Protecting your SaaS: A Guide to Cloud Application Security

DARKTRACE

DARKTRACE

CONTENTS

SaaS: A Changed World

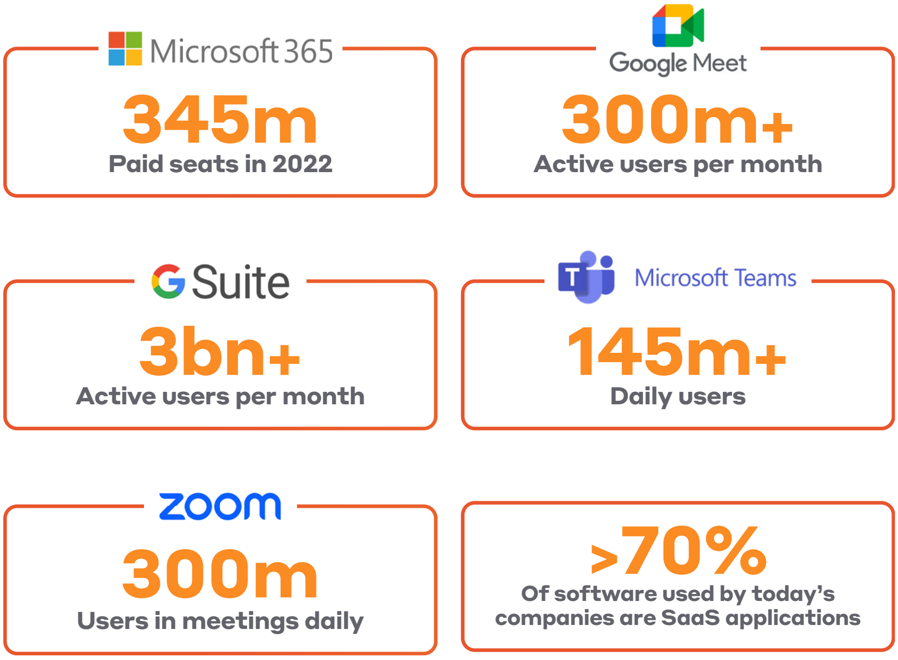
Following the mass adoption of remote and hybrid working patterns, more critical data than ever resides in cloud applications – from Salesforce and Google Workspace, to Box, Dropbox, and Microsoft 365.

While these applications fuel efficiency and innovation at scale, security teams are now tasked with defending a complex patchwork of services with native security controls that are generally reliant on historical attack data, and incompatible across platforms.

Meanwhile, the efficiencies and scalability that these applications offer also act as a pull for cyber-criminals, who can launch their attacks at blistering speed and scale up and across the organization.

As cloud applications look set to remain an integral part of the digital estate, organizations are being forced to rethink how they protect their users and data in this area.

Security leaders are turning away from tools focussed on the attack, reliant on Threat Intelligence and confined to a single area of the digital estate, and towards Self-Learning AI which understands the digital business, revealing subtle deviations that indicate a cyber-threat, and then actioning an autonomous, targeted response.



Microsoft 365
345m
Paid seats in 2022

Google Meet
300m+
Active users per month

G Suite
3bn+
Active users per month

Microsoft Teams
145m+
Daily users

zoom
300m
Users in meetings daily

>70%
Of software used by today's companies are SaaS applications

Figure 1: SaaS usage statistics in 2023 across a range of applications

The State of SaaS Security

Many organizations still rely on SaaS security tools that rely on predicting what the next attack will look like by referring to historical attack data. But with threat actors constantly innovating and updating their tools, techniques and procedures, novel and more sophisticated attacks bypass these static tools with ease.

Moreover, cloud security solutions have developed in siloes, and the complexity of managing this patchwork of disjointed technologies creates new vulnerabilities for stretched security teams. Whenever an innovative new SaaS platform begins to get adopted by business around the world, a familiar pattern can be found: a surge in micro-vendors focusing on a small set of security use cases, with no vision of the future or ability to innovate beyond features that are costly both in terms of money and time. In reality, defenders are having to protect an array of different platforms in an evolving threat landscape.

Common threat vectors that evade existing solutions include:

Account Takeover

Insider Threat

Data Exfiltration

Organizations today are looking to simplify their security stack, and this requires a broader, more holistic approach to cloud application security that protects multiple platforms with a single, proven approach to threat detection, response, prevention and recovery.

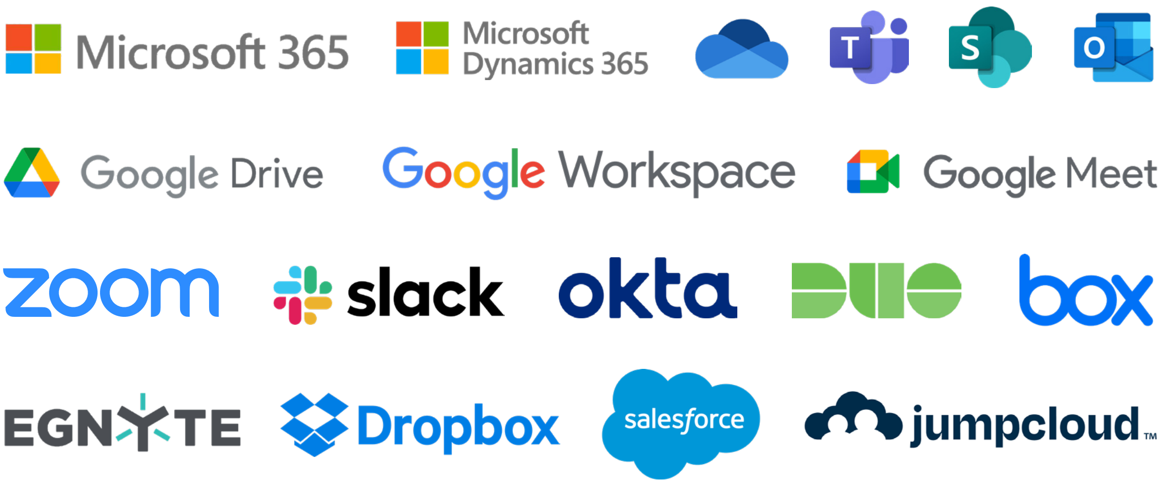
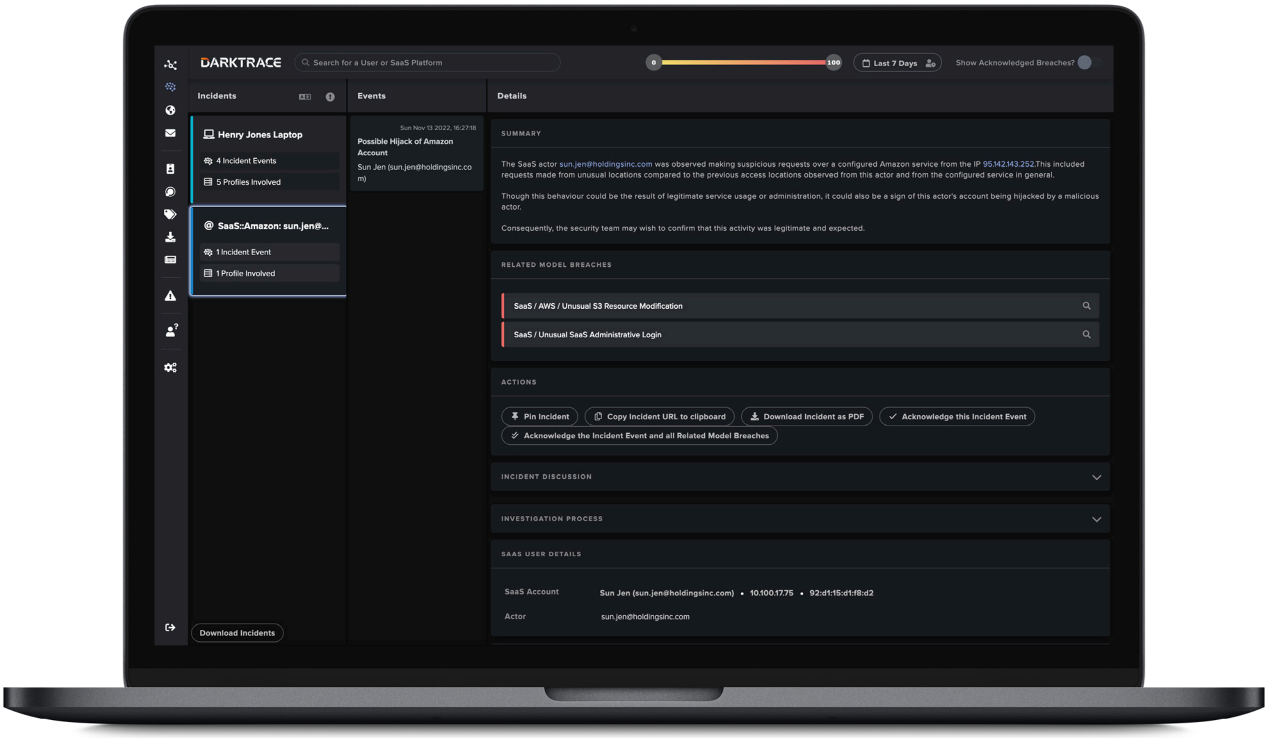


Figure 2: Companies need a security solution that encompasses the entirety of their SaaS, including platforms they might adopt in the future

DARKTRACE

Self-Learning AI in the Cloud



Sun Nov 13 2022, 16:27:18
Possible Hijack of Amazon Account
Sun Jen (sun.jen@holdingsinc.com)

The SaaS actor sun.jen@holdingsinc.com was observed making suspicious requests over a configured Amazon service from the IP 95.142.143.252.This included requests made from unusual locations compared to the previous access locations observed from this actor and from the configured service in general.

Though this behaviour could be the result of legitimate service usage or administration, it could also be a sign of this actor's account being hijacked by a malicious actor.

Consequently, the security team may wish to confirm that this activity was legitimate and expected.

SaaS / AWS / Unusual S3 Resource Modification
SaaS / Unusual SaaS Administrative Login

SaaS Account	Sun Jen (sun.jen@holdingsinc.com) • 10.100.17.75 • 92:d1:15:d1:f8:d2
Actor	sun.jen@holdingsinc.com

Figure 3: Darktrace's Threat Visualizer intuitively presents its findings

Darktrace is the first and only solution to deliver intelligent, self-learning protection that understands the full scope of your dynamic workforce in order to spot and stop threats across cloud applications.

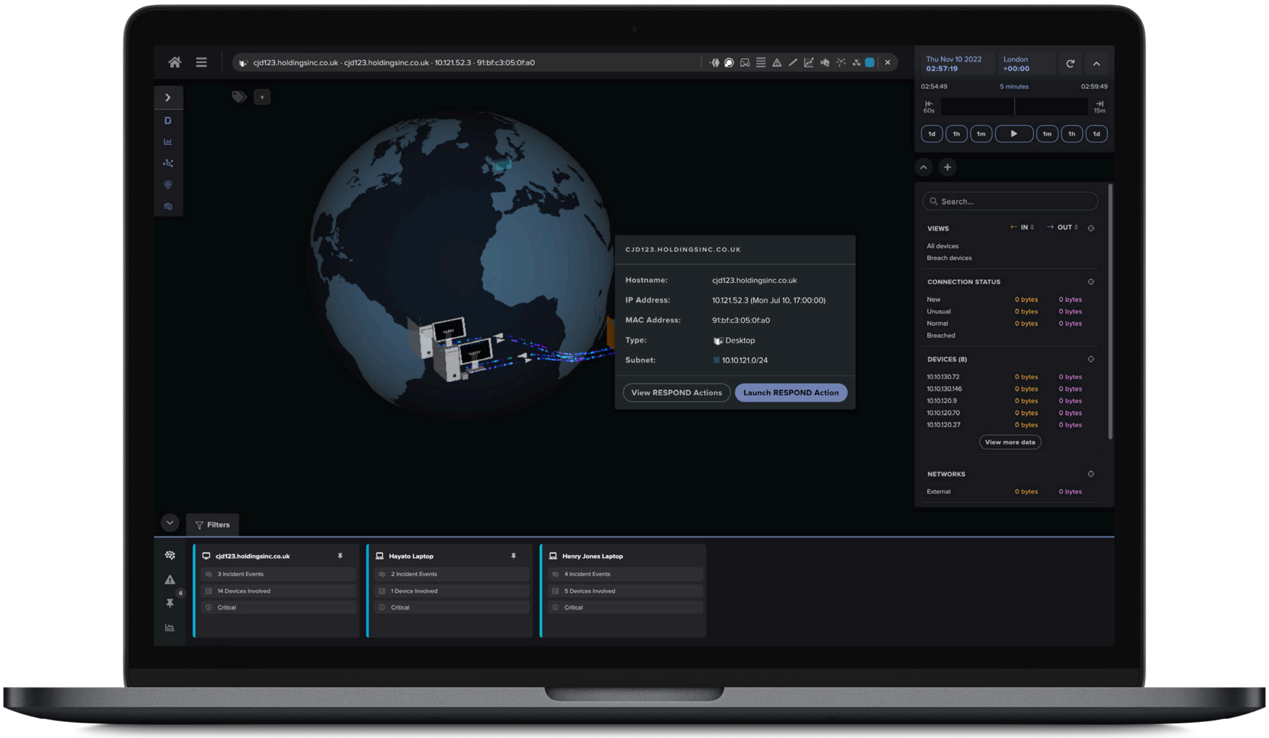
Without relying on prior assumptions or pre-defined rules, its Self-Learning AI technology continuously learns the 'patterns of life' for every user and device across the business, analyzing workforce behaviors in context and spotting subtle deviations that indicate a genuine threat. By learning a sense of 'self' for your entire workforce, the technology detects threats such as compromised SaaS credentials and malicious insiders, no matter which application is targeted.

Rather than focussing on a narrow set of use cases, the technology protects the full range of cloud platforms – including the full Microsoft 365 product suite, collaboration platforms like Slack, and file sharing applications like Dropbox. It is also uniquely able to counter threats in Salesforce.

This self-learning approach has been proven to protect over 8,800 organizations in all industries around the world, containing the most sophisticated threats in cloud applications and beyond.

> We added Darktrace to our cyber security stack and it has already paid off – we are notified within minutes when a Microsoft 365 account is breached.
>
> / Director of IT, Staffing Agency

Autonomous Response to Machine-Speed Attacks



cjd123.holdingsinc.co.uk · cjd123.holdingsinc.co.uk · 10.121.52.3 · 91:bf:c3:05:0f:a0

CJD123.HOLDINGSINC.CO.UK

Hostname: cjd123.holdingsinc.co.uk

IP Address: 10.121.52.3 (Mon Jul 10, 17:00:00)

MAC Address: 91:bf:c3:05:0f:a0

Type: Desktop

Subnet: 10.10.121.0/24

Thu Nov 10 2022 02:57:19

London +00:00

02:54:49 · 5 minutes · 02:59:49

VIEWS	← IN	→ OUT
All devices		
Breach devices		
CONNECTION STATUS		
New	0 bytes	0 bytes
Unusual	0 bytes	0 bytes
Normal	0 bytes	0 bytes
Breached		
DEVICES (8)		
10.10.130.72	0 bytes	0 bytes
10.10.130.146	0 bytes	0 bytes
10.10.120.9	0 bytes	0 bytes
10.10.120.70	0 bytes	0 bytes
10.10.120.27	0 bytes	0 bytes
NETWORKS		
External	0 bytes	0 bytes

cjd123.holdingsinc.co.uk: 3 Incident Events · 14 Devices Involved · Critical

Hayato Laptop: 2 Incident Events · 1 Device Involved · Critical

Henry Jones Laptop: 4 Incident Events · 5 Devices Involved · Critical

Figure 4: Darktrace responding to a threat, shown within the user interface

Cloud application security has historically put emphasis on detection over response, generally relying on human teams to initiate an action. Where response mechanisms are used, they usually come in the form of blunt, heavy-handed actions and pre-programmed responses, which tend to miss more sophisticated threats and can cause disruption to normal business.

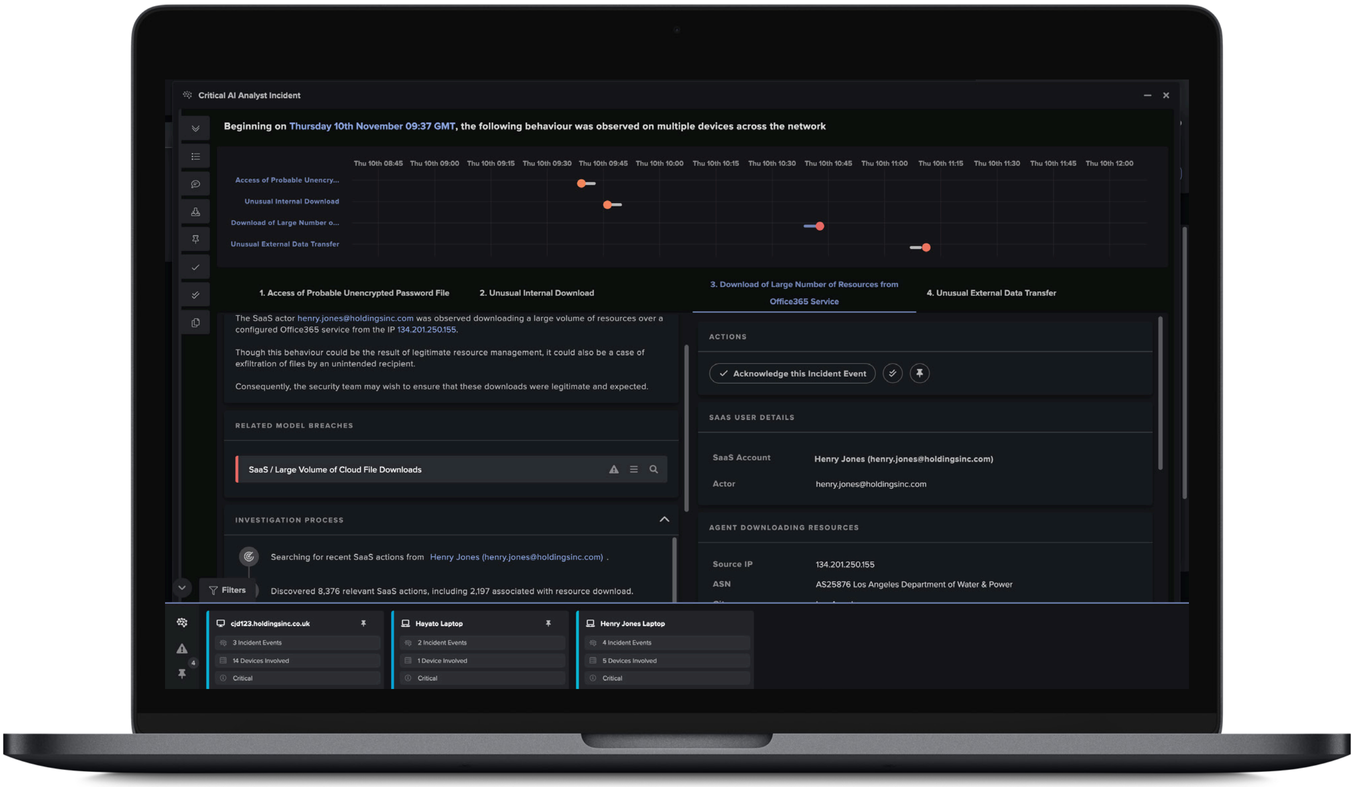
Organizations are finding that cyber-criminals are increasingly striking out-of-hours – on weekends or holidays – when they know human response time will be slower. The agility and scalability of the cloud drastically quickens the dwell time of a typical cyber-attack, and so a fast response is paramount.

Autonomous Response has changed the paradigm of cloud application security. As Self-Learning AI understands the business, Autonomous Response actions a targeted, proportionate response that sustains normal operations while interrupting the threat.

Its responses are universal, with the technology taking co-ordinated action across a user's mobile device, tablet, home laptop, and office desktop. And it reacts at machine-speed, stopping account takeovers, insider threat, and data exfiltration in seconds.

> For us, Autonomous Response technology combats the most sophisticated ransomware attacks out there and it does that within seconds of the threat emerging. This is the future of security.
>
> / CSO, Financial Services

Augmented Intelligence: Uplifting Human Teams



Critical AI Analyst Incident

Beginning on Thursday 10th November 09:37 GMT, the following behaviour was observed on multiple devices across the network

Thu 10th 08:45
Thu 10th 09:00
Thu 10th 09:15
Thu 10th 09:30
Thu 10th 09:45
Thu 10th 10:00
Thu 10th 10:15
Thu 10th 10:30
Thu 10th 10:45
Thu 10th 11:00
Thu 10th 11:15
Thu 10th 11:30
Thu 10th 11:45
Thu 10th 12:00
Access of Probable Unencry...
Unusual Internal Download
Download of Large Number o...
Unusual External Data Transfer
1. Access of Probable Unencrypted Password File
2. Unusual Internal Download
3. Download of Large Number of Resources from Office365 Service
4. Unusual External Data Transfer

The SaaS actor henry.jones@holdingsinc.com was observed downloading a large volume of resources over a configured Office365 service from the IP 134.201.250.155.

Though this behaviour could be the result of legitimate resource management, it could also be a case of exfiltration of files by an unintended recipient.

Consequently, the security team may wish to ensure that these downloads were legitimate and expected.

RELATED MODEL BREACHES

SaaS / Large Volume of Cloud File Downloads

INVESTIGATION PROCESS

Searching for recent SaaS actions from Henry Jones (henry.jones@holdingsinc.com) .

Discovered 8,376 relevant SaaS actions, including 2,197 associated with resource download.

ACTIONS

SAAS USER DETAILS

SaaS Account	Henry Jones (henry.jones@holdingsinc.com)
Actor	henry.jones@holdingsinc.com

AGENT DOWNLOADING RESOURCES

Source IP	134.201.250.155
ASN	AS25876 Los Angeles Department of Water & Power

cjd123.holdingsinc.co.uk	Hayato Laptop	Henry Jones Laptop
3 Incident Events	2 Incident Events	4 Incident Events
14 Devices Involved	1 Device Involved	5 Devices Involved
Critical	Critical	Critical

Figure 5: Cyber AI Analyst presents key information around an incident

Self-Learning AI not only reveals the subtle signs of advanced threats, but augments human teams by automating the process of threat triage, investigation, and reporting. Darktrace's Cyber AI Analyst launches an enterprise-wide investigation into every security event, connecting the dots between suspicious events in different areas of the business before settling on a high-level conclusion about the nature and root cause of the wider security incident.

Trained on an ever-growing data set of expert analyst behavior, Cyber AI Analyst automates analyst workflows at speed and scale, reporting on security incidents characterized by innovative attack techniques that would be impossible to capture with pre-defined playbooks.

Cyber AI Analyst produces a dynamic situational dashboard as well as written reports that immediately put strained security teams in a position to take action.

> The new capabilities in Cyber AI Analyst have added real value to my team, especially the ability to launch on-demand investigations and query SaaS data or suspicious devices at any time.
>
> / CISO, Data Management Services

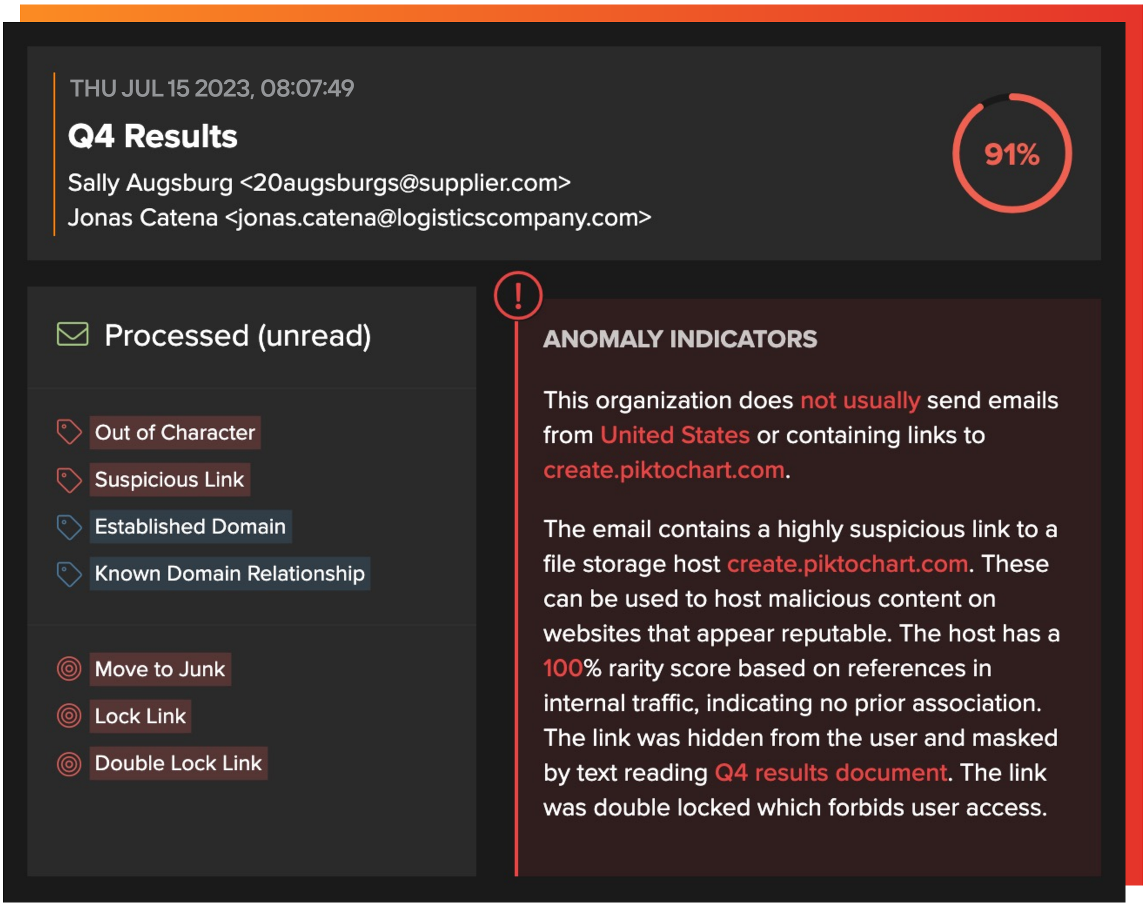
Threat Finds

/Phishing Emails Lead to Multiple Microsoft 365 Account Compromises

During a trial at a logistics company, Darktrace's AI detected a mass compromise when a phishing email led to multiple account takeovers.

The email came from a trusted source with a well-established history of correspondence. It therefore slipped under the radar of traditional tools, and the recipient was coaxed into clicking on a malicious link leading to a fake login page, where they were tricked into divulging their credentials.

Four days later, the attacker logged into the account from an unusual location, and proceeded to read files with sensitive information.



THU JUL 15 2023, 08:07:49

Q4 Results

Sally Augsburg <20augsburgs@supplier.com>
Jonas Catena <jonas.catena@logisticscompany.com>

91%

Processed (unread)

- Out of Character
- Suspicious Link
- Established Domain
- Known Domain Relationship

- Move to Junk
- Lock Link
- Double Lock Link

ANOMALY INDICATORS

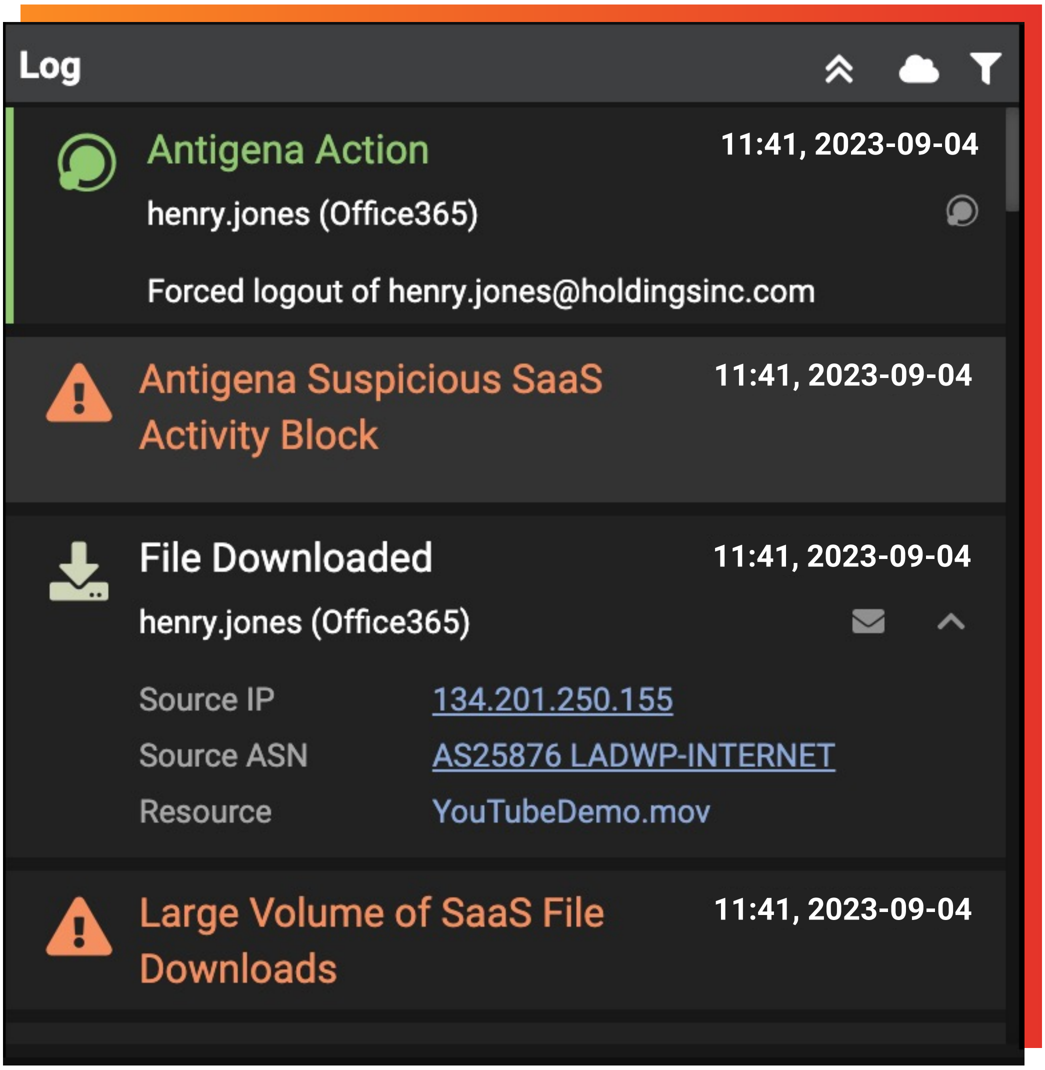
This organization does not usually send emails from United States or containing links to create.piktochart.com.

The email contains a highly suspicious link to a file storage host create.piktochart.com. These can be used to host malicious content on websites that appear reputable. The host has a 100% rarity score based on references in internal traffic, indicating no prior association. The link was hidden from the user and masked by text reading Q4 results document. The link was double locked which forbids user access.

Figure 6: Darktrace reveals the indicators of threat in plain English (data has been anonymized)

The following day, Darktrace detected a new email rule from another unusual location. Almost immediately, a large volume of outbound emails was sent from the account, all containing the same suspicious link.

After this set of outbound emails, Darktrace alerted to unusual activity from anomalous locations on other company accounts – these users had been tricked into giving away their details from the emails supposedly sent by their colleague.



Log

Antigena Action 11:41, 2023-09-04

henry.jones (Office365)

Forced logout of henry.jones@holdingsinc.com

Antigena Suspicious SaaS Activity Block 11:41, 2023-09-04

File Downloaded 11:41, 2023-09-04

henry.jones (Office365)

Source IP 134.201.250.155

Source ASN AS25876 LADWP-INTERNET

Resource YouTubeDemo.mov

Large Volume of SaaS File Downloads 11:41, 2023-09-04

Figure 7: An example of Darktrace autonomously locking a SaaS account

More sensitive customer files were read, followed by a second spike in outbound emails from these hijacked accounts. This time, the emails were sent to external contacts. In total, over 450 phishing emails were sent to a wide range of third parties. Many of these third parties in turn had their credentials compromised – repeating the cycle once again.

Darktrace surfaced multiple subtle anomalies which revealed the initial email to be suspicious, and if in active mode the Autonomous Response capability would have held the email back.

However, as this was a trial, it was set in passive mode, so the attack was allowed to unfold.

We can also see how Darktrace would have recognized the unusual SaaS activity following the account hijacks, and intervened to lock the compromised accounts.

/ Data Exfiltration from Salesforce

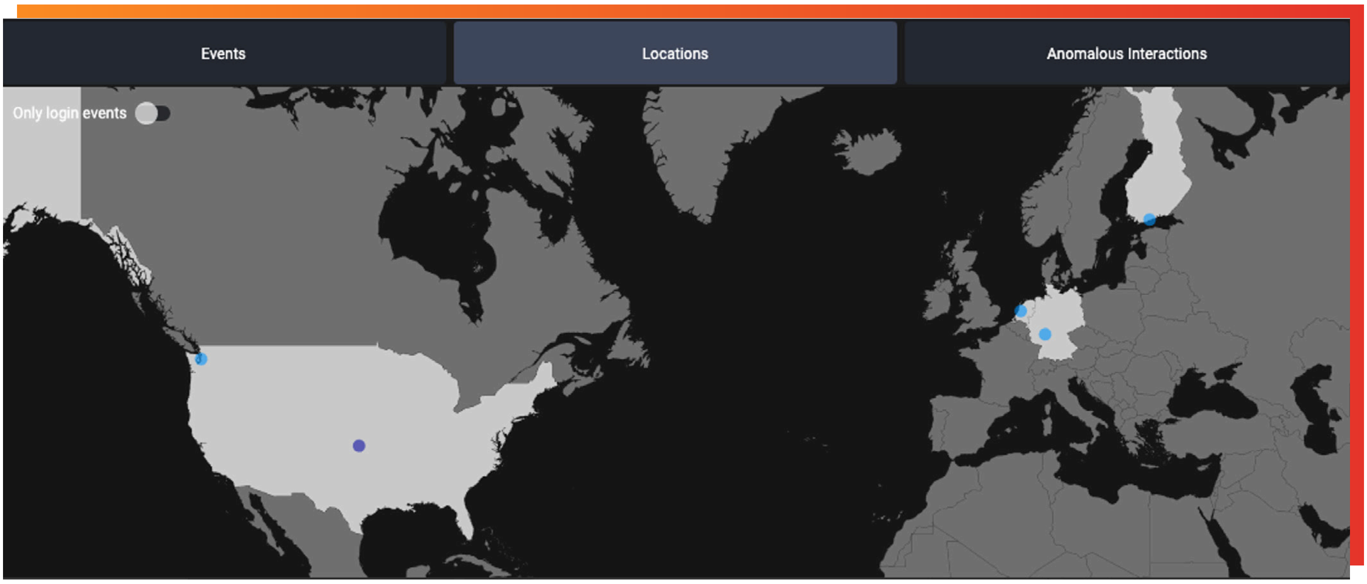
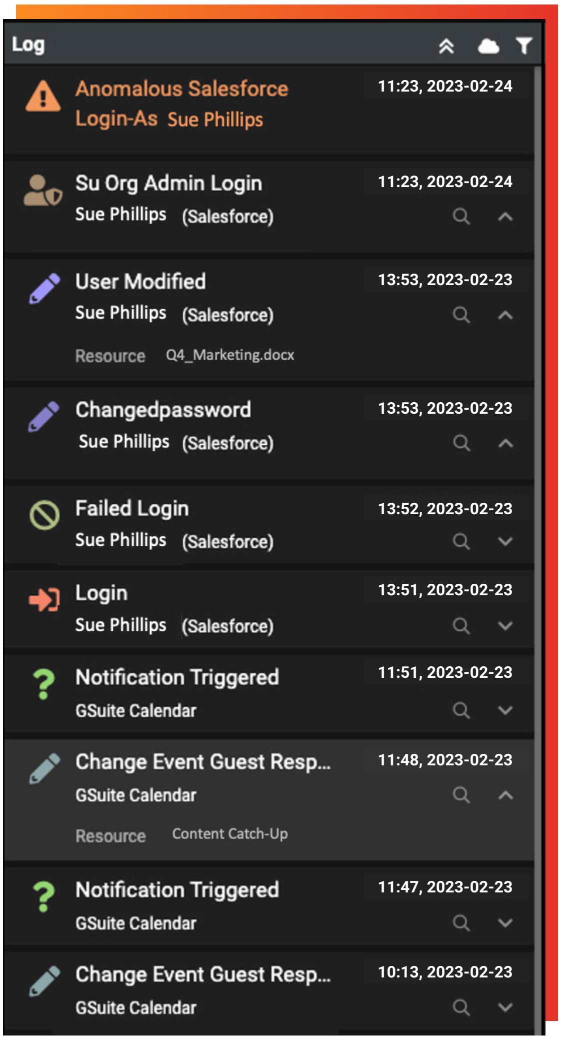


Figure 8: The geographical locations associated with the account, including the anomalous location in Finland

At a financial services organization, an employee was supposedly logged in and active on both their Salesforce and their Google Workspace account, from two separate locations, one of which was in a country not associated with the company in any way.

Darktrace picked up on further suspicious activity when a large amount of data was exported from the Salesforce account to an unusual destination, correlating multiple indicators of threat, and locking the attacker out of Salesforce, preventing the data exfiltration.



```
Anomalous Salesforce Login-As  Sue Phillips        11:23, 2023-02-24
Su Org Admin Login                                  11:23, 2023-02-24
Sue Phillips  (Salesforce)
User Modified                                       13:53, 2023-02-23
Sue Phillips  (Salesforce)
Resource   Q4_Marketing.docx
Changedpassword                                     13:53, 2023-02-23
Sue Phillips  (Salesforce)
Failed Login                                        13:52, 2023-02-23
Sue Phillips  (Salesforce)
Login                                               13:51, 2023-02-23
Sue Phillips  (Salesforce)
Notification Triggered                              11:51, 2023-02-23
GSuite Calendar
Change Event Guest Resp...                          11:48, 2023-02-23
GSuite Calendar
Resource   Content Catch-Up
Notification Triggered                              11:47, 2023-02-23
GSuite Calendar
Change Event Guest Resp...                          10:13, 2023-02-23
GSuite Calendar
```

Figure 9: Darktrace correlated activity across multiple SaaS platforms to conclude that this was highly suspicious behavior

/ Account Takeover across Office 365 and SharePoint

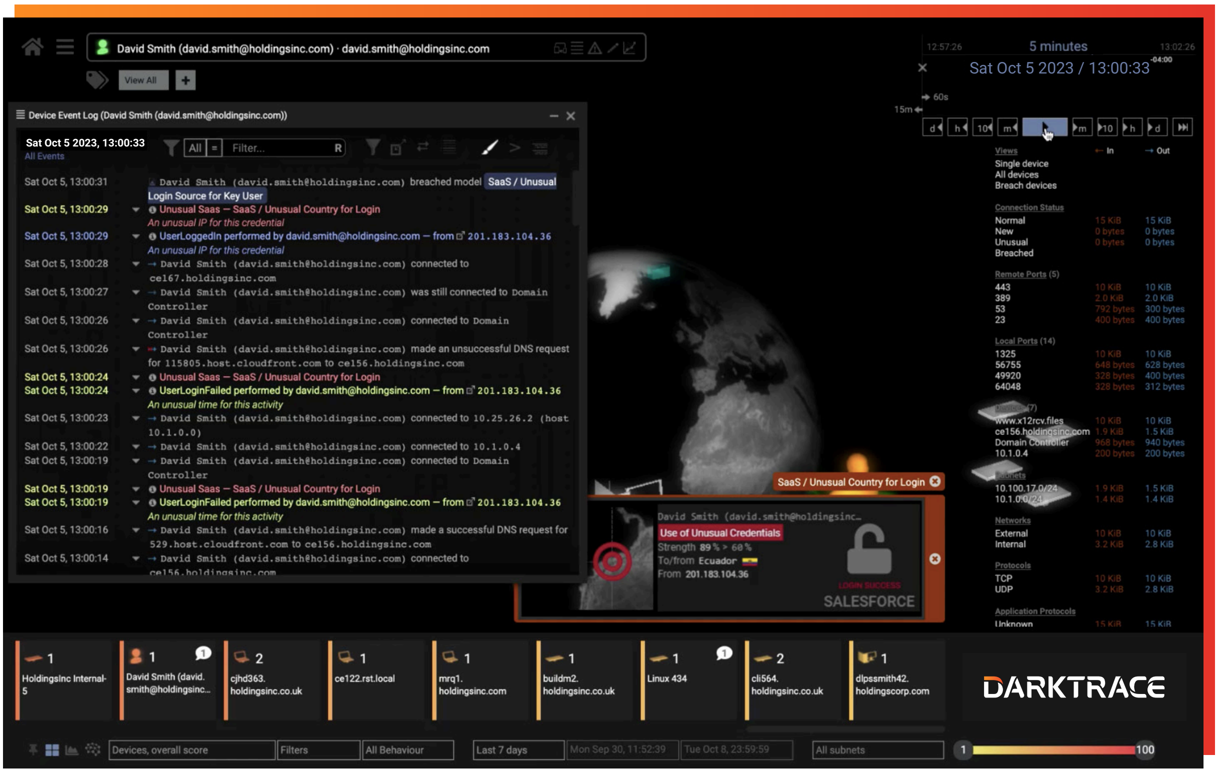
At a US-based insurance company, Darktrace's bespoke understanding of the business across multiple applications was crucial for stopping an attack that started with a compromised Microsoft 365 account.

When a threat actor successfully logged in to one of the client's Microsoft 365 accounts from an IP address located in the United Arab Emirates, Self-Learning AI identified the behavior as suspicious, as no other Microsoft 365 accounts had ever been observed logging in from this IP address.

Four days later, another rare IP located in the UAE was seen accessing the same compromised account.

This time, the threat actor set up a new email rule, and further used their illegitimate access to read and write to files on the user's personal SharePoint account.

Darktrace had not previously seen any other user accounts communicating with UAE-based IPs from the particular network identified in these incidents, indicating that the observed behavior was highly unusual for the customer and the result of compromise. Self-Learning AI stitched together these signs of anomalous behavior and locked the account, preventing the intruder from gaining further access.



David Smith (david.smith@holdingsinc.com) · david.smith@holdingsinc.com

Device Event Log (David Smith (david.smith@holdingsinc.com))

Sat Oct 5 2023, 13:00:33
All Events

```
Sat Oct 5, 13:00:31      David Smith (david.smith@holdingsinc.com) breached model SaaS / Unusual
                         Login Source for Key User
Sat Oct 5, 13:00:29      Unusual Saas — SaaS / Unusual Country for Login
                         An unusual IP for this credential
Sat Oct 5, 13:00:29      UserLoggedIn performed by david.smith@holdingsinc.com — from 201.183.104.36
                         An unusual IP for this credential
Sat Oct 5, 13:00:28      → David Smith (david.smith@holdingsinc.com) connected to
                         ce167.holdingsinc.com
Sat Oct 5, 13:00:27      → David Smith (david.smith@holdingsinc.com) was still connected to Domain
                         Controller
Sat Oct 5, 13:00:26      → David Smith (david.smith@holdingsinc.com) connected to Domain
                         Controller
Sat Oct 5, 13:00:26      → David Smith (david.smith@holdingsinc.com) made an unsuccessful DNS request
                         for 115805.host.cloudfront.com to ce156.holdingsinc.com
Sat Oct 5, 13:00:24      Unusual Saas — SaaS / Unusual Country for Login
Sat Oct 5, 13:00:24      UserLoginFailed performed by david.smith@holdingsinc.com — from 201.183.104.36
                         An unusual time for this activity
Sat Oct 5, 13:00:23      → David Smith (david.smith@holdingsinc.com) connected to 10.25.26.2 (host
                         10.1.0.0)
Sat Oct 5, 13:00:22      → David Smith (david.smith@holdingsinc.com) connected to 10.1.0.4
Sat Oct 5, 13:00:19      → David Smith (david.smith@holdingsinc.com) connected to Domain
                         Controller
Sat Oct 5, 13:00:19      Unusual Saas — SaaS / Unusual Country for Login
Sat Oct 5, 13:00:19      UserLoginFailed performed by david.smith@holdingsinc.com — from 201.183.104.36
                         An unusual time for this activity
Sat Oct 5, 13:00:16      → David Smith (david.smith@holdingsinc.com) made a successful DNS request for
                         529.host.cloudfront.com to ce156.holdingsinc.com
Sat Oct 5, 13:00:14      → David Smith (david.smith@holdingsinc.com) connected to
                         ce156.holdingsinc.com
```

SaaS / Unusual Country for Login

David Smith (david.smith@holdingsinc…
Use of Unusual Credentials
Strength 89 % > 60 %
To/from Ecuador
From 201.183.104.36
LOGIN SUCCESS
SALESFORCE

12:57:26 5 minutes 13:02:26
Sat Oct 5 2023 / 13:00:33 -04:00

```
Views                      ← In          → Out
Single device
All devices
Breach devices

Connection Status
Normal                     15 KiB        15 KiB
New                        0 bytes       0 bytes
Unusual                    0 bytes       0 bytes
Breached

Remote Ports (5)
443                        10 KiB        10 KiB
389                        2.0 KiB       2.0 KiB
53                         792 bytes     300 bytes
23                         400 bytes     400 bytes

Local Ports (14)
1325                       10 KiB        10 KiB
56755                      648 bytes     628 bytes
49920                      328 bytes     400 bytes
64048                      328 bytes     312 bytes

Devices (7)
www.x12rcv.files           10 KiB        10 KiB
ce156.holdingsinc.com      1.9 KiB       1.5 KiB
Domain Controller          968 bytes     940 bytes
10.1.0.4                   200 bytes     200 bytes

Subnets
10.100.17.0/24             1.9 KiB       1.5 KiB
10.1.0.0/24                1.4 KiB       1.4 KiB

Networks
External                   10 KiB        10 KiB
Internal                   3.2 KiB       2.8 KiB

Protocols
TCP                        10 KiB        10 KiB
UDP                        3.2 KiB       2.8 KiB

Application Protocols
Unknown                    15 KiB        15 KiB
```

Figure 10: Darktrace's AI detects the unusual SaaS login location

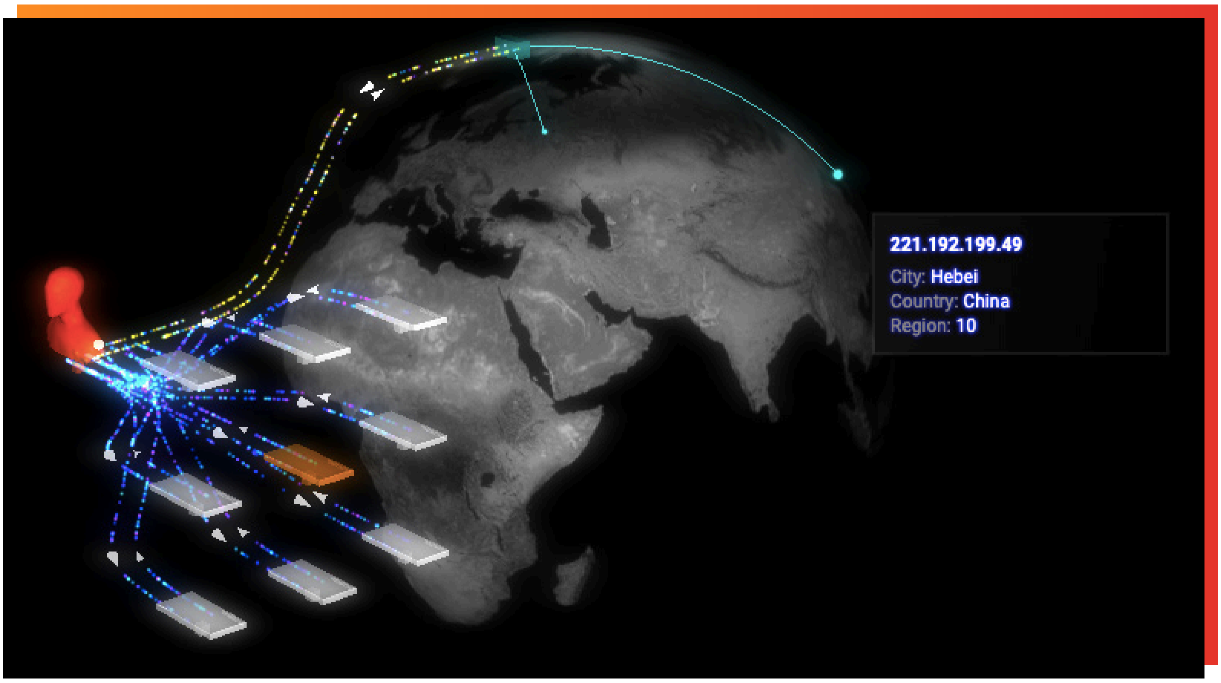
/ Malicious File Download in Box

At a global produce supplier, several suspicious requests within the company's Box platform suggested that a user account had been compromised.

The actor behind the account logged in to Box successfully, and then proceeded to download expense reports, invoices, and other financial documents. The potential threat actor also went on to unlock a file containing a list of sensitive passwords.

With Self-Learning AI's bespoke knowledge of 'self' for every member of the organization's workforce, the technology was able to identify the threat immediately. Darktrace detected that the activity occurred at a highly unusual time for the legitimate user, and that the location of the actor's IP address was also anomalous compared to the employee's previous access locations for this particular SaaS service.

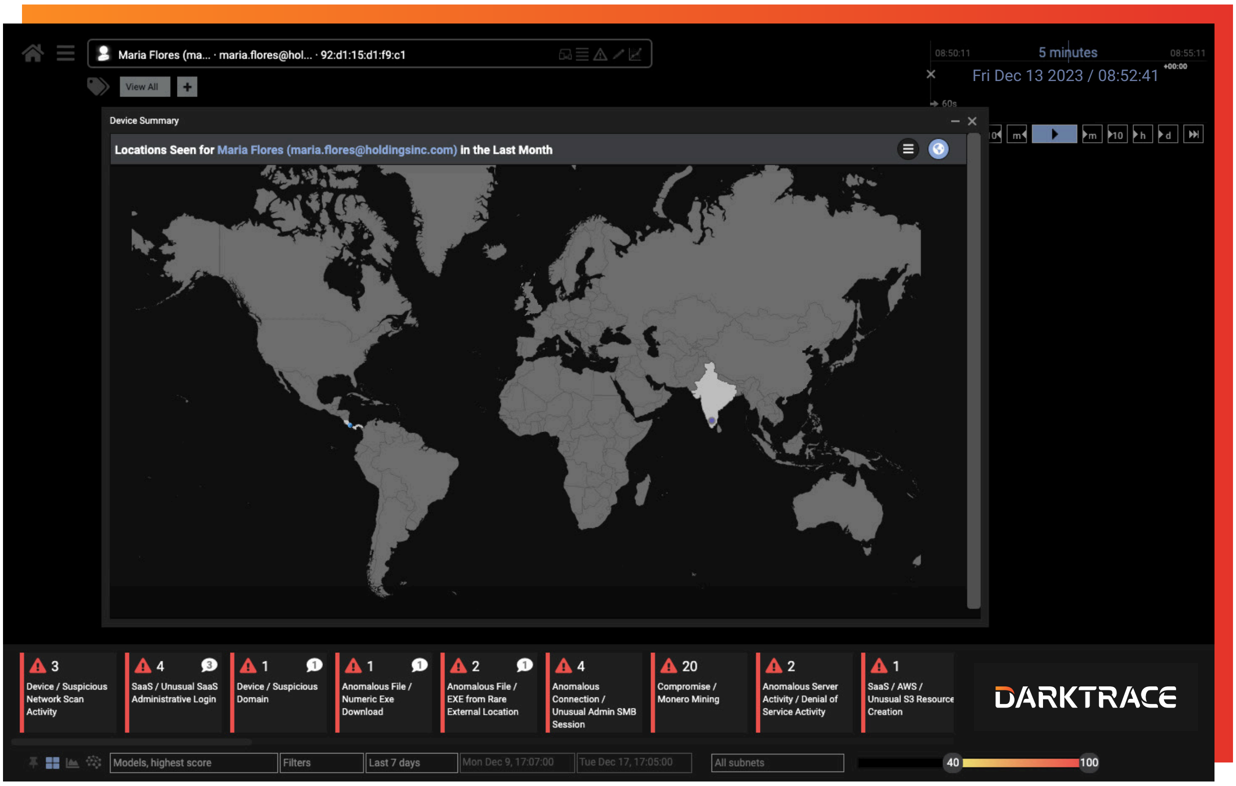
While accessing these documents may have been normal for the employee in another context, Darktrace AI's deep understanding of user behavior and granular visibility within Box allowed it to spot the subtle signs of account compromise. Moreover, when Cyber AI Analyst automatically investigated, it was able to illuminate the wider narrative, understanding that each unauthorized file exposure was part of a connected incident and highlighting the breach as a key concern for the security team.



221.192.199.49
City: Hebei
Country: China
Region: 10

Figure 11: Darktrace showing the location of the unusual IP address

/ Multiple Indicators of Attack Unveiled



Maria Flores (ma... · maria.flores@hol... · 92:d1:15:d1:f9:c1

Fri Dec 13 2023 / 08:52:41

Device Summary

Locations Seen for Maria Flores (maria.flores@holdingsinc.com) in the Last Month

Models, highest score | Filters | Last 7 days | Mon Dec 9, 17:07:00 | Tue Dec 17, 17:05:00 | All subnets

View All
+
08:50:11
5 minutes
08:55:11
+00:00
60s
3 Device / Suspicious Network Scan Activity
4 SaaS / Unusual SaaS Administrative Login
1 Device / Suspicious Domain
1 Anomalous File / Numeric Exe Download
2 Anomalous File / EXE from Rare External Location
4 Anomalous Connection / Unusual Admin SMB Session
20 Compromise / Monero Mining
2 Anomalous Server Activity / Denial of Service Activity
1 SaaS / AWS / Unusual S3 Resource Creation
DARKTRACE
40
100

Figure 12: The user interface showing login locations

One Microsoft 365 account was used in a brute force attack against a well-known bank in Panama, with logins originating from a country that deviated from the normal 'patterns of life' of the company's operations. Darktrace identified 885 logins over a period of 7 days.

While the majority of authentications originated from IP addresses in Panama, 15% of the authentications originated from an IP address that was 100% rare and located in India. A further analysis revealed that this external endpoint was included in multiple spam blacklists, and that it had recently been associated with abusive behavior online – possibly unauthorized Internet scanning or hacking.

Darktrace then witnessed what appeared to be an abuse of the password reset function, as the user in India was observed changing account privileges in a highly unusual manner.

What marked the activity as particularly suspicious was that after the password reset, failed log-in attempts from an IP normally associated with the organization were observed, suggesting the legitimate user was locked out.

> Using AI, Darktrace can detect and respond to email-borne threats and cloud-based attacks that other tools miss.
>
> / CIO, Local Government

Autonomously strengthen defenses with an end-to-end security ecosystem

Self-Learning AI empowers a complete, always-on solution with autonomous feedback continuously improving the state of security.

Comprehensive Protection Wherever You Need It

Cloud Apps Email Endpoint Network Zero Trust OT

Dropbox Google Cloud slack zscaler CROWDSTRIKE Microsoft 365 box

aws okta DUO Microsoft Azure PAS Google Workspace cisco SentinelOne salesforce

Darktrace offers an interconnected set of cyber security solutions for cloud, email, network, apps, zero trust, endpoint and OT, designed to augment humans at every stage of an incident life-cycle – from before an attack begins, to real-time detection and response to in-progress threats, through to incident management and post-incident recovery. Darktrace/ Apps is part of this security ecosystem, sharing its insights with the rest of the security stack – and human teams through Explainable AI.

/ Multi-platform coverage

A cross-platform understanding of user behavior across email, network and cloud applications allows Darktrace to reveal the full scope of an incident – with each stage of the attack presented to security teams.

Darktrace/Apps + Darktrace/Email™

Darktrace/Apps brings additional insight from inbox behavior and works with Darktrace/Email to highlight the full picture of account takeovers and other cloud-based attacks (for example how an application login from an unusual destination relates to mass outbound emails from the same user).

Darktrace/Apps + Darktrace/Network™

Working with Darktrace/Apps, Darktrace/Network also provides an important piece of the puzzle, highlighting any lateral movement between the two areas of your digital estate. Key use cases include data exfiltration and insider threat.

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. Breakthrough innovations from its R&D Centers have resulted in over 145 patent applications filed. Darktrace employs over 2,200 people around the world and protects c.8,800 organizations globally from advanced cyber-threats.

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