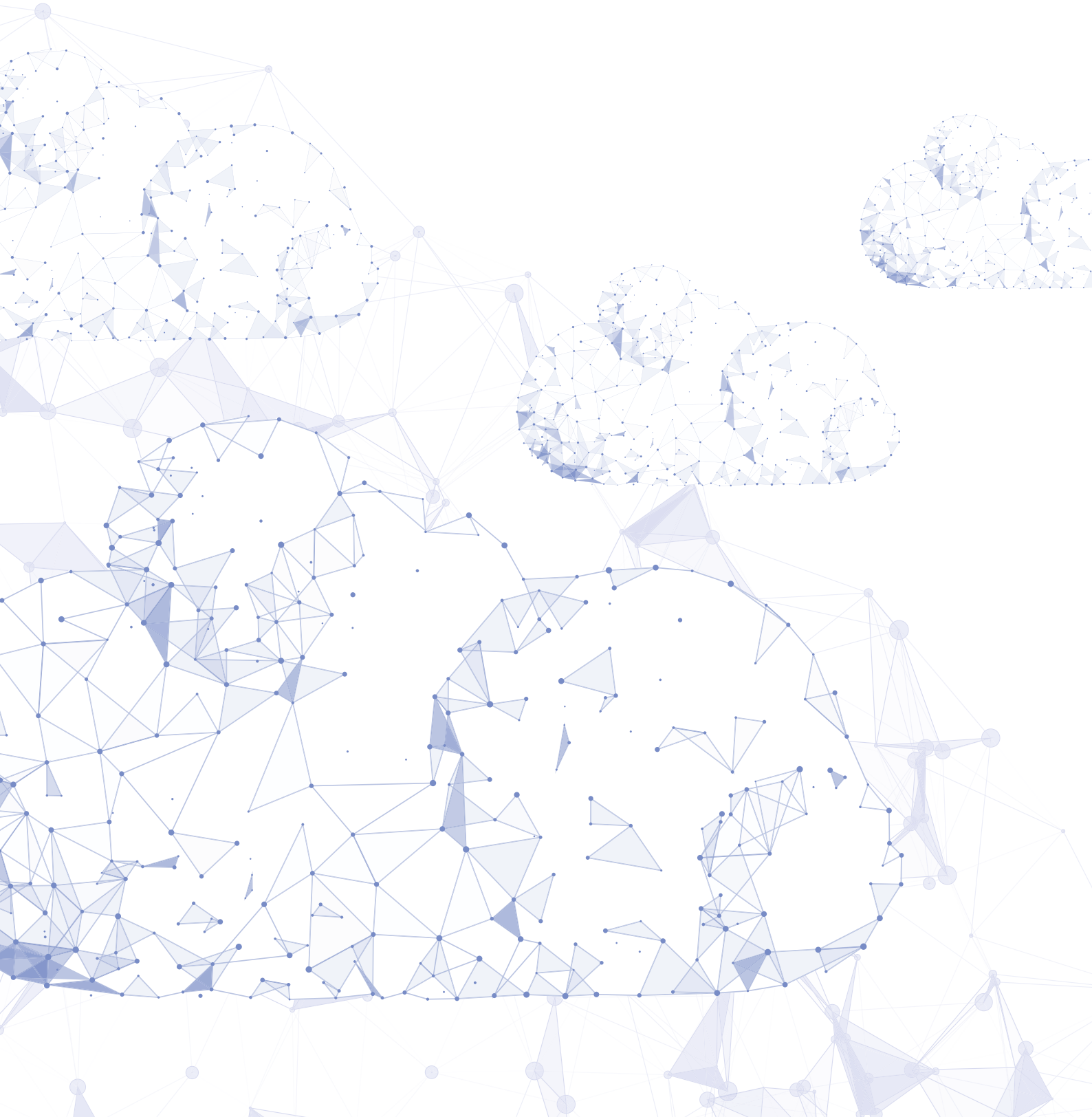
DARKTRACE

Darktrace Cyber AI

An Immune System for Cloud Security



> As organizations increase their digital capabilities across hybrid, multi-cloud, and IoT environments, they're faced with more areas to protect and control. This also means more opportunities for criminals to damage operational reliability, undertake new types of crimes, and directly affect the running of a business.
>
> **– Forrester**

Introduction

Contents

From small businesses seeking to cut costs to corporate innovation centers launching digital transformation projects, the large-scale journey to the cloud has fundamentally reshaped the digital business and the traditional paradigm of the network perimeter. As this perimeter dissolves, hybrid and multi-cloud infrastructure has become a part of the furniture of an increasingly diverse digital estate, empowering organizations to push the upper limits of innovation while expanding the attack surface at an alarming rate.

This trend of course represents the double-edged sword of the digital age, and the security challenges that business leaders must face on their journey to the cloud are difficult to overstate. The 'cloud' itself encompasses a wide range of systems and services, and a single security team can often be responsible for securing cloud workloads across AWS and Azure, email communications in Microsoft 365, customer data in Salesforce, file sharing via Dropbox, and virtualized servers in traditional on-premise data centers.

This complex patchwork of cloud-based platforms often fuels efficiency, flexibility, and innovation at the cost of a coherent and tractable security strategy. The cloud in all its various forms is unfamiliar territory for traditional security teams, and prior tools and practices are often too slow, siloed, or not even applicable to defend hybrid and multi-cloud environments against advanced attacks.

And while many cloud-native security solutions can often help with compliance and log-based analytics, they are rarely robust and unified enough to provide sufficient coverage – both because they continue to encourage a 'stove-pipe' approach to security, and because they rely on rules, signatures, or prior assumptions and therefore fail to detect novel threats and subtle insiders before they have time to escalate into a crisis.

Still worse, the lack of visibility and control that security teams face in this area – together with the new and unfamiliar mindset required by the agility and speed of the cloud – also renders it an attractive target for cyber-criminals, who invariably seek to generate maximum profits while avoiding detection. Cloud security is not where it needs it be, and cyber-criminals know this better than anyone.

Yet in many ways, organizations today need more than just cloud security – they need enterprise-wide security, and a unified platform that can operate at the speed of digital business, adapt to future threats, and correlate the subtle hallmarks of an advanced attack as it broadens its presence within a network.

The Cyber AI Platform

Limitations of the Siloed Approach to Cloud Security

Cloud Service Providers and third-party vendors offer a range of 'cloud-native' security solutions that help customers defend their portion of the Shared Responsibility Model. However, these point solutions – whether native or third-party – are generally ill-equipped to detect and respond to advanced threats in the cloud.

Native Controls: Necessary, but Not Sufficient

Native security controls are often exclusively designed for a single cloud provider, covering only one portion of a vast hybrid and multi-cloud enterprise. This drastically limits the scope of detection and adds complexity to an already complex security stack.

In general, native controls can help with compliance, log collection, and static policy creation, but they are not designed for advanced threat detection and response across multiple cloud services and siloes.

Third-Party Controls: Helpful, but Not Sufficient

Third-party controls such as CASBs and CWPPs are also helpful, but not sufficient. CASBs, for example, can help with discovery, granular policy creation, and compliance, but they often fail to detect cyber-threats that occupy the more advanced end of the spectrum - from compromised credentials and ransomware, through to disgruntled insiders and corporate espionage.

While third-party controls typically provide cross-cloud visibility, they do not have any insight into an organization's physical network. This is a significant limitation – correlating insights across the cloud and corporate network is often the only way a security system can illuminate the presence of an emerging threat.

An Immune System for the Cloud and Beyond

Powered by artificial intelligence, Darktrace's Cyber AI Platform fills these critical gaps with a unique enterprise-wide approach that detects and responds to cloud-based threats that other tools miss.

Like the human immune system, the technology develops an innate sense of 'self', learning the normal 'pattern of life' for every user, device, and container across hybrid and multi-cloud environments. By continuously analyzing the behavior of everyone and everything in the business, Darktrace's self-learning AI can uniquely correlate the weak and subtle signals of an advanced attack, without defining 'benign' or 'malicious' in advance.

While pre-programmed point solutions can certainly complement this approach, Darktrace is the only proven technology to stop the full range of cyber-threats in the cloud, from malicious insiders and external attacks, through to critical misconfigurations that can expose the business to future compromise – whether they originate from targeted spear phishing campaigns, corporate account takeovers, 'low and slow' data exfiltration, or lateral movement across the cloud.

Unified and Bespoke Protection

With an enterprise-wide understanding of the digital estate, Darktrace correlates all on-prem activity with traffic across hybrid and multi-cloud environments in real time. This enables it to understand that an unremarkable behavior seen in isolation in the cloud may point to a greater picture of malicious activity.

For example, we might see that a user has logged into AWS in the cloud. This is not malicious per se, but Darktrace also knows that the same user's Microsoft 365 account was likely compromised moments prior, as a highly unusual login location was detected. Darktrace understands that the connection to AWS is in fact highly suspicious.

> Security leaders increasingly envisage improving their efficiency by collapsing point products into broader security platforms.
>
> **– Gartner**

Correlating Insights at Container Level

Despite the increasing adoption of containers by developers, security has often lagged behind. The virtualized nature of containers makes intra-server traffic difficult to monitor. Whereas rules-based systems track data across servers only, Darktrace is able to provide visibility into the containerized environments within individual servers.

Crucially, Darktrace extends this container visibility and connects it to activity across the entire digital infrastructure (cloud, IoT, email, industrial and all other environments). An anomaly in one container's network traffic could therefore be linked to a cloud database which itself could be correlated with an enterprise's email account.

See page 14 for deployment scenarios

Cyber AI Analyst: Autonomous Triage

Cyber AI Analyst takes the additional step of automatically investigating threats detected by the Enterprise Immune System and producing a dynamic situational dashboard as well as AI-generated reports that communicate the full scope of a security incident.

By correlating real-time cloud traffic with the rest of the network, the AI Analyst can conduct hundreds of investigations simultaneously, stitching together a constellation of alerts and indicators and developing a meaningful understanding of incidents at machine speed. It then communicates its results and recommendations in the form of AI Analyst Incidents, which are enriched with context and security insights that can be reviewed and actioned by executives and end-users alike.

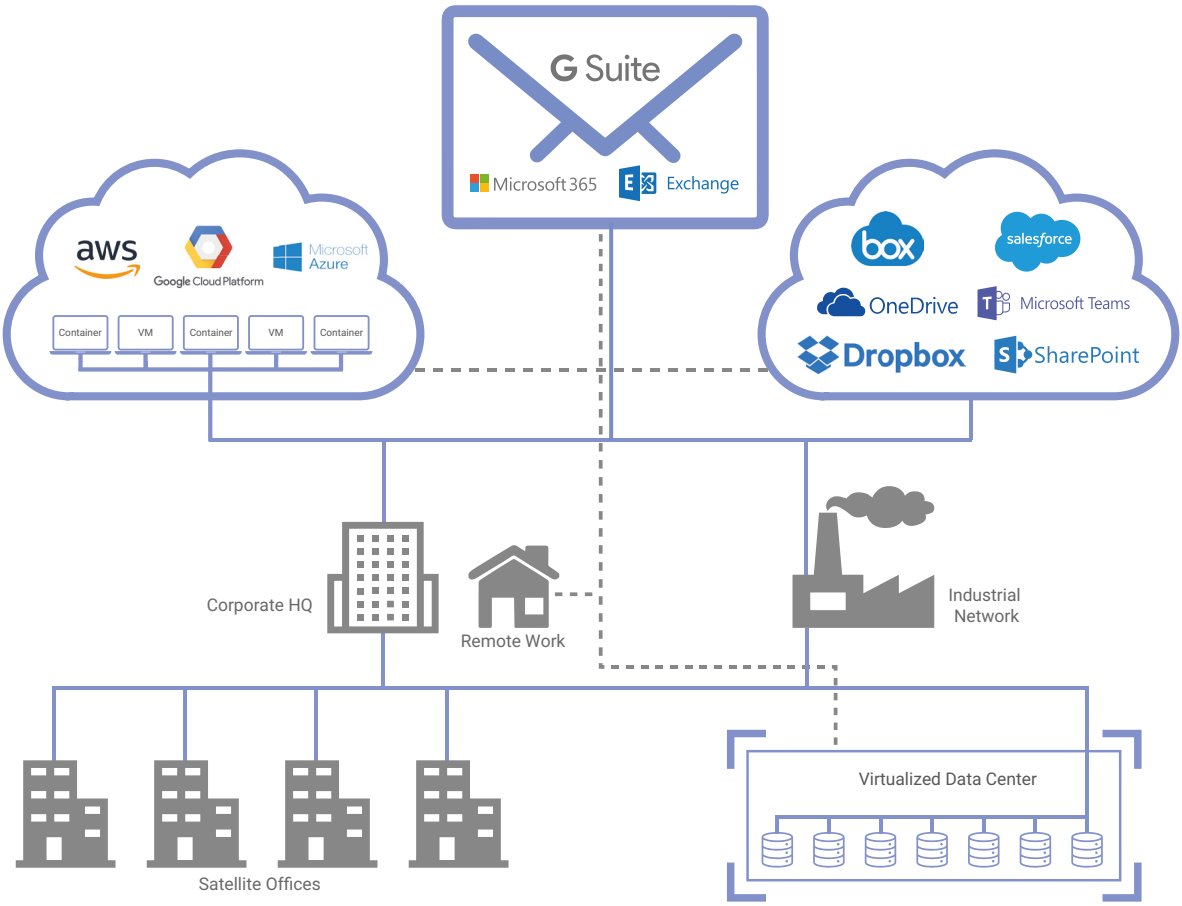


Figure 1: Darktrace's unified coverage of the entire digital estate

Compromised Credentials

29% of data breaches involve the use of stolen credentials

Source: Verizon 2019

Advanced cyber-criminals can steal corporate account credentials in a variety of ways, from social engineering attacks to 'smart' malware that combs through traffic and ephemeral cloud assets in search of passwords. And with stolen data readily available to buy and sell on the Dark Web, the frequency and severity of credential theft is increasing year on year.

Cases of account takeover encompass just the first stage of a cyber-threat. The endgame of a credential-based attack is the actual use of compromised passwords to authenticate applications and steal data. Once an attacker has the credentials to operate like a valid user, little can be done to distinguish an intruder from the legitimate employee they are impersonating.

By correlating data across hybrid and multi-cloud environments, Darktrace learns each user's 'pattern of life' from hundreds of metrics, allowing it to immediately detect deviations in behavior that are indicative of an account takeover. Even in cases of a pre-existing compromise, by learning the 'pattern of life' of that user's peer group, as well as the wider business, Darktrace's AI will retrospectively flag any unusual behavior.

Figure 2: Darktrace's AI detects unusual activity relating to a compromised cloud account

SharePoint Attack

After obtaining stolen credentials or otherwise gaining access to an organization's cloud-based file transfer service, cyber-criminals will frequently run scripts to identify files containing keywords like 'password'. Darktrace discovered one such incident at a European bank, where attackers managed to find an Microsoft 365 SharePoint file that stored unencrypted passwords. Having already bypassed Microsoft's native controls, the attackers could have reasonably expected to be in the clear.

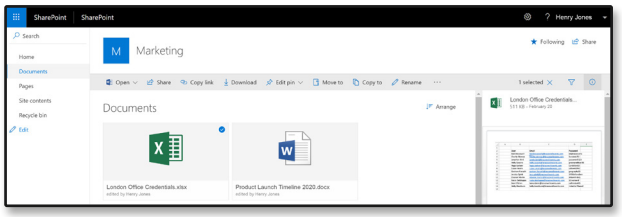


Figure 3: The sensitive files accessed on SharePoint

However, Darktrace's AI flagged the activity as anomalous for the corporate user, his peer group, and the wider organization, detecting the unusual access to these sensitive files among other indicators. Ultimately, the AI's nuanced and evolving understanding of 'normal' across the entire organization proved critical, given that the suspicious file access may well have been benign in other circumstances.

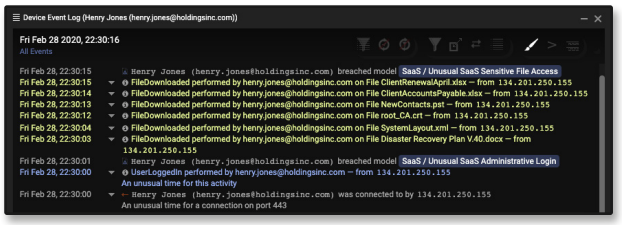


Figure 4: Darktrace surfaces the sensitive file downloads

These attackers would likely have leveraged the cleartext passwords to escalate their privileges and further infiltrate the organization. Yet by learning unique 'patterns of life' for every user and device in the organization, Darktrace's AI was able to alert the security team to the incident before it could escalate into a crisis.

Attack Evades 'Impossible Travel' Rule in M365

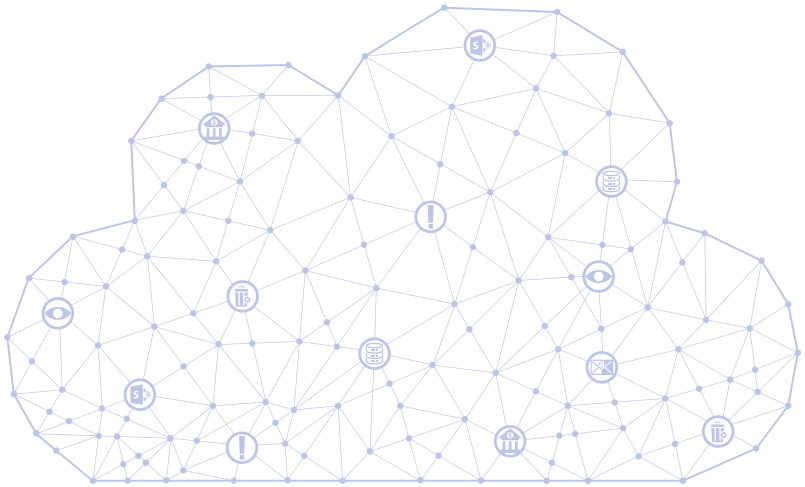
In one international non-profit, Darktrace detected an account takeover in Microsoft 365 that bypassed Azure AD's static 'impossible travel' rule. While the organization had offices in every corner of the globe, Darktrace's self-learning AI identified a login from an IP address that was historically unusual for that user and her peer group and immediately alerted the security team.

Darktrace then alerted to the fact that a new email processing rule, which deletes inbound and outbound emails, had been set up on the account. This indicated a clear sign of compromise and the security team was able to lock the account before the attacker could do damage.

With this new email processing rule in place, the attacker could have initiated numerous exchanges with other employees in the business, without the legitimate user ever knowing. This is a common strategy used by cyber-criminals seeking to gain persistent access and leverage multiple footholds within an organization, potentially in preparation for a large-scale attack.

Analyzing the rare IP address in conjunction with the out-of-character behavior of the apparent user, Darktrace confidently identified this as a case of account takeover, preventing serious damage to the business.

> **Darktrace detected an account takeover in Microsoft 365 that bypassed Azure AD's static 'impossible travel' rule.**



Unusual Login at Panamanian Bank

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.

Figure 5: The user interface showing login locations

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 login attempts from an IP normally associated with the organization were observed, suggesting the legitimate user was locked out.

03/12 20:45:39	Saas::Admin	Regular	UpdateUser
03/12 20:45:39	Saas::Admin	Regular	ChangeUserLicense
03/12 20:26:43	Saas::Login	Regular	UserLoggedIn
03/12 20:26:43	Saas::FailedLogin	Regular	UserLoginFailed
03/12 20:26:36	Saas::FailedLogin	Regular	UserLoginFailed
03/12 18:31:31	Saas::Login	Regular	UserLoggedIn
03/12 17:57:46	Saas::Admin	Regular	ChangeUserLicense
03/12 17:57:46	Saas::Admin	Regular	UpdateUser
03/12 17:06:57	Saas::Admin	Regular	UpdateUser

Figure 6: The activity associated with the SaaS account, highlighting the changed credentials

Automated Brute Force Attack

Darktrace detected several failed login events on a SaaS account every day over the course of a week. Each batch of login attempts was performed at precisely 6.04pm on six days. The consistency in both the time of day and the number of login attempts was indicative of an automated brute force attack, which is programmed to discontinue after a certain number of failed attempts in order to avoid lockouts.

Darktrace considered this pattern of failed attempts highly anomalous and so alerted the security team. Were it not for Darktrace correlating multiple weak indicators and fleshing out the subtle signs of emerging threat, this automated attack could have continued for weeks or months, making educated guesses at the users' password based on other information it had already gathered.

Figure 7: A graph illustrating the repeated login attempts

Compromise Across Microsoft 365 and Teams

A Microsoft 365 account was recently compromised at a public accounting firm based in the United States. Darktrace initially picked up on several anomalies, including a sudden surge in outbound email traffic as well as the unusual login location – while the company and nearly all of its users were located in Wisconsin, an IP address located in Kansas was used to log in to the Microsoft 365 account. Along with the unusual login, a login to Microsoft Teams from the same Kansas IP address was detected.

Figure 8: Just after the new email rule was created, a Microsoft Teams 100% rare IP login occurred

'Impossible travel' rules alone would have missed these anomalies, but an understanding of activity and behavior across different SaaS applications allowed Darktrace's AI to recognize these events as one systematic case of credential theft. When the threat actor subsequently created a new email rule, Darktrace was able to connect this event with the other anomalous behavior and understand its potentially malicious nature.

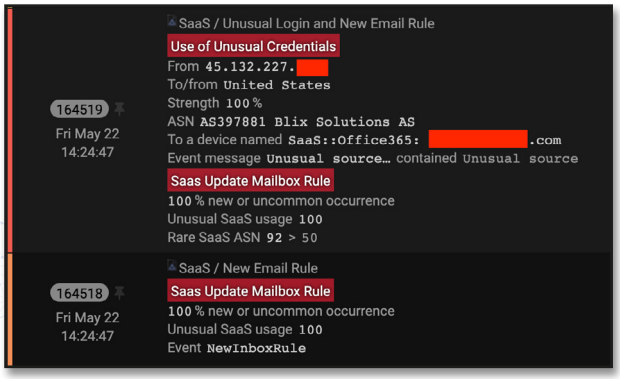


Figure 9: Darktrace's SaaS Module noted a 100% rare IP logging into the user's Microsoft 365 account and the creation of a new mailbox rules. All factors indicated 100% unusual SaaS activity

Five minutes later, Antigena Email alerted on a large number of outbound emails containing a generic subject line and an attached PDF. The technology also detected that there was a clear spike in outbound emails from this user and flagged each of these emails with the "Out of Character" tag, which in this case denoted a change from normal behavior with the surge in recipients, and likely internal compromise.

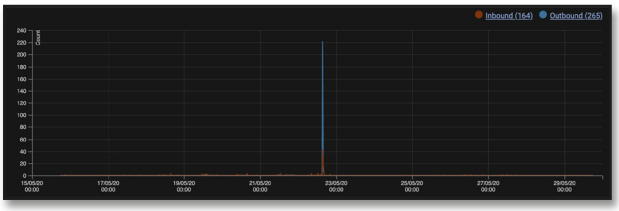


Figure 10: Antigena Email detected a surge in recipients that indicated a serious breach of normal behavior for this user

The unusual login behavior detected by Darktrace's SaaS Module could be connected to the anomalous outbound email behavior flagged by Antigena Email, allowing the security team to see the extent of the attack and neutralize it as it emerged. It was clear that the account was being used to engage in malicious activity, as each of the 220 outbound emails used a generic subject line and contained a suspicious attachment. The security team therefore immediately disabled the compromised account.

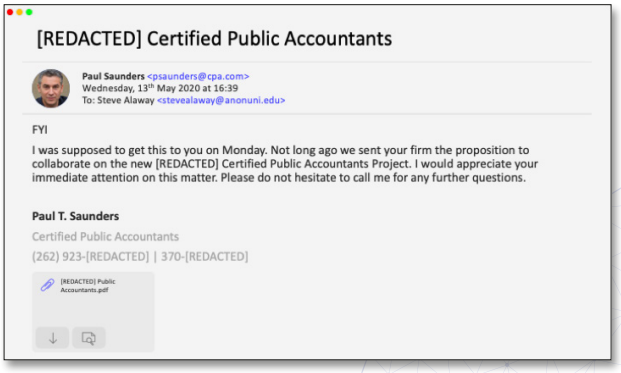


Figure 11: A recreation of the email sent by the attacker, containing the malicious attachment

Malicious Insiders

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

Insider threats in the cloud often pose more of a cyber-threat to organizations than external attackers, for the obvious reason—they're already inside. An employee with nefarious intentions is uniquely positioned to evade traditional tools given their privileged access and intimate knowledge of the network.

Cloud services have vastly expanded the scope of insider threat, with the sheer number of applications presenting a broad range of vectors for data exfiltration, and the limited visibility in this realm allowing data exfiltration to go under the radar.

By nature, legacy security tools are blind to malicious activity already occurring within the organization. Cloud security now requires a more comprehensive approach that analyzes traffic across the entire digital estate and continuously builds an evolving 'pattern of life' for the organization.

Whether it's a salesperson jumping ship and bringing customer information with them, or a disgruntled IT administrator subtly manipulating critical data, artificial intelligence can be used to detect any anomalous and unusual activity indicative of a cyber-threat.

Figure 12: Darktrace Antigena blocks a malicious insider's attempt to exfiltrate sensitive data

Disgruntled IT Employee

Darktrace witnessed a case of insider threat after an employee was fired from their position as an IT System Administrator. The organization had been forced to make a series of redundancies in the office that week, but had neglected to take the employee's laptop or delete their corporate account. The former IT admin logged into their SaaS account and quickly downloaded many sensitive files – including contact details and credit card numbers – from the customer database.

Figure 13: The Threat Visualizer showing a large spike in the number of connections

They then attempted to secretly transfer these files to a home server via one of the company's regular data transfer services. Before doing so, they created a new 'dark account' to create a backdoor, ensuring that they could still have a foothold in the company when the IT team eventually got around to shutting down their corporate account.

The IT Administrator knew that this particular service was not only sanctioned by corporate policies but also cloud-based, and he assumed that the security team would have limited visibility in this area. However, Darktrace dynamically analyzes logins and file access events in corporate cloud services, correlating them with learned 'patterns of life' for every user in the organization in light of new evidence. As a unified self-learning system, Darktrace's Cyber AI Platform immediately picked up on the unusually large file downloads, the new account creation, and the exfiltration, and its Autonomous Response technology Antigena kicked in to block the attempted upload.

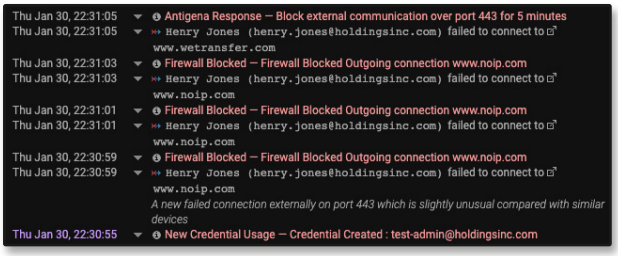


Figure 14: Darktrace Antigena actioning a targeted autonomous response

Subsequent investigation revealed that the employee first tried to send these files to a personal server at home. When this failed, they continually sought to exfiltrate the data to several other sources. However, because Antigena can dynamically adapt to threats as they unfold, and escalate its response in kind, it was able to surgically interrupt these attempts at every turn.

When all else failed, the employee then tried to transfer all the files to an internal server he used to use at the company – attempting to send the files out from there – but Darktrace stepped in and neutralized that connection as well.

Figure 15: Antigena blocks the employees attempt to transfer files via the cloud

While this subtle activity easily evaded the cloud provider's native controls, Darktrace's AI detected the threatening behavior within seconds. By continuously learning 'normal' for every user and device, the system was able to intelligently correlate highly suspicious connections and downloads from the IT Administrator's device, even though the cloud service was regularly used for legitimate purposes by other employees.

Darktrace's AI Platform instantly alerted the security team and provided detailed and precise information about the nature of the compromise, prompting them to revoke his credentials and quickly retrieve and secure the data.

Misconfiguration

> Nearly all successful attacks on cloud services are the result of customer misconfiguration.
>
> **– Neil MacDonald, Gartner**

Configuring security controls in hybrid and multi-cloud environments is often a complex process, as native and third-party solutions in this area are diverse, incompatible, and insufficient. A lack of familiarity with the cloud often leads to critical misconfigurations that expose the business to attack. Modern developers now have the ability to spin up a cloud instance in minutes, often without having to consult their firm's security team. As a consequence, the majority of organizations lack visibility over their own cloud environments, and hurried installments can result in gaping vulnerabilities that go unnoticed for months.

The potential ramifications of a misconfiguration surfaced with the Capital One data breach, which affected more than 100 million people by exploiting a vulnerability in the cloud. This major financial institution with a mature cloud security posture was made aware only after receiving a tip from an outsider who had stumbled upon the stolen data – three months after the breach had occurred.

Artificial intelligence is now used to understand the normal 'patterns of life' for every user, device and container, recognizing the subtle behavioral patterns associated with a misconfiguration. By employing self-learning technology like Darktrace's Cyber AI Platform, organizations can gain the necessary knowledge of complex cloud environments to catch latent vulnerabilities in their nascent stages — before they escalate into crises.

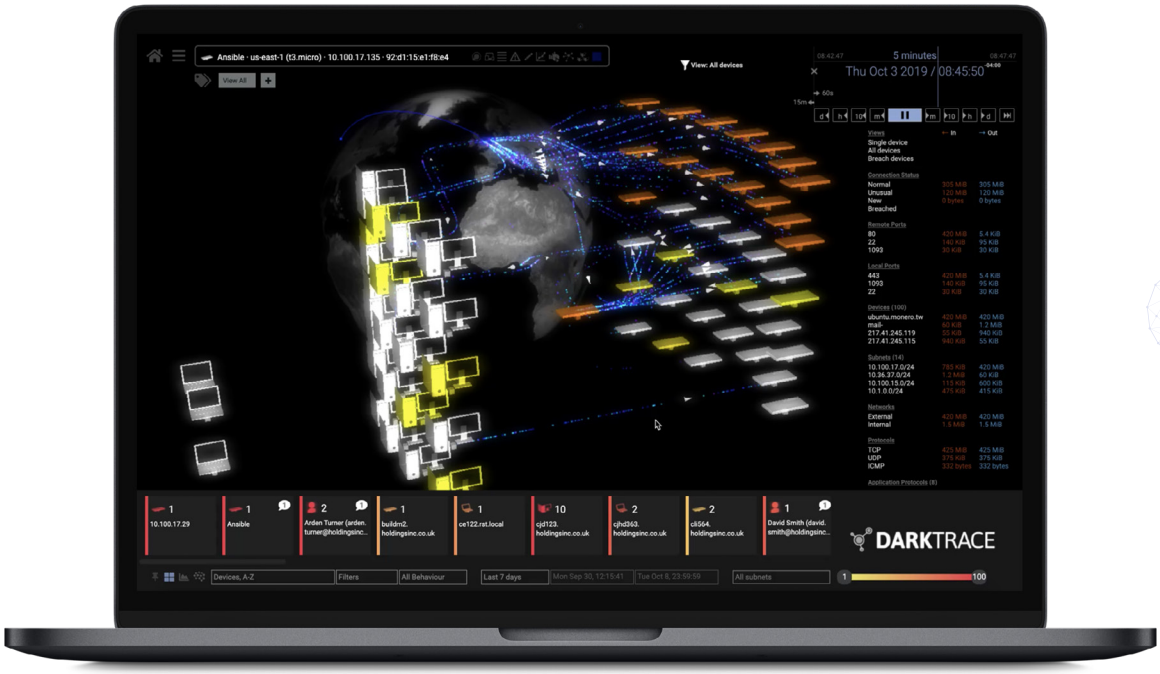


Figure 16: A DevOps configuration error leading to the rapid spread of crypto malware

Shodan Attack on Cloud Vulnerability

A financial services organization was hosting a number of critical servers on VMs in the cloud, some of which were meant to be public-facing, some of which were not. When configuring their native cloud controls, they mistakenly left an important server exposed to the Internet when it was meant to be isolated behind a firewall. This could have happened for a variety of reasons, possibly because of a quick and chaotic migration, or possibly due to lack of familiarization with the native controls provided by their CSP.

While the security team was completely unaware of the misconfiguration, the exposed server was eventually discovered and targeted by cyber-criminals scanning the Internet via Shodan. Within seconds, Darktrace's AI detected that the device was receiving an unusual amount of incoming connection attempts from a wide range of rare external sources and alerted the security team to the threat.

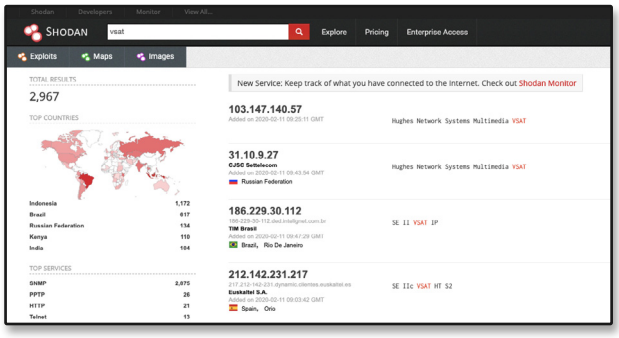


Figure 17: The Shodan website was used for vulnerability scanning

Unencrypted PII in AWS

A city government in the US in the process of outsourcing databases to AWS failed to properly interrogate the protocols the server used to download information. As a result, the addresses, phone numbers, and vehicle registration numbers of its citizens were all being uploaded to an external database via unencrypted connections.

This highly sensitive data was intended for limited access by select employees within the city government, but the security oversight had made the data available to any attacker capable of scanning the perimeter of the network and collecting the data-rich packets that came their way.

The organization was initially unaware of the misconfiguration, which remained under the radar of its entire security stack. However, when Darktrace detected an unusual connection to a rare external IP from a desktop device within the company, it verified that this communication was revealing sensitive public data, which an attacker could access to gather material for future spear phishing attacks or even identity fraud. The complete, real-time visibility that Darktrace provides revealed this dangerous blind spot and allowed the security team to correct the misconfiguration.

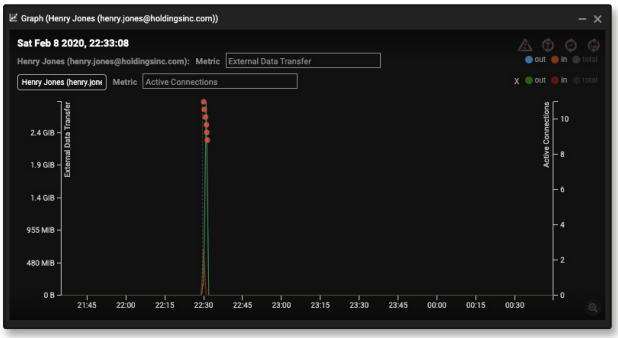


Figure 18: The Threat Visualizer showing over 2GBs of data being transferred externally

Crypto Mining Malware Inadvertently Installed

Darktrace detected a mistake from a junior DevOps engineer in a multinational organization with workloads across AWS and Azure, and leveraging containerized systems like Docker and Kubernetes. The engineer accidentally downloaded an update that included a crypto miner, which led to an infection across multiple cloud production systems.

After the initial infection, the malware started beaconing out to an external command and control server, which was immediately picked up by Darktrace. With the external connection established and the attack mission instructions delivered, the crypto malware infection was then able to rapidly spread across the organization's expansive cloud infrastructure at machine speed, infecting 20 cloud servers in under 15 seconds.

Thanks to Darktrace's AI, the organization's cloud environment was no blind spot, with a dynamic and unified view across its sprawling hybrid and multi-cloud infrastructure allowing the security team to contain the attack within minutes, rather than hours or days. Even though the attack moved at machine speed, Darktrace caught it at an early enough stage, well before the costs could start to mount.

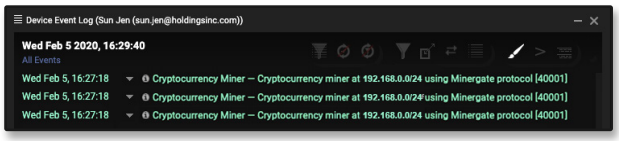


Figure 19: The crypto mining malware detected in real time

Exposed IP in Azure

A leading manufacturing company in Europe was using a Microsoft Azure server to store files containing product details and sales projections. Whilst the files on the server and the root IP were gated with a username and password, this sensitive data was then left unencrypted. Anomalous activity was detected when a device downloaded a ZIP file from a rare external IP address that Darktrace deemed highly anomalous.

It was later discovered that the external IP was a newly configured Microsoft Azure server and the ZIP file was accessible to anyone who knew the URL, which could have been obtained by simply intercepting network traffic, either internally or externally. More dedicated attackers could have even brute-forced the file 'key' parameter of the URL.

The loss or leakage of the sensitive files in question could have placed an entire product line at risk, but in reporting this incident as soon as it was detected, Darktrace helped to prevent the loss of valuable intellectual property, and proceeded to assist the security team in revising their data storage practices in the cloud in order to better protect their product information moving forward.

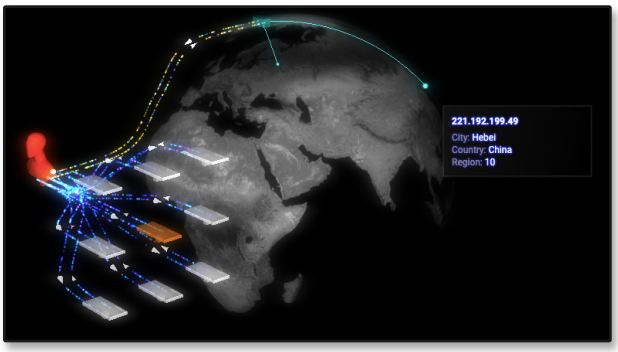
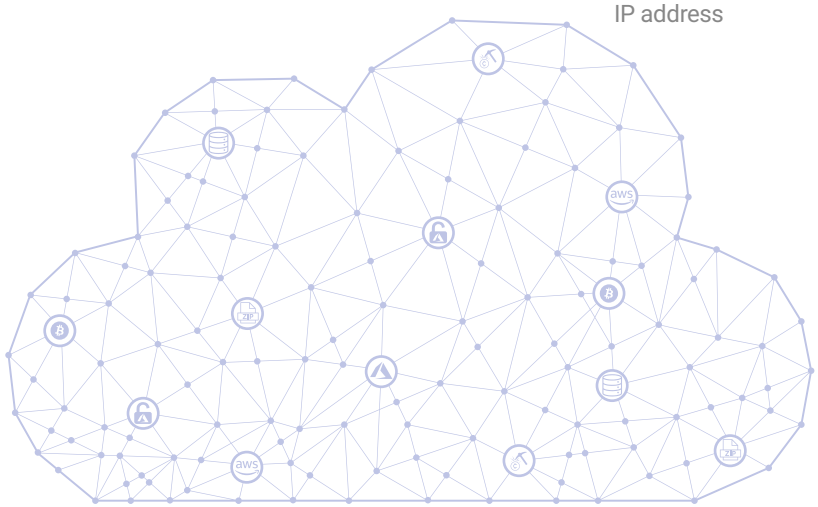


Figure 20: Darktrace showing the location of the unusual IP address



The Overzealous DevOps Engineer

At an insurance group, a DevOps Engineer was attempting to build a parallel back-up infrastructure within AWS to replicate the organization's data center production systems. The technical implementation was perfect and the back-up systems were created. However, the cost of running the system would have been several million dollars per year.

The DevOps Engineer was unaware of the costs associated with the project and kept management in the dark. The cloud infrastructure was launched and the costs started rising. Yet Darktrace's AI alerted to this unusual behavior, and the security team was able to take preventative action immediately.

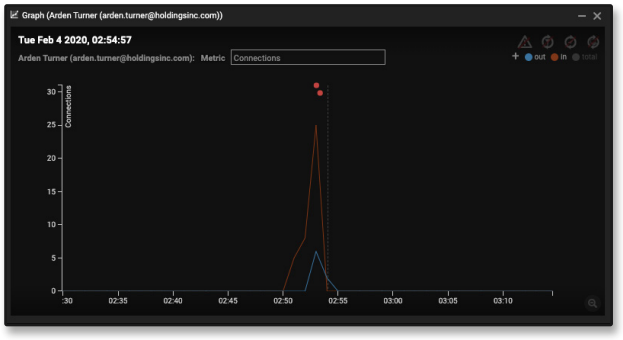
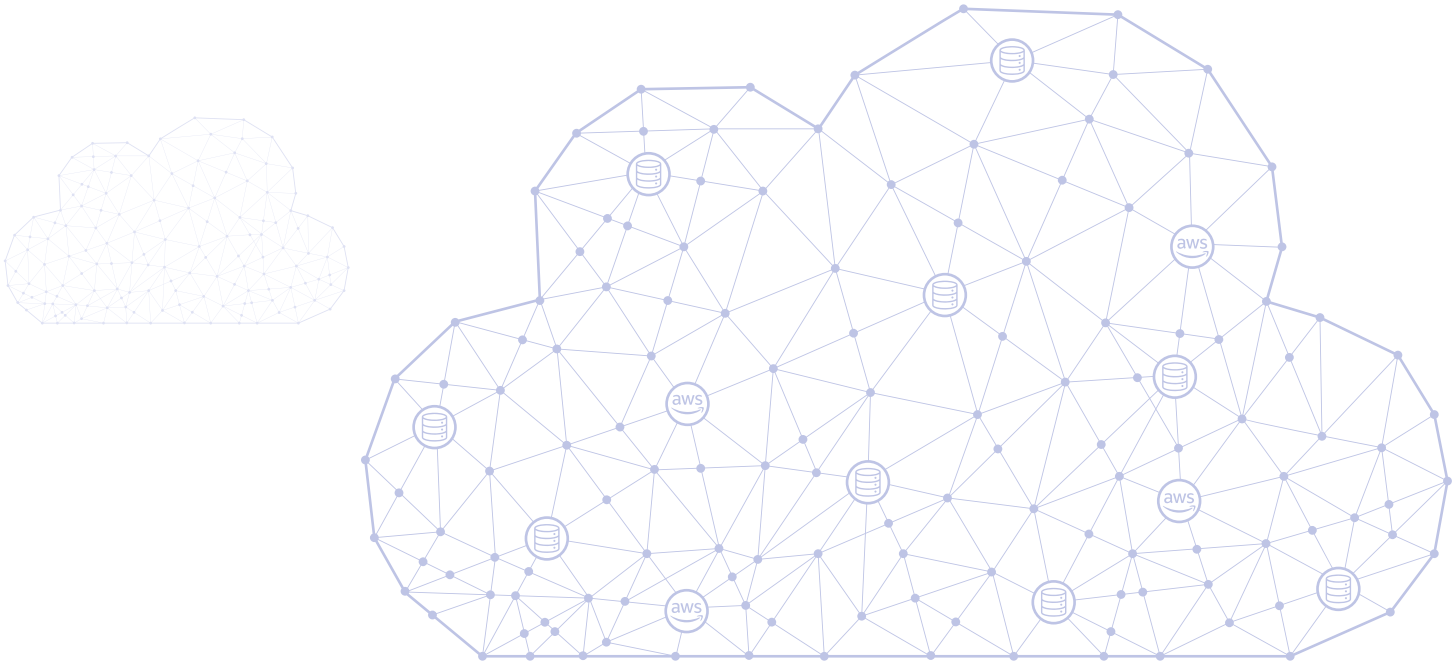


Figure 21: The Threat Visualizer showing a spike in internal and external connections



Deployment Scenarios

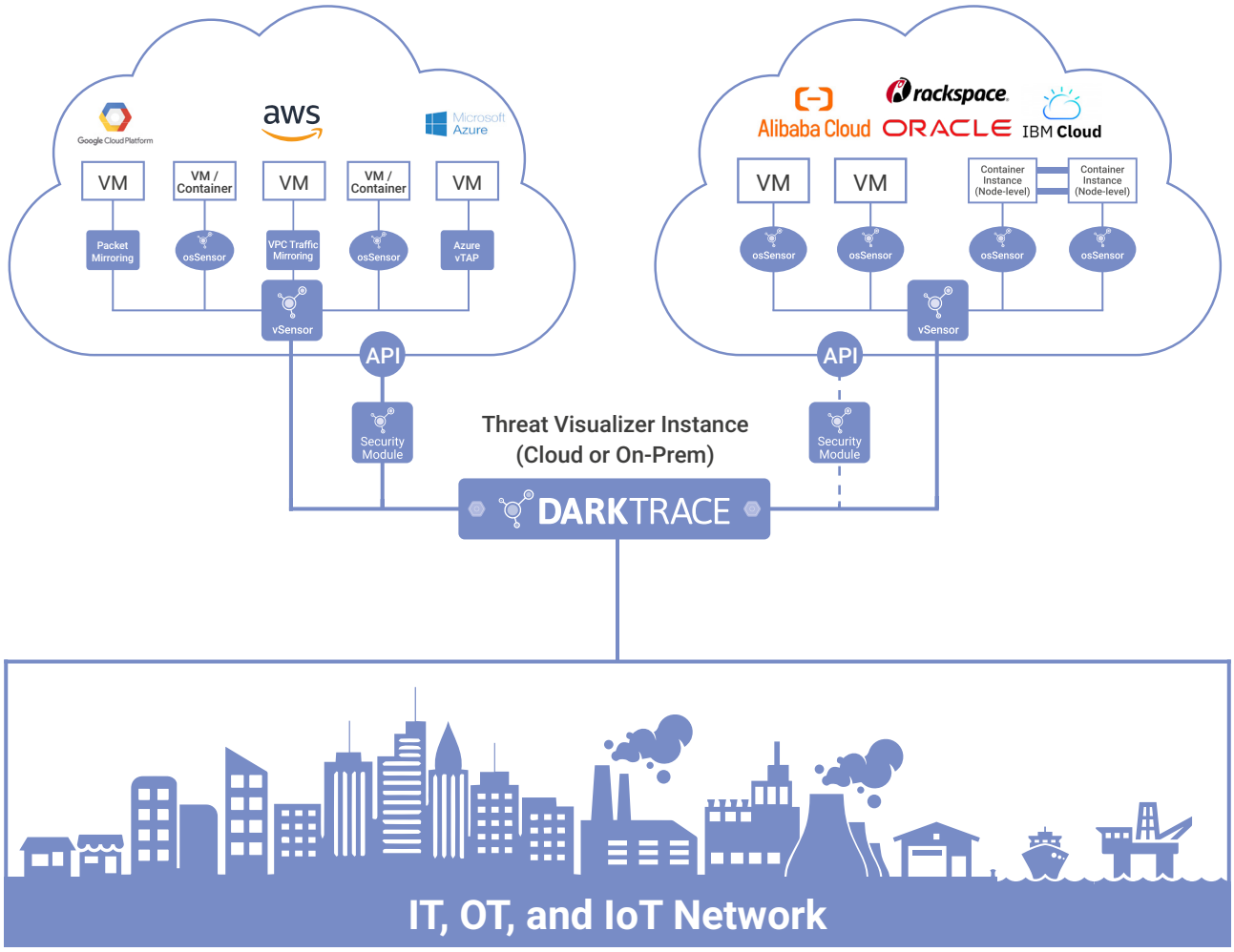
Hybrid Cloud (IaaS)

Depending on the deployment scenario and CSP, Darktrace coverage in IaaS environments can include 'vSensors' and 'osSensors' that ingest real-time cloud traffic, as well as 'Security Modules' that ingest event logs highlighting admin activity, such as logins and resource creations.

In AWS, Azure, and GCP, vSensors capture real-time traffic directly from AWS VPC Traffic Mirroring, the Azure vTAP, and GCP Packet Mirroring, respectively. The receiving vSensor processes the data and feeds it back to a central Darktrace instance for analysis.

To cover other IaaS environments (e.g. Alibaba Cloud, Rackspace, and others), osSensors are installed on each cloud endpoint and configured to send intelligent copies of cloud traffic to a local vSensor, and in turn, to a central Darktrace probe.

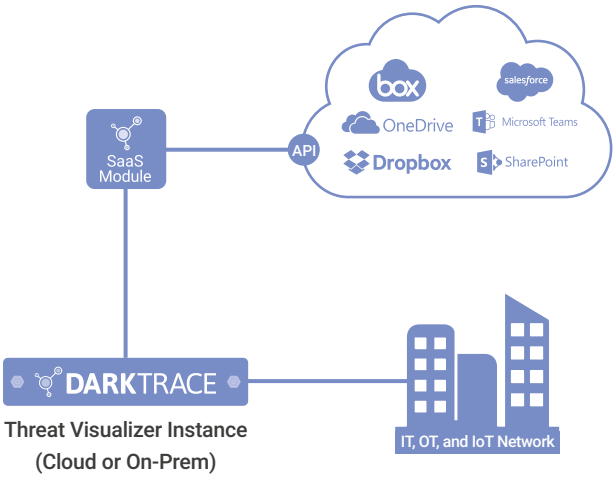
Darktrace can also capture container traffic in Docker and Kubernetes via a specialized osSensor, which similarly feeds data to a local vSensor and Darktrace instance for analysis.



Hybrid Cloud (SaaS)

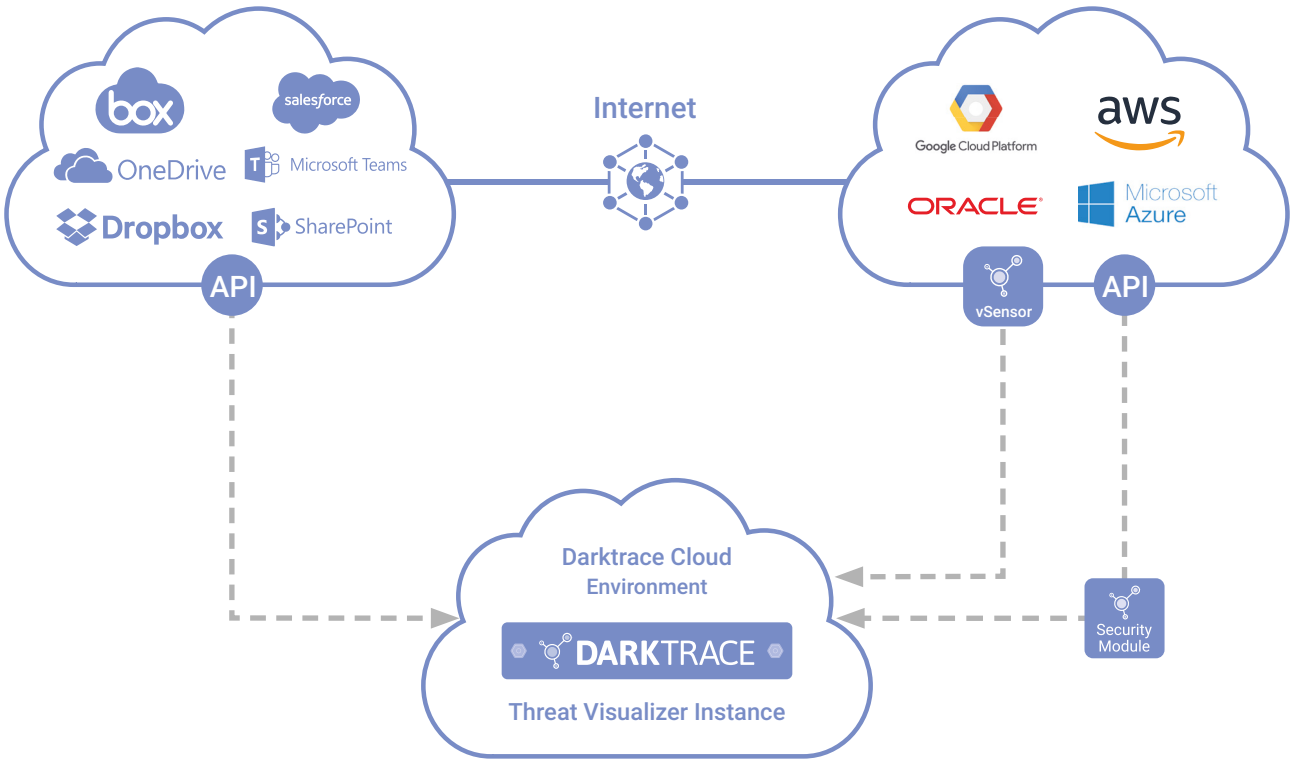
For hybrid SaaS deployments, Darktrace SaaS Modules are remotely installed on a core Darktrace instance (whether cloud or on-prem) to interrogate the security APIs of the relevant SaaS solutions. This includes Microsoft 365, Salesforce, Dropbox, Box, Egnyte, and many more.

Once the Modules are deployed Darktrace continuously analyzes and correlates SaaS data with traffic across the rest of the business in a unified view.



Cloud Only (IaaS and/or SaaS)

If a customer leverages the cloud but doesn't have an on-premise network, Darktrace can deliver a cloud-only deployment as a dedicated service. For cloud-only deployments, Darktrace manages a master cloud probe which receives traffic from sensors and connectors in the customer's IaaS and/or SaaS environments.



Conclusion

As organizations increasingly rely on cloud and SaaS services to streamline business practices and supercharge innovation, the familiar paradigm of the network perimeter has rapidly dissolved, leaving a porous and ever-changing digital estate in its wake.

While the benefits of cloud computing will ensure that migration continues apace, the unique security challenges in this area will not only require a more agile mindset, but also self-learning technologies that can move at the speed of digital business and spot subtle threats at an early stage. The increasing emergence of hybrid, multi-cloud, and IoT environments will also require a single security platform that can correlate activity across diverse digital systems in a unified view, and in real time.

Thanks to its unique 'immune system' approach, Darktrace's Cyber AI Platform is the first and only solution that works seamlessly across multiple stove-pipes to detect cyber-threats wherever they emerge. Rather than rely on static rules and policies, the technology embraces the uncertainty inherent in today's complex digital environment and leverages it to regain the advantage.

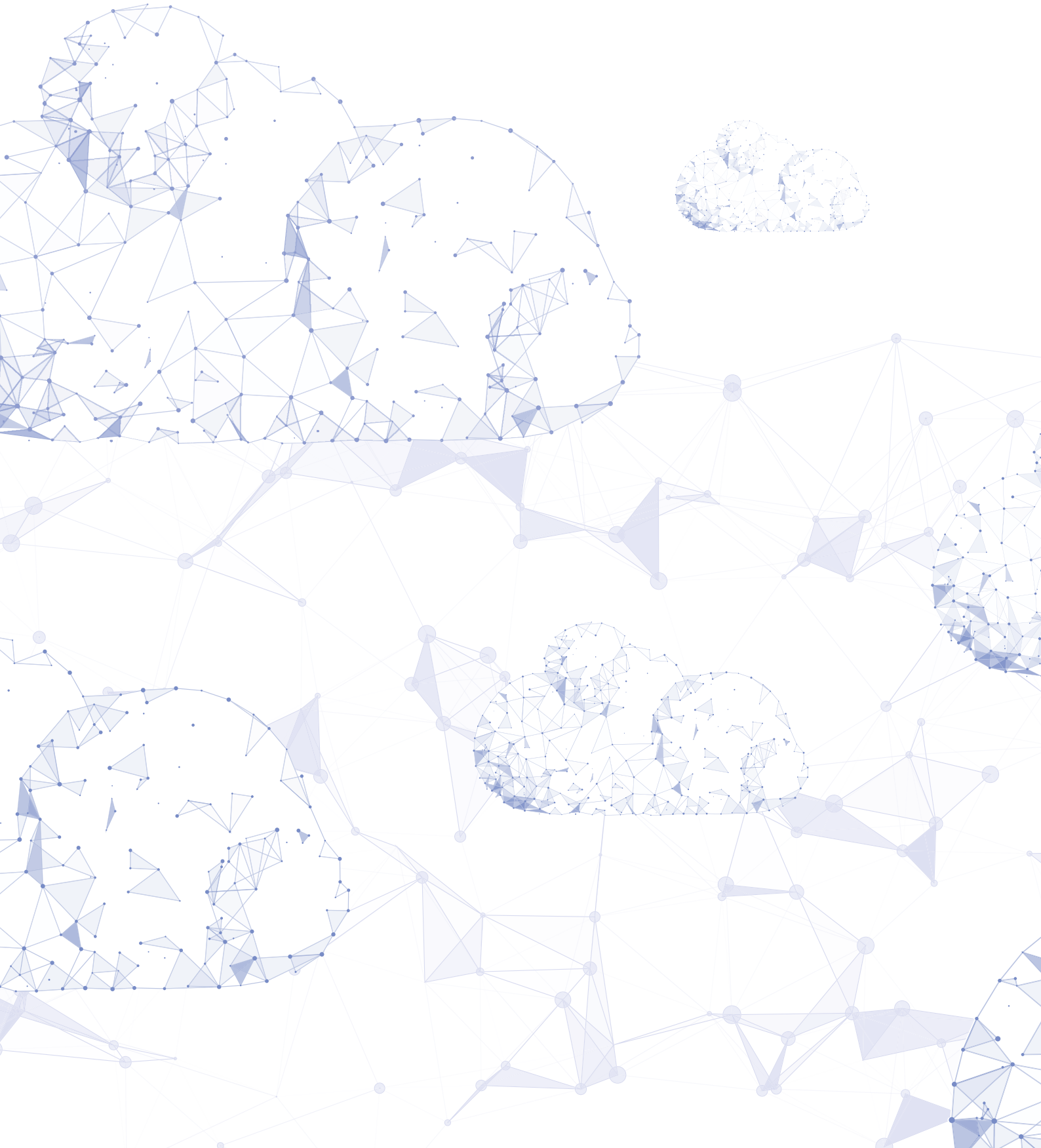
By deploying Darktrace's Cyber AI, business leaders can embark on their journey to the cloud with the confidence that their security posture is resilient and their critical data is secure.

Key Takeaways

- Learns 'self' to detect cloud-based threats other tools miss
- Correlates activity across hybrid and multi-cloud environments
- 100% real-time visibility that leaves attackers with nowhere to hide
- Automatically investigates security incidents with Cyber AI Analyst

> Darktrace represents a new frontier in AI-based cyber-defense. Our team now has complete real-time coverage across our SaaS applications and cloud containers.

– CIO, City of Las Vegas



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 3,500 organizations to protect against threats to the cloud, email, IoT, networks and industrial systems.

The company has over 1,200 employees and headquarters in San Francisco and Cambridge, UK. Every 3 seconds, Darktrace AI fights back against a cyber-threat, preventing it from causing damage.

Contact Us

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

@darktrace