Solve Cloud Forensics at Scale

Archived: 2026-04-05 23:17:31 UTC

10,000

Darktrace customers

LOUVRE
ASTON MARTIN

CITY OF LAS VEGAS
NEVADA

playmobil

LOUVRE

STEVE MADDEN
ASTON MARTIN

CITY OF LAS VEGAS
NEVADA

The challenge

Multi-cloud investigations are manual and slow, and data disappears fast

1/3rd

of alerts in cloud environments do not get investigated due to lack of information

89%

of organizations suffer damage before containing and investigating incidents

Darktrace's report: "Organizations require a new approach to handle investigations and response in the cloud"

Automated data capture across your business

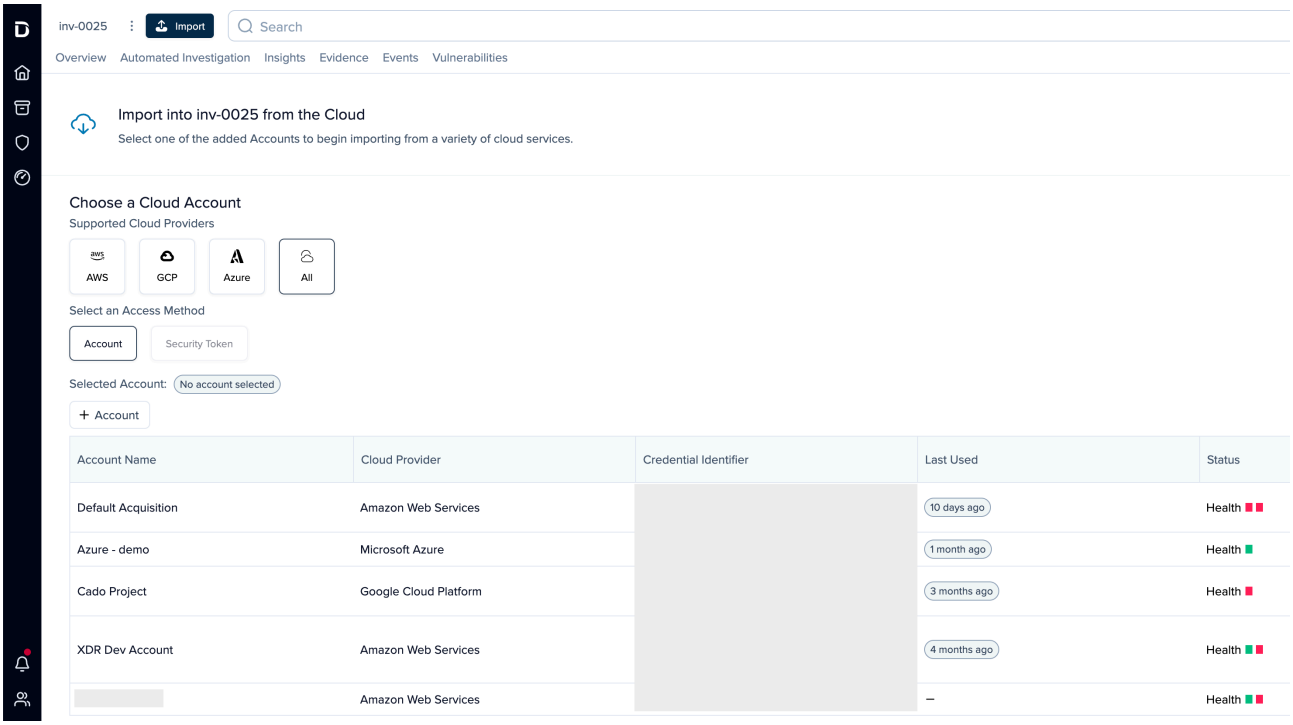
Integrates with any alert source and deploys via API to enable fast, low-overhead response within existing workflows.

Support containers and ephemeral assets

Leverage automation to ensure incident data is captured and preserved before it disappears. Automatically collect key data sources and memory from individual processes for forensic analysis.

Parallel collection and processing

Capture more data in less time, resulting in deep forensic insight delivered in minutes, not days.



Full attack timelines in minutes, not hours

Timelines enriched with context to shows exactly what happened, when, and how

Eliminate tedious manual work

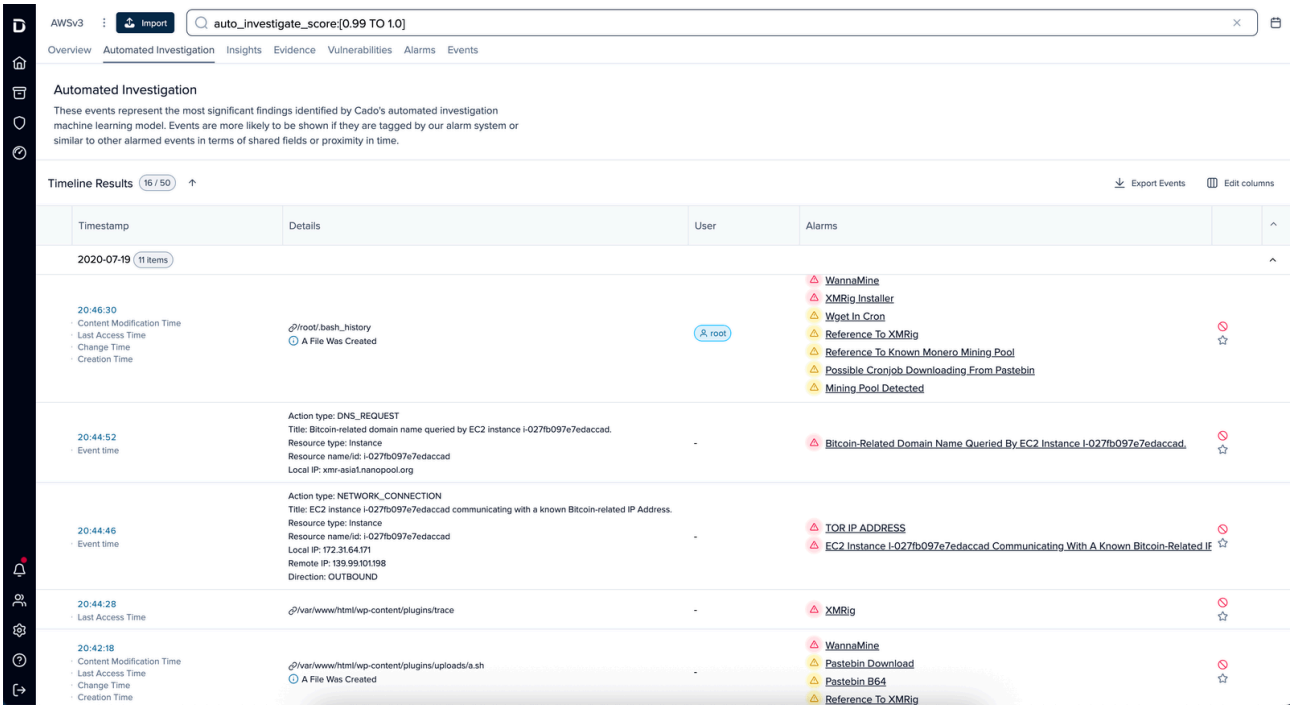
Get root cause analysis for cloud security alerts without combing through logs or artifacts manually.

Accelerate investigations

A visual timeline links files, commands, and lateral movement.

Reduce uncertainty

Ensure response decisions are informed by a complete and accurate picture of the threat.



Use cases

Empowers organizations to respond to threats faster

Better understand risk across complex environments, reduce MTTR, and rapidly deploy with this first-of-its-kind technology

SOC triage

Get immediate insights into malicious activity, saving analysts precious time during event triage. Perform automated triage of acquisitions of endpoint resources to gain deeper context in a shorter period of time.

Cross-cloud investigations

Investigate incidents identified in any cloud environment in a single solution. Findings are unified in one timeline to allow seamless investigation and response.

Container & K8 investigations

Perform investigation and response in ephemeral environments, leveraging automation to ensure incident data is captured and preserved before it disappears.

SaaS investigations

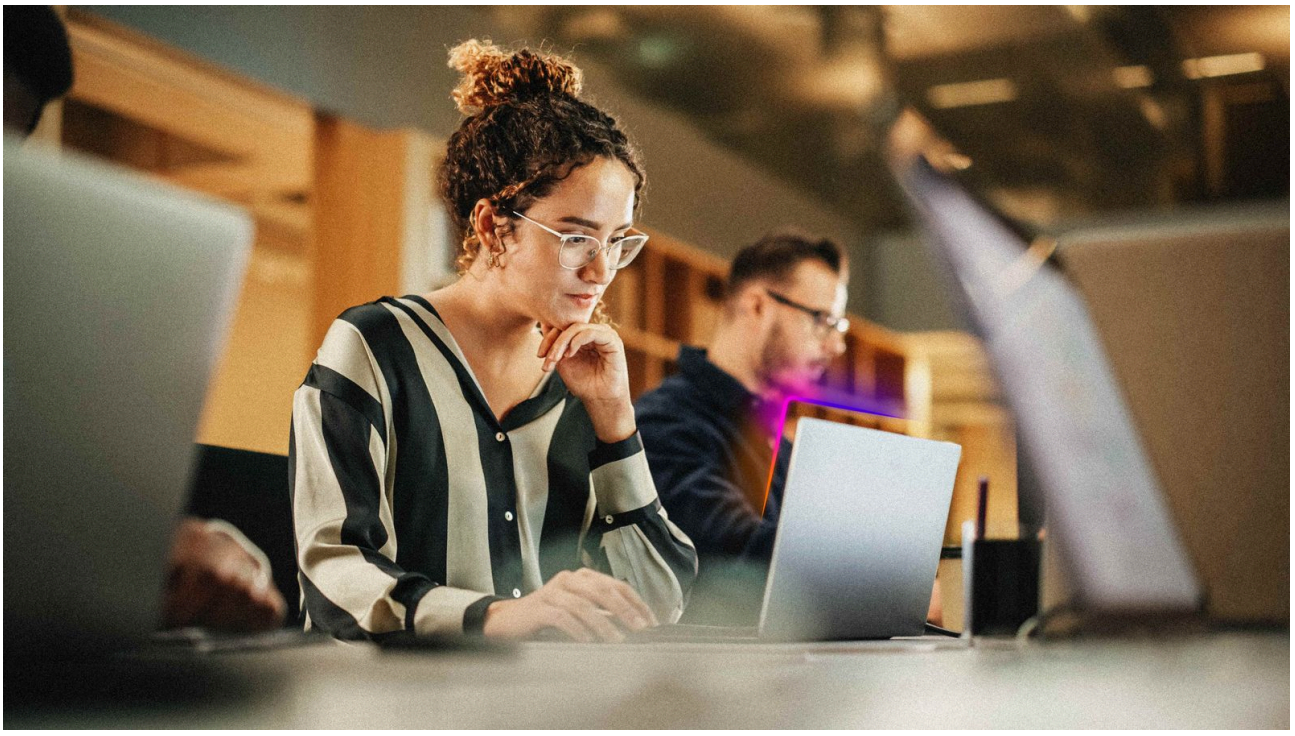
Investigate key SaaS logs, alongside other sources captured across on-premises and cloud assets to gain a better understanding of the scope and impact of malicious activity.

Cloud detection & response

Marry threat detection with automated collection and investigation - with critical forensic-level context - to expedite response to cloud threats as soon as malicious activity is detected.

Evidence preservation

Automate the collection, processing, analysis, and preservation of evidence so it’s accessible to all teams when needed, every time – before it disappears.



“We resolve hundreds of potential incidents in minutes. By assisting analyst investigations, we've been able to drastically increase efficiency by 250%.”

Global Gaming Company

Head of Security Operations

“We have a cloud team that takes countless manual steps to capture and process forensic data...I can’t wait to tell them I can do this in just a few clicks!”

Fortune 500 US Company

DFIR Team Lead

“The fact that I no longer have to wait 24 hours to start a forensics investigation is game changing.”

Top Cybersecurity Consulting Firm

DFIR Manager

Resource

Read the solution brief

250%

increase in capacity

Discover how Darktrace / Forensic Acquisition & Investigation enables faster and deeper investigations in the cloud

Source: https://www.cadosecurity.com/forensic-triage-of-a-windows-system-running-the-backdoored-3cx-desktop-app/