Cloud Threat Report 2019

Threat Case Studies

Summary

This report summarizes 11 case studies of cloud-based attacks identified by cyber AI, including spear phishing, insider threat, and zero-day malware. The case studies demonstrate how weak indicators of malicious activity were only detectable using Darktrace AI, a cloud-native solution that detects and responds to advanced cyber-threats in hybrid and multi-cloud environments.

Introduction

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 enterprise, 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 Office 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 remaining sufficiently low profile to avoid attention from law enforcement. 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 solution 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.

Darktrace AI: A Cyber Immune System for the Cloud and Beyond

Powered by artificial intelligence, Darktrace's Enterprise Immune System fills these critical gaps with a unique self-learning approach that detects and responds to cloud-based attacks that others miss.

The solution works by learning the normal 'pattern of life' for every user, device, and container across hybrid and multi-cloud environments, without defining 'benign' or 'malicious' in advance. 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 as it emerges in disparate corners of the network.

And while pre-programmed point solutions can certainly complement this approach, Darktrace's cloud-native AI is the only proven solution 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.

By deploying Darktrace's cyber AI, organizations can now leverage the full benefits of the cloud with the confidence that their security posture is resilient and their critical data is secure.

> "Darktrace represents a new frontier in AI-based cyber defense. Our team now has complete, real-time coverage across our SaaS applications, cloud containers, and city-wide distributed sensors."
>
> **City of Las Vegas**

A Unified View for Hybrid & Multi-Cloud Environments

Through its intuitive Threat Visualizer interface, Darktrace provides complete visibility across your diverse digital infrastructure – from cloud environments like AWS and Azure, to business applications like Salesforce and Office 365.

box
salesforce
JumpCloud
Google Cloud Platform
rackspace the open cloud company
aws
EGNYTE
G Suite
Dropbox
Microsoft Azure
Office 365

Insider Threat in the Cloud

Unlike external threat actors, malicious insiders are often uniquely positioned to evade traditional controls given their privileged access and intimate knowledge of the network. Whether these controls rely on binary detection logic or merely monitor the perimeter, a disaffected employee can often easily bypass static defenses in the cloud and exfiltrate or manipulate critical data without triggering suspicion.

A retailer in the UK decided to restructure its IT department and let a number of employees go. One of the affected employees – an IT manager – downloaded contact details and credit card numbers from the customer database before leaving, secretly transferring them to a home server via one of the company's regular data transfer services. The IT manager 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 very limited visibility in this area.

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 Manager's device, even though the cloud service was regularly used for legitimate purposes by other employees.

Darktrace's AI 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.

Spear Phishing Attack in Office 365

While many phishing attacks are launched as indiscriminate 'drive by' campaigns, Darktrace's AI has detected a wide range of targeted email-borne attacks with the markings of coordinated and sophisticated cyber-crimes. In one case, a threat actor had gotten hold of the address book of a US municipality, delivering an attack to recipients alphabetically, from A to Z. While each email was well-crafted and customized to the recipient, the messages all contained a malicious payload hiding behind a button that was variously disguised as a link to Netflix, Amazon, and other trusted services.

Darktrace's AI was able to analyze these hidden links in connection with all Office 365 email traffic and the normal 'patterns of life' of the intended recipients in the network. When the first email came through, Darktrace immediately recognized that neither the recipient nor anyone in his peer group or the rest of the city's staff had visited that domain before. Darktrace instantly raised a high-confidence alert, and suggested autonomously locking each link as it entered the network.

Interestingly enough, the fact that Darktrace Antigena – the system's autonomous response capability – was deployed in 'Passive Mode' provided plain and concrete evidence of Darktrace's ability to thwart subtle attacks that native controls miss. Whereas Darktrace detected the campaign at the letter "A," the city's legacy tools finally woke up to the threat at "R." In 'Active Mode', Antigena would have neutralized the attack before it could reach a single user.

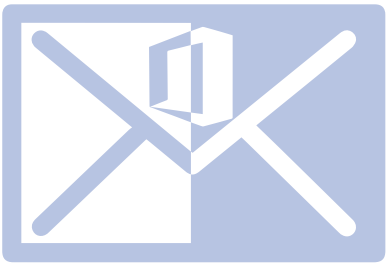
Cloud Misconfiguration

Configuring security controls in hybrid and multi-cloud environments is often an overwhelming and complex process, as native and third-party solutions in this area are often diverse, unfamiliar, and incompatible across platforms. This complexity, together with the unprecedented speed and agility of the cloud, has often led to critical misconfigurations that expose the business to attack.

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.

Email Spoof in Office 365

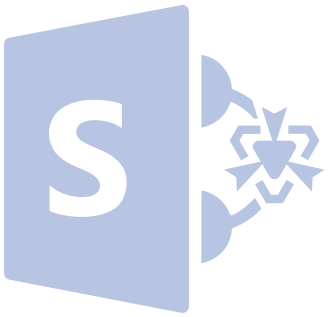


A malicious email spoof involves registering a seemingly legitimate domain that closely resembles that of a trusted contact or service, such that an attacker can trick an unsuspecting recipient and infiltrate a network with ease. More often than not, the attacker will seek to impersonate a high-level executive and make an urgent request, hoping that the employee will comply before spotting the forged sender address. For years this method has allowed attackers to evade traditional controls, as a newly registered domain would not only trick a recipient but also bypass solutions that rely on blacklists.

At one electricity distributor, Darktrace's AI detected a convincing spoof attempt discovered in an Office 365 email account. Allegedly from the company's CEO, the email was sent to a member of the payroll department requesting that the employee update the CEO's direct deposit information. Since the domain used for the spoof did not appear on traditional blacklists used by other solutions, the attack could have easily succeeded if Darktrace's AI hadn't been analyzing the firm's Office 365 mail flow in connection with the rest of the business.

By learning the normal 'pattern of life' of the employee, the CEO, and the wider organization across cloud and network traffic, Darktrace was able to immediately flag a number of subtle anomalies in the email, including the forged sender address. Among other weak indicators, Darktrace's AI automatically calculated the anomalous proximity of the domain to those of internal employees and trusted contacts. The AI responded immediately, locking the email's links and clearly marking it as a spoof before it could reach the payroll department. Darktrace's rich understanding of cloud and network traffic allowed it to neutralize a high-severity threat that signature-based tools would have missed.

SharePoint Attack



After obtaining stolen credentials or otherwise gaining access to an organization's cloud-based file sharing and 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 had managed to find an Office 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.

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.

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.

Supply Chain Account Takeover in Office 365

By hijacking the account details of a trusted contact in your supply chain, sophisticated threat actors can easily gain the trust of a recipient in the network and coax them into clicking a malicious link or transferring millions out of the business. Darktrace's AI caught one such attack targeting a film production studio in LA, after the Office 365 credentials of a contact at a trusted supplier had been compromised and hijacked.

Account details can be leveraged for many nefarious purposes, but in this case, the criminal seems to have used them to read through the contact's historical correspondence with an employee at the studio. After reviewing previous threads, he sent a plausible reply to the employee's latest email, which mirrored the contact's writing style and made sense in the context of the relationship and previous discussions, but also included a malicious link.

Darktrace's cyber AI discerned the weak indicators that revealed this 'trusted contact' to be a hijacked account controlled by an attacker, detecting that the email and its content were outside the 'pattern of life' of the supposed sender. The employee was alerted, and the malicious payload was neutralized.

Crucially, Darktrace's decision was informed by the fact that this particular link would have been rare for both the sender and recipient given their prior communications. Unlike siloed point solutions, Darktrace's AI did not treat the recipient in the network as a mere email address, but understood the full scope of the employee's 'pattern of life' in the context of their interactions and the wider network.

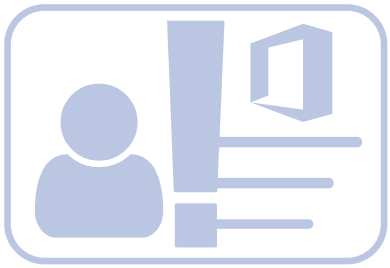
Unencrypted PII in AWS

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.

Compromised Credentials in Office 365



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.

In one international organization, Darktrace caught a compromise in an Office 365 account that bypassed Azure Active Directory's native controls. While the organization had offices in every corner of the globe, Darktrace's 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 incoming 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.

When the security team investigated the incident further, they learned that the user had received a phishing email just hours before Darktrace detected the threat. While the company had also deployed Microsoft's Advanced Threat Protection (ATP) for Office 365, static defenses such as ATP can only spot phishing attacks by correlating links in emails with known malicious addresses, and the phishing link did not appear on the list. This demonstrated the clear limitations of a signature-based approach in this area, and the organization soon deployed Antigena for additional protection in Office 365 given its ability to spot similarly threatening phishing emails without relying on blacklists.

Unencrypted Intellectual Property 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 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.

Zero-Day Attack in Office 365

Legacy security tools that look for the pre-defined hallmarks of an attack are invariably blind to new threat variants, consistently failing to detect novel malware. Only Darktrace's rich and evolving understanding of 'normal' across all cloud and network traffic enables organizations to detect bespoke and zero-day trojans at an early stage.

At one publishing company in the US, Darktrace detected a spoof email sent to the Office 365 account of an employee. The email claimed to be from a trusted colleague requesting an invoice, but contained a disguised malware download link. The never-before-seen link easily bypassed Microsoft's native controls, and did not even appear on VirusTotal until the following day.

Yet Darktrace's AI was able to correlate multiple weak indicators of unusual activity, including the rarity of the domain and the lack of prior communication between the two users. It flagged the email as highly suspicious, enabling the security team to neutralize the threat and prevent significant damage.

The Over-Zealous DevOps Engineer in AWS

While the agility and limited visibility of anomalous cloud activity often introduces considerable security risks, it can also result in equally significant damages and costs that originate from a well-intentioned administrator.

In one notable example, 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 mounting. Yet Darktrace's AI alerted to this unusual behavior, and the security team was able to take preventative action immediately.

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 3,000 organizations to protect against threats to the cloud, email, IoT, networks and industrial systems.

The company has over 900 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