusual and an indication of a significant threat.

Subsequent investigation revealed that the malicious admin continually sought to exfiltrate the stolen SaaS files through several other methods, including through an internal server they had used regularly at the company and, as a last-ditch attempt, through a third-party file transfer service on their endpoint device off the VPN.

While this activity from a supposedly trusted administrator easily evaded both traditional solutions and native SaaS security controls, Darktrace Cyber AI detected the threatening behavior within seconds. The system instantly alerted the security team and provided detailed and precise information about the nature of the compromise, prompting them to revoke the admin's credentials and quickly retrieve and secure the data.

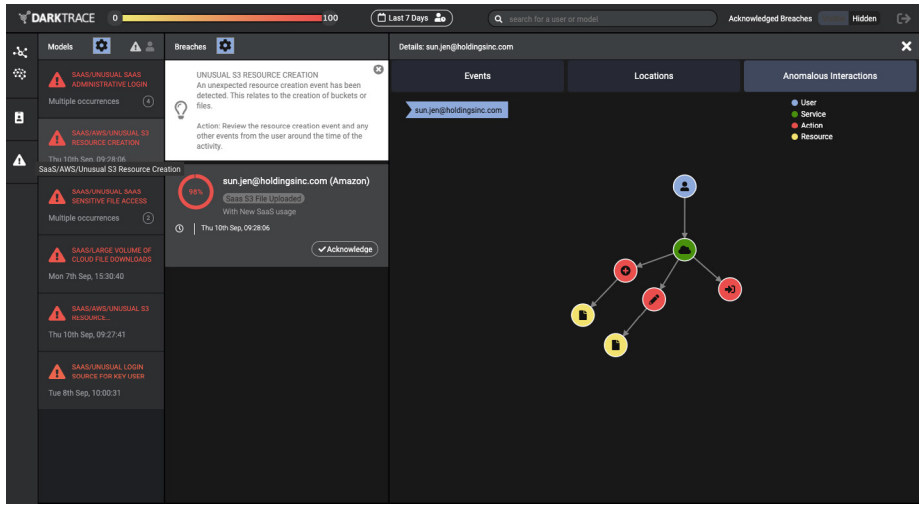


Figure 9: Darktrace's SaaS Console allows users to visualize and analyze SaaS behaviors across the workforce from one central location

> "The reality of cyber security today is that border defenses are not enough to keep fast-moving attacks out. Darktrace detects zero-day threats and suspicious insider behaviors, without having to define the activity in advance."
>
> CIO, City of Las Vegas

Stopping a Malicious Member of the IT Team

Darktrace detected and neutralized a malicious insider at a major investment firm in South Africa.

Reconnaissance activity began with a laptop scanning hundreds of internal IP addresses to identify which ones were active. It then swept the network for the names of responsive machines and scanned them for open channels of communication.

Cyber AI identified the suspicious behavior as unusual network scanning, prompting Darktrace Antigena to enforce the device's group 'pattern of life' for one hour, preventing the laptop from deviating from its prior behavior or that of its peers.

A few hours later, the threat returned. The laptop started running commands on hundreds of other internal computers in the IP range it had initially identified. This involved moving multi-purpose script files and using a remote administration tool. Based on its dynamic evaluation of the threat, Darktrace Antigena blocked all outgoing connections using the SMB file-transfer channel, instantly containing any lateral movement.

Once the threat had been neutralized, the security team was able to investigate and confirm that the laptop belonged to a member of the IT team who had been using an illegitimate scanning tool to look for vulnerabilities.

of organizations are affected by insider threats every year.

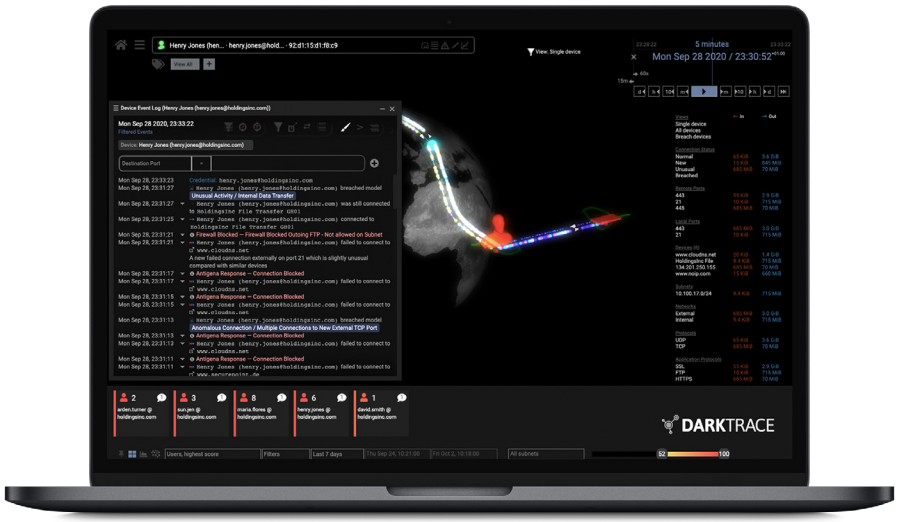


Figure 10: Darktrace Antigena responds to an emerging cyber-threat around the world every second

"The Enterprise Immune System identifies all kinds of novel threats, including polymorphic malware, stealthy insiders, and highly sophisticated social engineering attacks, without the need for rules or signatures."

IT Director and Data Protection Officer, OpinionWay

Caught in the Act

One incident occurred while Darktrace was onsite training a customer. A member of the IT team was skeptical about Darktrace's ability to detect certain activities and ended up leaving the room.

Shortly after, Darktrace detected a device that was downloading an unusual volume of data from internal servers, and the customer recognized this as sensitive information on critical projects and infrastructure.

The device belonged to the IT member who had left the room, and they were immediately called back in to explain themselves. It turned out that the employee was attempting to collect information to send to their home server.

Figure 11: Darktrace's Threat Visualizer displaying unusual connectivity on a similar device

Unauthorized Server Access via the VPN

A recently terminated employee at a US-based mining company had previously been working from home and retained unsanctioned VPN access to the company's network following their termination. With this means of entry, the former employee was able to connect to a company server and read more than 9,000 files. Darktrace's Cyber AI detected over 10,000 unauthorized SMB actions in total.

While the employee had regularly used this server as a part of their daily role at the company, Darktrace identified a surge in connectivity to the server that differed significantly from normal. The user then went on to delete at least 160 files across the products, marketing, customers, internal business, weekly reports, transportation, and systems folders.

With the power of Cyber AI, the security team could recognize that this behavior, which may have been harmless in another context, constituted a serious insider threat. Darktrace was able to supply granular data that showed exactly when and where the malicious insider accessed the server, as well as the specific files the user read and deleted, allowing the team to see the extent of the attack and jumpstart remediation.

> "Cyber-risk is one of the biggest challenges facing businesses today, and Darktrace gives us an edge against fast-moving attackers and malicious or accidental insider threat."
>
> Network and Infrastructure Lead, Waverton

Malicious Insider Harvests Data

At a large healthcare provider, two devices began exhibiting signs of highly anomalous activity. Not only was the activity unusual, but the devices themselves had never been observed across the digital ecosystem before.

Shortly after joining the network, the devices started acting like gateways. They funneled internal traffic to pre-determined destinations. The MAC addresses of these devices identified them as Raspberry Pi devices: small, inexpensive, high-performance computers the size of a credit card that are easy to smuggle into a system.

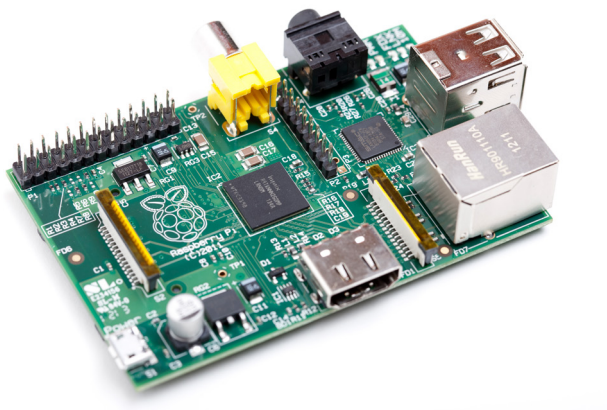


Figure 12: Raspberry Pi computer

The Raspberry Pi computers were communicating with a suspicious external website that was made to look like it belonged to the company. However, the website was hosted on an alternative server. The redirected users were being presented with a fake login page and 'security survey' where they were required to enter their usernames and passwords.

Darktrace identified the threat in real time, meaning no users fell victim to this malicious credential-grabbing attack. The Raspberry Pi devices quickly disappeared from the network.

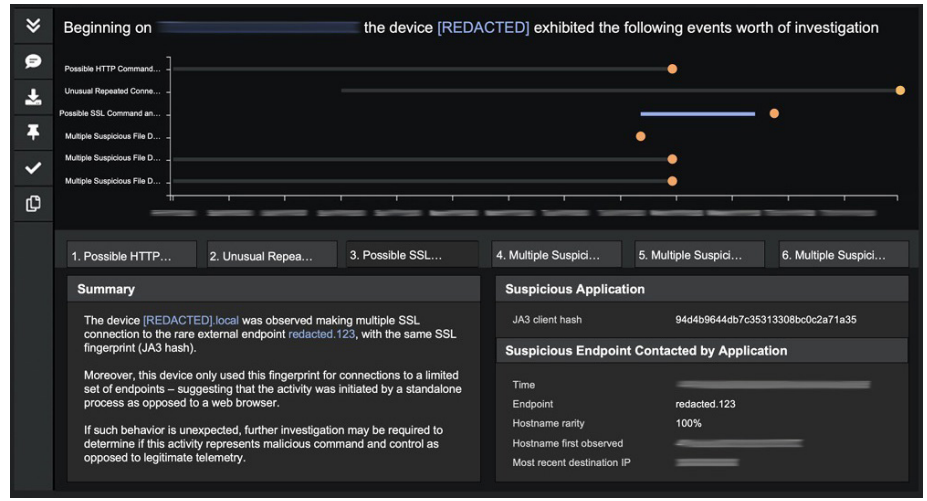


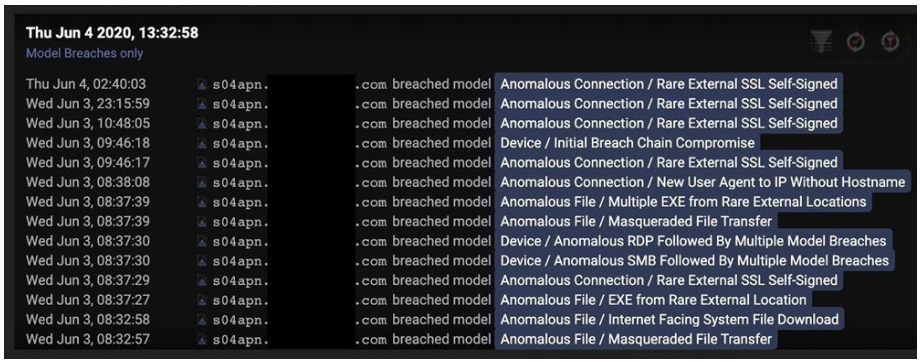
Figure 13: Cyber AI Analyst report observing C2 communications

> "Understanding the risks posed by cyber-criminals and insiders alike, we knew we needed to take a proactive and innovative approach to our cyber defense."

Information Systems Manager, University Federal Credit Union

Crypto-Mining Side Business Under The Floorboards

Bitcoin mining is very hard to detect, especially when carried out by an insider. Most miners use surplus computer capacity at night when offices are closed, but others go to more extreme lengths to slip under the radar.



Thu Jun 4 2020, 13:32:58

Model Breaches only

Thu Jun 4, 02:40:03	s04apn.	.com breached model	Anomalous Connection / Rare External SSL Self-Signed
Wed Jun 3, 23:15:59	s04apn.	.com breached model	Anomalous Connection / Rare External SSL Self-Signed
Wed Jun 3, 10:48:05	s04apn.	.com breached model	Anomalous Connection / Rare External SSL Self-Signed
Wed Jun 3, 09:46:18	s04apn.	.com breached model	Device / Initial Breach Chain Compromise
Wed Jun 3, 09:46:17	s04apn.	.com breached model	Anomalous Connection / Rare External SSL Self-Signed
Wed Jun 3, 08:38:08	s04apn.	.com breached model	Anomalous Connection / New User Agent to IP Without Hostname
Wed Jun 3, 08:37:39	s04apn.	.com breached model	Anomalous File / Multiple EXE from Rare External Locations
Wed Jun 3, 08:37:39	s04apn.	.com breached model	Anomalous File / Masqueraded File Transfer
Wed Jun 3, 08:37:30	s04apn.	.com breached model	Device / Anomalous RDP Followed By Multiple Model Breaches
Wed Jun 3, 08:37:30	s04apn.	.com breached model	Device / Anomalous SMB Followed By Multiple Model Breaches
Wed Jun 3, 08:37:29	s04apn.	.com breached model	Anomalous Connection / Rare External SSL Self-Signed
Wed Jun 3, 08:37:27	s04apn.	.com breached model	Anomalous File / EXE from Rare External Location
Wed Jun 3, 08:32:58	s04apn.	.com breached model	Anomalous File / Internet Facing System File Download
Wed Jun 3, 08:32:57	s04apn.	.com breached model	Anomalous File / Masqueraded File Transfer

Figure 14: A sample of models breached by the server at the time of this compromise

At a major Italian bank, Darktrace picked up on puzzling data traffic patterns, including servers that seemed to be connecting from a strange IP address in the company's data center. The security team insisted that the servers didn't exist on the asset log. After a lot of back and forth, they allowed Darktrace to come in and investigate.

Darktrace traced wires in the data center to 12 servers under the floorboards. It turned out that an employee was responsible for installing the servers: they had been slowly siphoning them off to set up an extensive bitcoin mining operation from within the company.

Figure 15: Cyber-attacks can originate in even the most innocuous places

About Darktrace

Darktrace is a leading autonomous cyber security 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, SaaS, traditional networks, IoT devices, endpoints, and industrial systems.

The company has over 1,500 employees and is headquartered in Cambridge, UK. Every second, Darktrace AI fights back against a cyber-threat, before it can cause damage.

Darktrace © Copyright 2021 Darktrace Holdings Limited. All rights reserved. Darktrace is a registered trademark of Darktrace Holdings Limited. Enterprise Immune System, and Threat Visualizer are unregistered trademarks of Darktrace Holdings Limited. Other trademarks included herein are the property of their respective owners.

For More Information

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