

Self-Learning Cloud Security

White Paper

The Coming Storm: A New Era of Cloud Attacks

The Coming Storm

Vulnerabilities of the Cloud

Traditional Approach

Self-Learning

Autonomous Response

Case Study

Real-World Threat Finds

Technical Overview

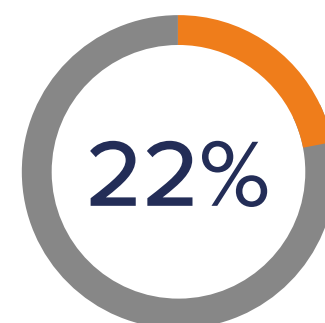
Cloud-Delivered

Organizations are embracing cloud infrastructure with the aim of achieving greater efficiency, flexibility, and innovation. Although these business goals are largely met, they often come at the price of a coherent and effective security approach.

While the decision to migrate to the cloud is usually taken by business leaders, the burden of setting up and safeguarding these environments falls to IT teams, who often lack the required expertise and resources to defend this complex infrastructure.

The same benefits that have attracted organizations to the cloud have drawn attackers, who seek to generate maximum profits faster while avoiding detection. As cyber-threats grow in scale and speed, the need to protect cloud infrastructure is critical.

But today's new era of cyber-threats demands more than just cloud security – organizations need enterprise-wide defense that can operate at the pace of digital business, adapt to future threats, and correlate the subtle hallmarks of an advanced attack.



22% of organizations feel they have adequate visibility in the cloud
Cybersecurity Insiders

Self-Learning AI for Cloud Security

Self-Learning AI is the only technology that understands what 'normal' looks like across your cloud environments, enabling it to detect and respond to subtle deviations indicative of threat that other tools miss. Continuously updating this knowledge in real time, Darktrace for Cloud provides dynamic and contextual protection across your digital infrastructure, unifying defense in a single AI system.

Key Benefits

- Stops novel and sophisticated cyber-threats across hybrid, multi-cloud environments
- Thrives in complexity, with coverage including AWS, Microsoft Azure, and Google Cloud
- Takes targeted action to contain threats at machine speed
- Delivered from the cloud, global coverage in minutes



Vulnerabilities of Cloud Computing

The Coming Storm

Vulnerabilities of the Cloud

Traditional Approach

Self-Learning

Autonomous Response

Case Study

Real-World Threat Finds

Technical Overview

Cloud-Delivered

Mass-scale migration to the cloud has surged in the wake of widespread remote and hybrid working. But this rapid transformation, born out of business necessity, has resulted in new security challenges. IT teams are now having to play catch up, discovering latent vulnerabilities and weaknesses in their cloud infrastructure.

Complexity

Cloud infrastructure usually involves multiple unique providers, divided security responsibilities, and an array of siloed security controls. Not only must teams get to grips with this wealth of technology but they must regularly configure and manually fine tune it – leading to overlooked cloud instances and unencrypted data.

Interconnectivity

Cloud scalability and interconnectivity allows threats to spread more quickly – with attacks taking days instead of weeks to fully advance. To capitalize on this, cyber-criminals have started to target underlying cloud hosts, before moving into client environments disguised as legitimate admins.

Small Margin for Error

Human error is inevitable. But in the cloud, a single misconfiguration or compromised credential can have a broad impact across far-reaching environments. Attackers are then able to act as legitimate users, easily evading detection - thanks to just one open port or publicly accessible secret key.

“Darktrace has enabled us to migrate to a pure cloud architecture”

SVP Operations & Strategy, Differentia Consulting

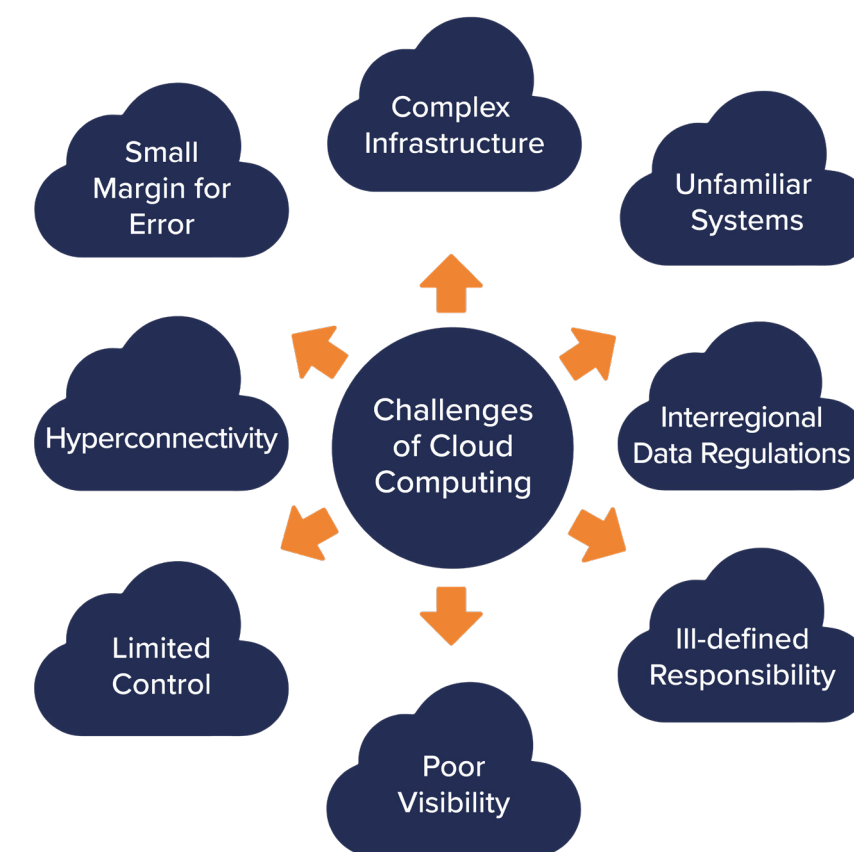


Figure 1: Challenges faced by defenders when safeguarding cloud infrastructure

Traditional Defenses: A Complex Patchwork

The Coming Storm

Vulnerabilities of the Cloud

Traditional Approach

Self-Learning

Autonomous Response

Case Study

Real-World Threat Finds

Technical Overview

Cloud-Delivered

Traditional cloud security comes in two forms: native controls and third-party tools. But while these may help defend an organization’s portion of the Shared Responsibility Model, they are typically preventative and focus on policy enforcement as opposed to advanced detection and response – with organizations having to employ tools from multiple vendors just to get a sense of complete coverage.

Such a fractured arrangement creates blind spots and results in more manual work for security teams, leading to overly relaxed permissions, simple mistakes, and missed attacks.

Native Security Controls

Native security controls are often exclusively designed for a single cloud provider, covering only one portion of a vast, hybrid, multi-cloud enterprise. This drastically limits the scope of detection and adds another tool for teams to fine tune.

While these help with compliance, log collection, and static policy creation, they are not designed for advanced or contextualized threat detection and response – meaning sophisticated, novel, and cross-platform threats get through.

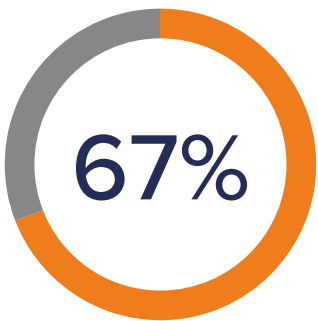
“Darktrace acts autonomously, freeing up our team to work on higher-level tasks”

Principal Digital Architect, McLaren Racing

Third-Party Cloud-Specific Tools

To address the siloed approach of native security tools, third-party vendors have begun to develop cloud-specific security solutions like Cloud Access Security Brokers (CASBs), Cloud Workload Protection Platforms (CWPPs), and Cloud Security Posture Management (CSPM).

But these third-party tools often suffer from the same pitfalls as their native counterparts, relying on historical attack data and preconceived ideas of ‘bad’ – meaning that by design, novel threats are undetected.



of cyber security professionals believe their teams do not have enough time/resources to investigate, understand, and contain urgent cyber-threats

Autonomous Systems: The Future of Cyber Security, SINC

Self-Learning Cloud Security

The Coming Storm

Vulnerabilities of the Cloud

Traditional Approach

Self-Learning

Autonomous Response

Case Study

Real-World Threat Finds

Technical Overview

Cloud-Delivered

4

Learns Your Organization, Stops the Threat

Powered by Self-Learning AI, Darktrace for Cloud learns the normal ‘patterns of life’ for users, devices, and instances from scratch in order to detect and respond to unknown and unpredictable cyber-attacks, all without relying on training data or preconceived ideas of ‘bad’.

Thrives in Complexity

Self-Learning AI is agnostic to different data forms and continuously revises its understanding of ‘normal’ across multiple cloud workloads in real time.

Such a holistic approach means the AI recognizes that actions which appear benign in isolation can point to a greater picture of threat.

Complete Visibility

Darktrace for Cloud provides total visibility of your organization in a single pane of glass. This comprehensive view means that, for example, the AI can understand how a user login in AWS is linked to highly unusual login activity on that same user’s Microsoft 365 account moments earlier. In such a case, Darktrace would immediately realize that an account takeover had occurred and autonomously stop the threat.

Augmenting Security Teams With Automated Threat Investigations

To buy back time for security teams, Cyber AI Analyst autonomously triages, investigates, and reports on every part of an attack in the cloud, connecting signals of malicious activity across technologies and infrastructures. It then auto-generates a natural language report which puts your team in a position to take action: detailing the initial entry point, laying out affected assets and environments, and providing remediation advice.

With Cyber AI Analyst, you can rapidly understand the full scope of a security incident, even in the most complex cloud environments.

Cyber AI Analyst saves up to 92% of security analysts’ time

Autonomous Response

- The Coming Storm
- Vulnerabilities of the Cloud
- Traditional Approach
- Self-Learning
- Autonomous Response**
- Case Study
- Real-World Threat Finds
- Technical Overview
- Cloud-Delivered

Pre-Programmed Response Mechanisms

Today’s attacks are consistently outpacing even the most experienced cyber analysts – occurring at a speed, scale, and level of sophistication that humans are fundamentally unable to counter. On top of this, cyber-criminals are increasingly striking out-of-hours, when no-one is around to action a response. This has led to a surge in demand for automated response solutions.

However, these tools typically use pre-defined threat lists, resulting in a mechanical and heavy-handed response. And pre-programmed actions have to be specifically configured by human teams – an arduous, manual process.

But most successful attacks today are novel in some way. If the threat is unknown, defenders can’t possibly have an appropriate response planned in advance.

“Seeing the attacks Darktrace stopped that were otherwise getting through gave us the confidence to fully activate this for all of our userbase”

CISO, Calligo

Autonomous: Fast and Precise

Autonomous Response takes a fundamentally different approach. By using Self-Learning AI that understands what ‘normal’ looks like across the business, it can calculate the best action to take, at the right time, to effectively contain unpredictable attacks targeting your cloud.

Crucially, the AI decides how to react for itself to stop the in-progress threat. Darktrace for Cloud works by specifically targeting the ‘bad’ behavior and continuing to monitor the incident in case the attacker changes tactics and further intervention is needed.

As a result, Darktrace’s response is targeted and proportionate, taking precise action to interrupt attacks without disrupting your business.

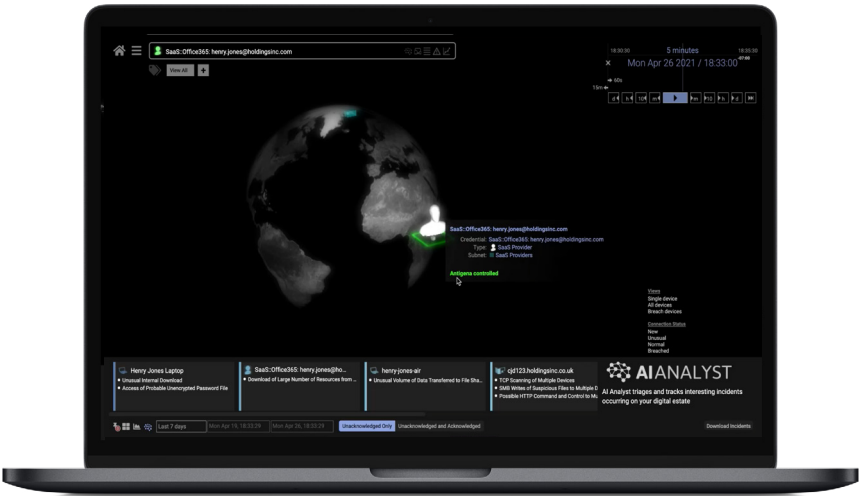


Figure 2: Autonomous Response surgically contains in-progress attacks - without the need for human input

Case Study: Mainstream Renewable Power

- The Coming Storm
- Vulnerabilities of the Cloud
- Traditional Approach
- Self-Learning
- Autonomous Response
- Case Study
- Real-World Threat Finds
- Technical Overview
- Cloud-Delivered

Microsoft and Darktrace: Better Together

Mainstream Renewable Power is one of the world’s leading pure-play developers of renewable energy.

In 2014, the team began its transition to the cloud in order to support its expansion into new markets. Mainstream embraced the full suite of Microsoft products and was one of the first companies to implement MS Sentinel in 2019 to monitor its cloud infrastructure.

But this journey to the cloud brought new security challenges. Faced with an upsurge in cyber-threats, Mainstream choose Darktrace’s Self-Learning AI to complement Microsoft’s native security products, enhance the security team, and protect its critical digital assets.

Darktrace’s Self-Learning AI and Autonomous Response capabilities have provided an additional layer of defense, covering the full range of threats including those ‘unknown unknowns’ never seen before in the wild.

With Autonomous Response technology, emerging attacks are stopped in seconds – before the damage is done – keeping the team’s cloud infrastructure, users, and data safe, no matter where or when threats emerge.



Figure 3: Darktrace’s dedicated interface for cloud-based threats

“We are leveraging all of Microsoft’s security technologies but adding Darktrace takes us to another level”

Global Head of Information Solutions, Mainstream Renewable Power

Real-World Threat Finds

The Coming Storm

Vulnerabilities of the Cloud

Traditional Approach

Self-Learning

Autonomous Response

Case Study

Real-World Threat Finds

Technical Overview

Cloud-Delivered

SharePoint Attack on Unencrypted Passwords

At a European bank, cyber-criminals infiltrated a corporate cloud instance. Darktrace identified the malicious activity as soon as it emerged, enabling the security team to leap into action and stop the attacker leveraging multiple corporate passwords for nefarious purposes.

While the exact method of entry is unclear, it is likely that a member of the IT team unwittingly made their access key publicly accessible. Given the complexities of the cloud and the small margin for error, such a mistake is all too easy.

Darktrace for Cloud first observed unusual activity occurring on the company's Microsoft 365 SharePoint file. A corporate user was accessing unencrypted passwords which was highly suspicious given their normal 'pattern of life', as well as that of their peer group and the wider organization.

Darktrace's extensive understanding of 'normal' across the organization enabled the AI to identify this as a high-fidelity attack, ensuring the security team was able to remediate the threat before it became a crisis.

Had the attack been allowed to continue, cleartext passwords would have been leveraged by the cyber-criminal to escalate their privileges and further infiltrate the organization.

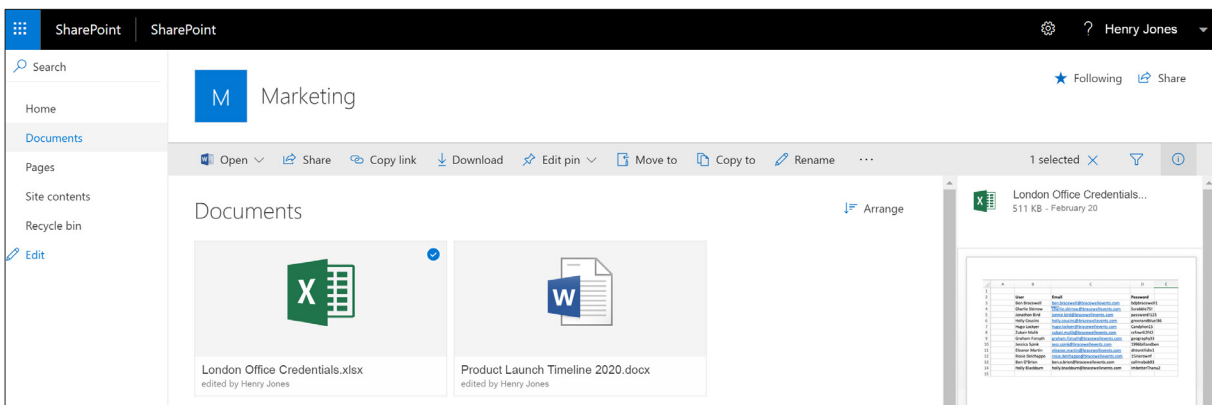


Figure 4: The sensitive files accessed on SharePoint

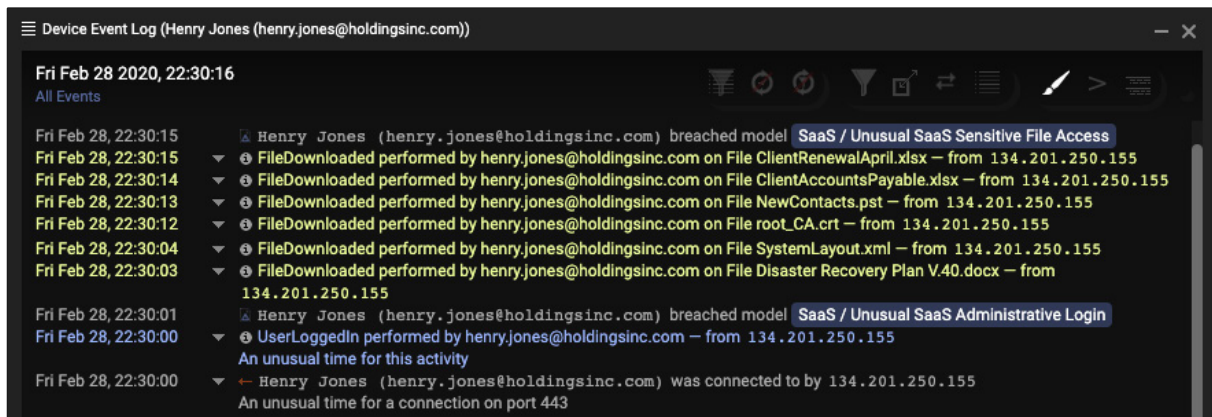


Figure 5: Darktrace surfaces the sensitive file downloads

The Coming Storm

Vulnerabilities of the Cloud

Traditional Approach

Self-Learning

Autonomous Response

Case Study

Real-World Threat Finds

Technical Overview

Cloud-Delivered

Account Compromise Evades Azure Active Directory

Darktrace for Cloud detected an account takeover that bypassed Microsoft Azure AD’s static ‘impossible travel’ rule at an international non-profit. The attacker proceeded to infiltrate a user’s email environment and set up new processing rules. Had Autonomous Response technology been activated, the attack would have been stopped after the initial login and would never have made it as far as the inbox.

The attack began when a user logged in from an unusual IP address and location. While the company operates globally, neither this user nor their peer group had logged in from here before. Once on the system, the attacker pivoted to the user’s email environment and set up a new processing rule which deleted inbound and outbound emails.

With this 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.

Thankfully, Darktrace’s early detection meant that the security team was able to lock the account after the new processing rule was implemented, preventing any damage

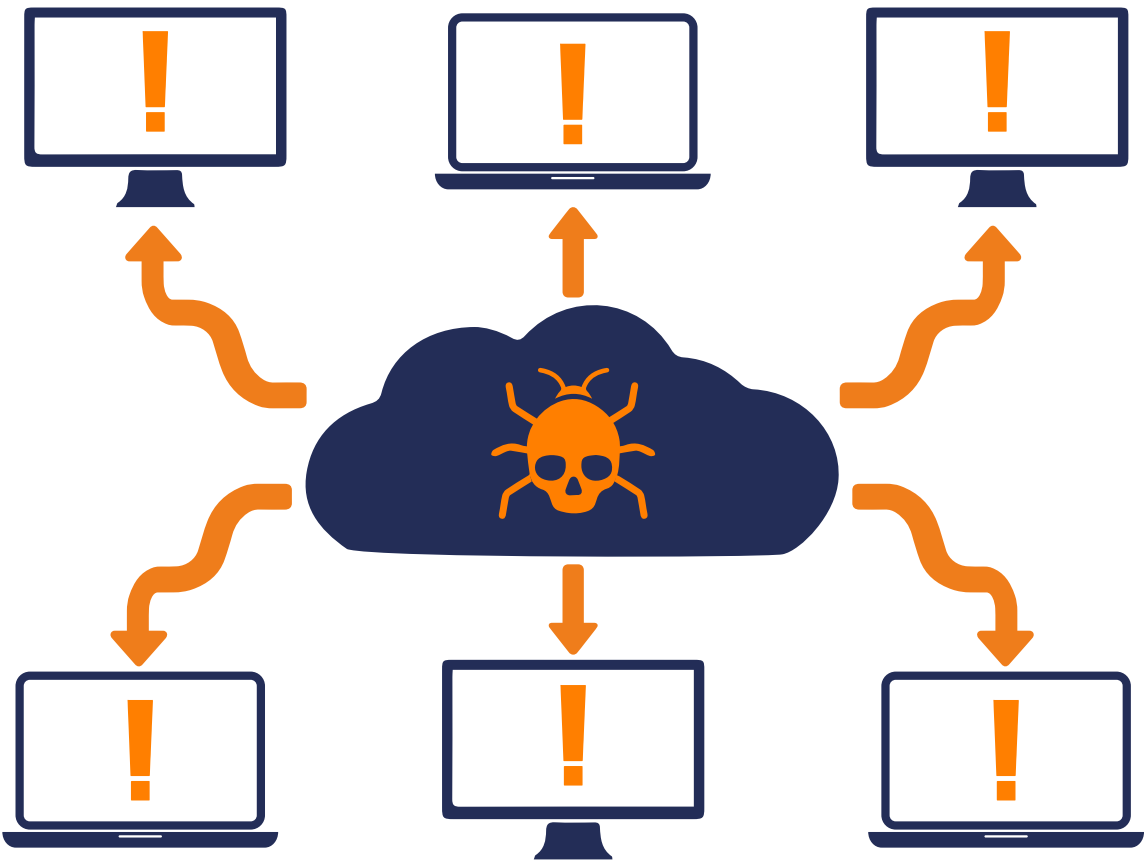


Figure 6: One infected cloud instance allows cyber-criminals to quickly spread throughout an organization

“Darktrace notified me of a compromised Microsoft account. Because of this alert I was able to lock the bad guys out and reset the user’s password within 7 minutes of the first improper access”

IT Manager, Hydrotech

The Coming Storm

Vulnerabilities of the Cloud

Traditional Approach

Self-Learning

Autonomous Response

Case Study

Real-World Threat Finds

Technical Overview

Cloud-Delivered

Unencrypted PII in AWS due to Protocol Misunderstanding

When a city government in the US outsourced its databases to AWS, it 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.

While this could have resulted in a serious cyber-attack, not to mention data privacy fines, Darktrace for Cloud was able to detect the misconfiguration and help the team remediate the threat.

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 address 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.

Had Autonomous Response technology been activated, this unusual connection would have been surgically interrupted – meaning no unauthorized data access would have occurred either internally or externally. As it was, Darktrace’s complete, real-time visibility was able to reveal this dangerous blind spot, and the security team was able to correct the misconfiguration before it turned into a crisis.

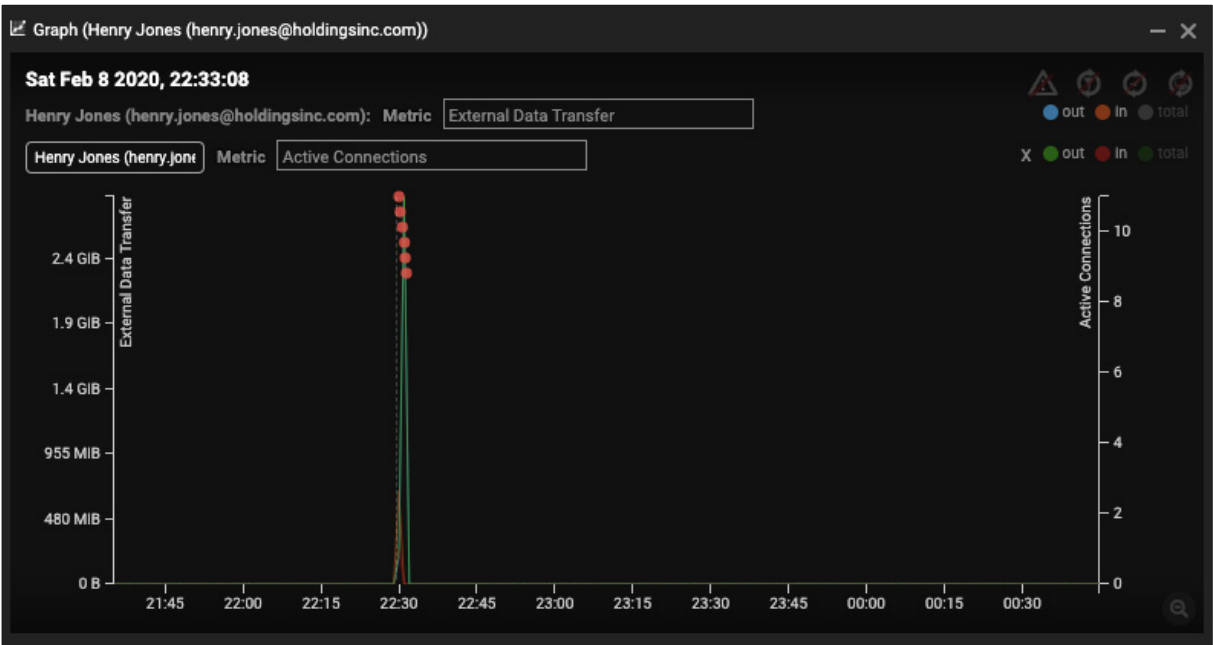


Figure 7: The Threat Visualizer showing over 2GBs of data being transferred externally

“Using AI, Darktrace can detect and respond to email-borne threats and cloud-based attacks that other tools miss”

CIO, City of Las Vegas

The Coming Storm

Vulnerabilities of the Cloud

Traditional Approach

Self-Learning

Autonomous Response

Case Study

Real-World Threat Finds

Technical Overview

Cloud-Delivered

Crypto-Mining Malware Infects 20 Servers in Under 15 Seconds

Darktrace detected a mistake from a junior DevOps engineer in a multinational organization which resulted in crypto-mining malware being installed. With Self-Learning AI, the infection was identified in its earliest stages, enabling the team to quickly remediate the threat.

The attack began when the engineer accidentally downloaded an update that included crypto-mining malware. Once in the cloud infrastructure, the malware began beaconing to an external command and control server, which Darktrace for Cloud immediately detected as unusual and highly indicative of attack.

Had Autonomous Response technology been deployed, the malware would have been stopped at this point. As it was, the attack was allowed to continue.

With the external connection established and the attack mission instructions delivered, the infection was then able to rapidly spread across the organization’s expansive cloud infrastructure at machine speed. 20 cloud servers were affected in under 15 seconds.

With large workloads across AWS and Azure, and leveraging containerized systems like Docker and Kubernetes, this attack could have ground the company’s business operations to a halt. But Darktrace’s complete, real-time visibility and autonomous threat detection capabilities meant that the security team was able to contain the attack within minutes, rather than hours or days – preventing the worst of the damage.

Even though this attack moved at machine speed, Darktrace caught it at an early enough stage, well before the costs could start to mount.

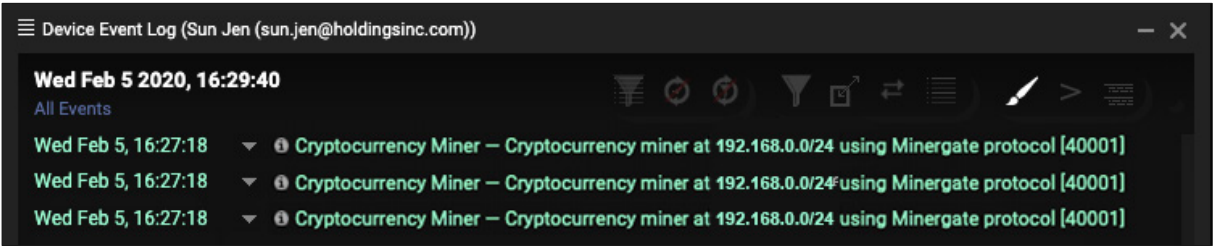


Figure 8: The Crypto-mining malware detected in real time

“Crypto-mining malware has the ability to hamper and even crash an organization’s digital environment, if unstopped”

Justin Fier, Director of Cyber Intelligence & Analytics, Darktrace











Technical Overview: AI Defense in the Cloud

- The Coming Storm
- Vulnerabilities of the Cloud
- Traditional Approach
- Self-Learning
- Autonomous Response
- Case Study
- Real-World Threat Finds
- Technical Overview
- Cloud-Delivered

AWS

By combining packet-level data from AWS VPC traffic mirroring with API logs generated from PaaS and SaaS usage, Darktrace is able to extract hundreds of features from the raw data and build rich behavioral models for each organization’s unique AWS cloud environment.

Self-Learning AI uses this deep knowledge of what ‘normal’ looks like in the cloud to deliver total coverage and defense across all AWS services, including:

- | | |
|---|--|
|  Certificate Manager |  RDS |
|  Athena |  Route 53 |
|  EC2 |  S3 |
|  IAM |  VPC |
|  Lambda |  DynamoDB |

Microsoft Azure

Self-Learning AI continuously monitors all Azure cloud traffic via Darktrace osSensors: lightweight, host-based, server agents.

Each osSensor feeds packet-level data to a local Darktrace vSensor, which then feeds the relevant metadata to a Darktrace master probe for analysis. This is analyzed alongside data generated from API audit logs, enabling Darktrace for Cloud to provide AI-powered monitoring of management activity, user access, and resource creation for additional visibility.

Such a comprehensive view allows Darktrace’s Self-Learning AI to deliver defense across all Azure services, including:

- | | |
|--------------------------|-----------------|
| o Azure DevOps | o Azure SQL |
| o Virtual Machines | o Blob Storage |
| o CosmosDB | o Queue Storage |
| o Azure Active Directory | o File Storage |
| o Azure Function | o Table Storage |

The Coming Storm

Vulnerabilities of the Cloud

Traditional Approach

Self-Learning

Autonomous Response

Case Study

Real-World Threat Finds

Technical Overview

Cloud-Delivered

Google Cloud

Darktrace combines Google’s Packet Mirroring service with API audit log data generated from PaaS and SaaS usage to monitor all traffic in an organization’s Google Cloud environment. This allows the AI to analyze the entire packet, including headers and payloads.

With Darktrace’s Google Workspace module, organizations can gain visibility of login and other user activity in Google Cloud as authenticated via the Google Workspace platform. Security teams are provided with full awareness of administrative activity and system events in Cloud Audit Log-compatible services, with additional support for Data Access logs for deeper visibility into specific component activity.

Darktrace delivers total coverage across all Google Cloud services, including:

- BigQuery
- Cloud Compute
- Cloud CDN
- Cloud Run
- Cloud SQL
- Cloud Storage*
- Cloud Translate
- Key Management
- Resource Manager



Figure 9: Darktrace protects users, data, and infrastructure wherever they are in real time

“Darktrace’s machine learning implementation is superior in the marketplace. Their coverage for cloud-based solutions makes their solution a top consideration”

John Tolbert, Lead Analyst, KuppingerCole

Cloud-Delivered Defense

The Coming Storm

Vulnerabilities of the Cloud

Traditional Approach

Self-Learning

Autonomous Response

Case Study

Real-World Threat Finds

Technical Overview

Cloud-Delivered

Whether your organization has fully embraced a hybrid, multi-cloud infrastructure, is primarily on-prem and transitioning to the cloud, or anywhere in between, Darktrace for Cloud will match your needs, with Self-Learning AI that can be delivered from the cloud, on-prem, or a mixture of both to achieve global coverage in minutes.

Deployment Scenario

Depending on the deployment scenario and CSP, Darktrace coverage in cloud environments can include vSensors and/or osSensors that ingest real-time cloud traffic, as well as security modules that ingest event logs and highlight admin activity, such as logins and resource creation.

Darktrace’s vSensors capture real-time traffic directly from AWS, Google Cloud, and Microsoft Azure. The receiving vSensor processes the data and feeds it back to a central Darktrace master cloud probe for analysis.

To cover other IaaS environments, 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 master cloud probe for analysis.

Meanwhile, Darktrace’s Self-Learning AI monitors all API logs generated elsewhere from your cloud usage to provide holistic coverage across IaaS, PaaS, and SaaS.

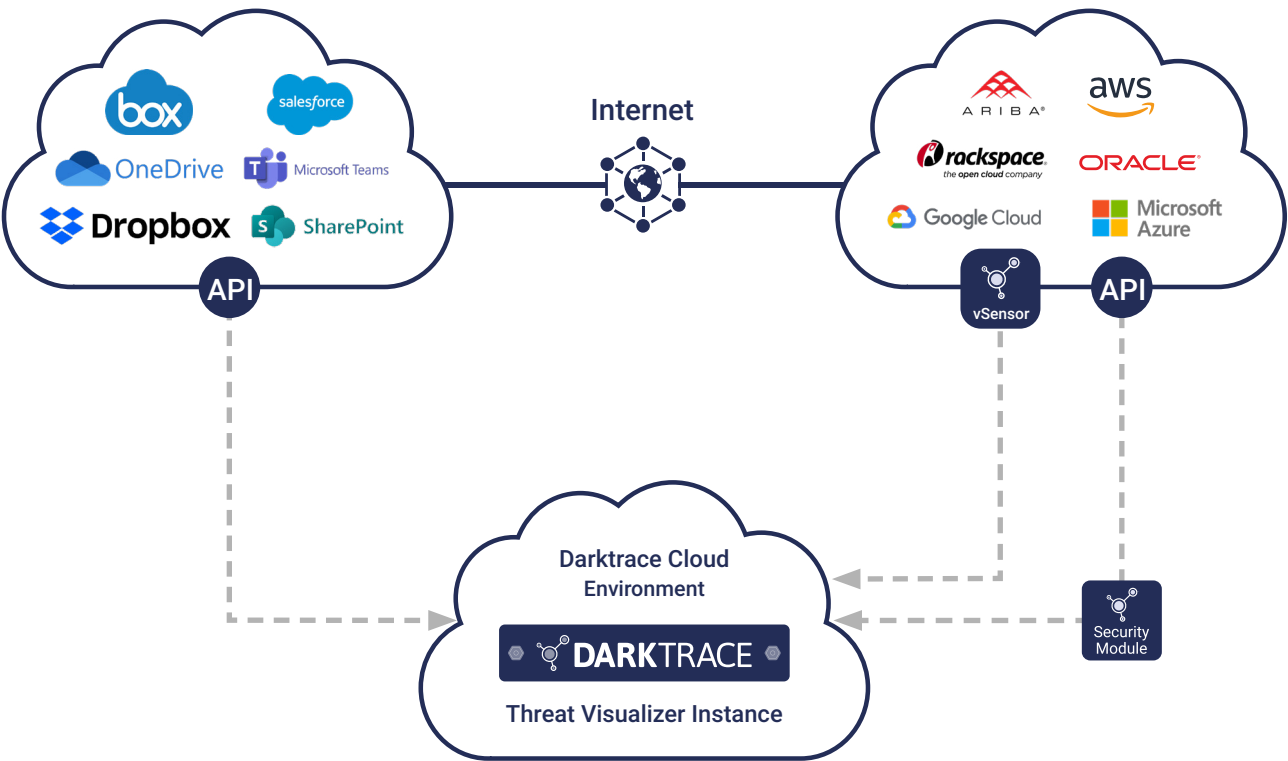


Figure 10: Darktrace’s cloud-only deployment provides autonomous protection across your entire infrastructure

“Darktrace can be set up in minutes and you’ll get value within the hour. It really does turn the lights on”






CISO, Calligo

About Darktrace

Darktrace (DARK:L) a global leader in cyber security AI, delivers world-class technology that protects over 5,000 customers worldwide from advanced threats, including ransomware and cloud and SaaS attacks. The company's fundamentally different approach applies Self-Learning AI to enable machines to understand the business in order to autonomously defend it. Headquartered in Cambridge, UK, the company has 1,500 employees and over 30 offices worldwide. Darktrace was named one of TIME magazine's 'Most Influential Companies' for 2021.

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 demo](#)
-  [Visit our YouTube channel](#)
-  [Follow us on Twitter](#)
-  [Follow us on LinkedIn](#)