

DARKTRACE

Secure
What AI
Can Do

Darktrace / HYBRID NETWORK

**Forensic Acquisition &
Investigation Capabilities**

Enrich investigations with deeper
host and workload context

Cloud Investigations are Broken

In today's hybrid, cloud-first world, security teams face unprecedented complexity. Existing cloud security tools are heavily dependent on posture management, which lack the forensic depth needed to fully understand the attack and leaving remediation incomplete, increasing risk for future compromise.

Analysts are left with alerts that cannot be easily triaged, resulting in wasted time, false positives, alerts being closed without a complete understanding, or missed threats altogether.

Active attacker behaviors such as lateral movement, privilege escalation, and command-and-control are often invisible in logs, allowing adversaries to move undetected. At the same time, ephemeral assets like containers and serverless functions disappear before evidence can be collected, creating blind spots in investigations.

SOC and DFIR Challenges in a Cloud-First World

The rapid growth and dynamic nature of cloud and hybrid environments have outpaced traditional security tools, leaving both SOC and DFIR teams without the visibility, scale, or speed required to keep investigations effective.

With more than a third of cloud alerts unable to be triaged or investigated before resources change or disappear^[1], security teams can no longer rely on manual data collection, ticketing, or heavy agent-based tools to evaluate alerts and run investigations. The result is delayed response, incomplete visibility, and growing risk exposure at the very moment attackers are moving faster than ever.

For security teams, the challenge is alert volume and context. Analysts are buried under floods of alerts from multiple tools, many of which lack the forensic depth needed to confirm or dismiss a threat. Manual triage creates alert fatigue and wastes valuable time, while ephemeral assets and siloed log data make it difficult to correlate activity or trace attacker movement. Without clear root cause, SOC's are often forced to escalate prematurely or close alerts without full confidence, leaving adversaries with more room to maneuver.

For DFIR teams, the challenge is depth and scale. Traditional forensics tools were built for static, on-premises environments and cannot keep pace with ephemeral workloads that may exist only for minutes. When incidents occur, investigators often find themselves chasing cloud snapshots, requesting access from other teams, or relying on external responders.

These delays not only increase the cost and complexity of investigations but also create blind spots that undermine compliance and litigation readiness. Combined with a global shortage of skilled investigators, the reliance on slow, manual methods has made cloud forensics unsustainable at scale.

Together, these challenges leave SOC and DFIR teams reactive and exposed. Without a unified approach to detection, response, and forensic investigation, critical alerts go uninvestigated, threats escalate unnoticed, and organizations are left vulnerable at cloud speed.

[1] Market Challenge

Darktrace / HYBRID NETWORK

Forensic Acquisition and Investigation Capabilities

Automatically investigate any cloud alert with full disk, memory, and log evidence.

Darktrace / HYBRID NETWORK’s forensic acquisition and investigation capabilities are the industry’s first is the industry’s first true automated forensic platform purpose-built for the cloud. It eliminates the delays and blind spots of traditional forensic tools by instantly capturing and preserving host-level evidence the moment a threat is detected, even from ephemeral workloads like containers or serverless resources.

By enriching investigations with deeper host and workload context, Darktrace / HYBRID NETWORK transforms incident response from slow and fragmented into fast, scalable, and forensically sound. Security teams can quickly uncover root cause, reconstruct attacker timelines, and investigate across AWS, Azure, GCP, SaaS, and on-prem environments, all within a single workflow. The result is faster triage, deeper visibility, and more confident response, giving SOC and DFIR teams the ability to stay ahead of threats and reduce risk in the cloud. It’s cloud forensics at cloud speed, finally built for the environments you run today.

Business Benefits

- Facilitates scalability of cloud-first and cloud-native businesses
- Supports digital transformation
- Improved communications across teams
- Integrates into current technology stack
- Regulatory compliance and audit readiness
- Faster incident response time

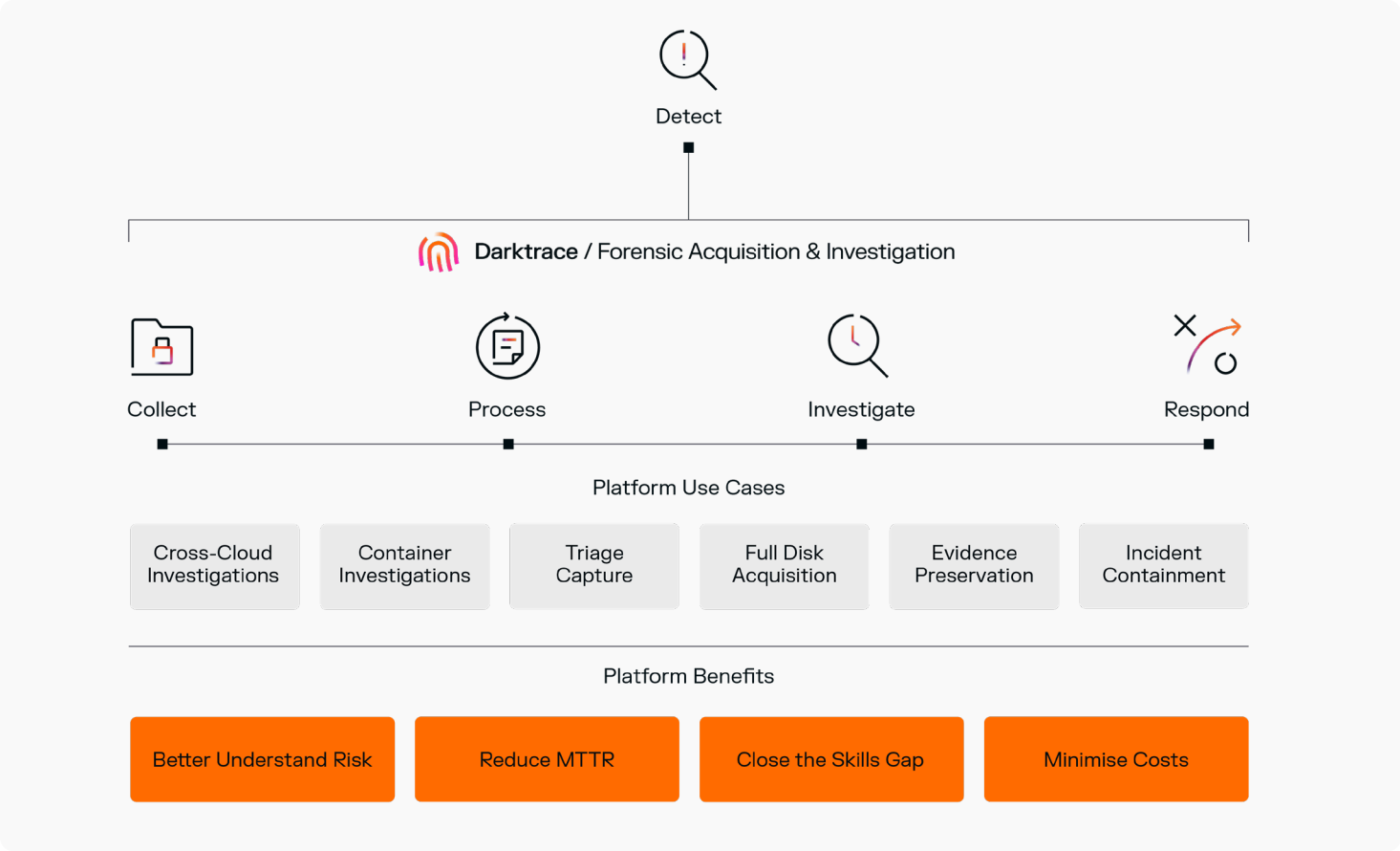


Figure 01: Reducing MTTR with / Forensic Acquisition & Investigation

Enrich Investigations With Deep Host and Workload Context

Cloud-native forensics, designed for scale

Traditional forensic tools were designed for static, on-premises infrastructures, leaving security teams struggling to capture evidence in ephemeral assets or scale investigations across distributed cloud accounts.

Investigating across modern hybrid environments is fragmented and inconsistent, with different tools, access models, and evidence formats slowing response. Darktrace / HYBRID NETWORK was purpose-built for the speed, complexity, and elasticity of modern environments. It closes this gap with cloud-native architecture that seamlessly spans AWS, Azure, GCP, containers, SaaS, and on-prem workloads. Whether deployed across hundreds of accounts or multiple regions, it scales instantly via API integration, eliminating the friction and delays of manual evidence collection.

250%

■ increase in case capacity
reported by a large financial company

Because the solution is designed to integrate with the broader security ecosystem, investigations can be triggered by alerts from any detection source—EDR, XDR, CNAPP, SIEM, or cloud-native tools—ensuring teams can rapidly pivot from detection to deep forensic investigation without switching contexts or waiting for manual processes. This flexibility allows organizations to extend forensic-level visibility and investigation capabilities across every environment, delivering the scale and agility today’s hybrid enterprises demand. The result is faster, more consistent investigations that strengthen response while reducing operational overhead.

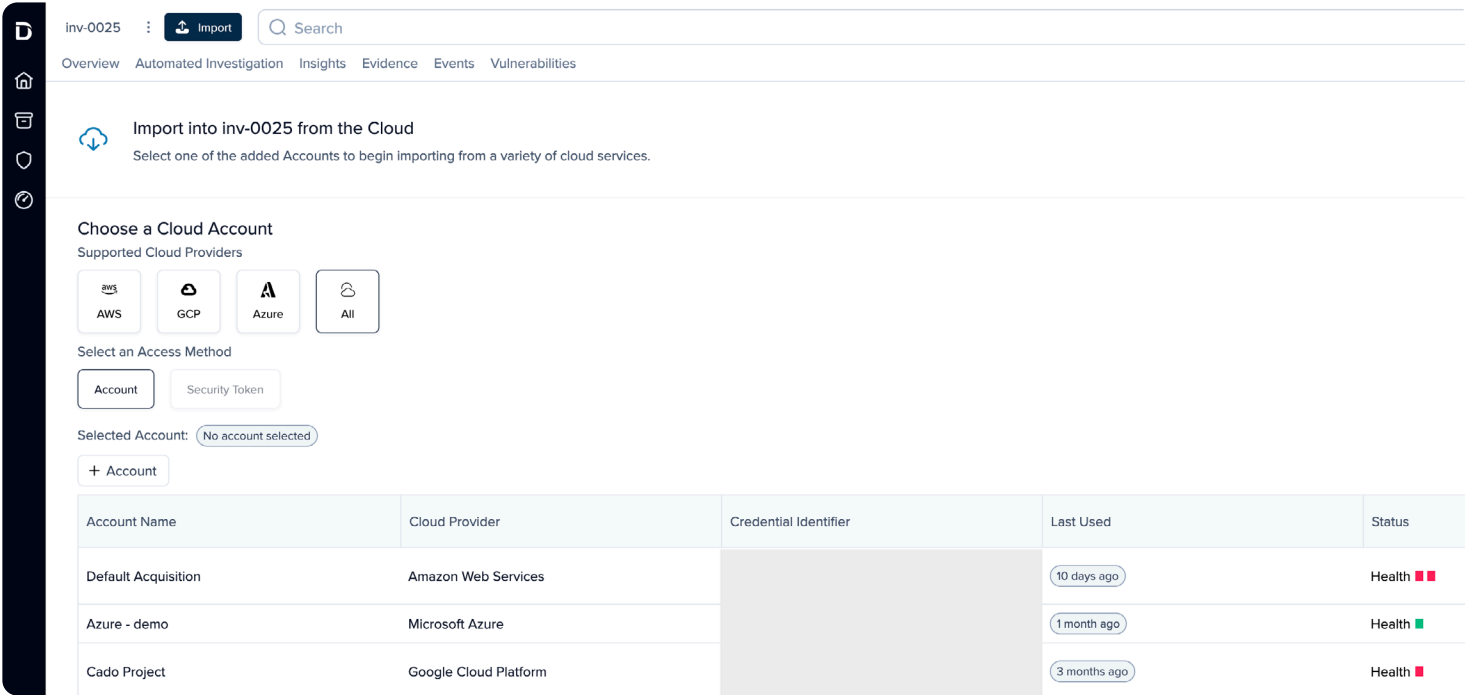


Figure 02: Ability to import data from Cloud, SaaS and on-prem environments

Automate evidence capture at the speed of cloud

Manual evidence collection is too slow for the cloud, often missing ephemeral assets and leaving blind spots in investigations. Darktrace / HYBRID NETWORK automates evidence collection, one of the most time-consuming and error-prone parts of incident response.

Instead of relying on tickets, snapshots, or manual processes that often miss time-sensitive workloads, the solution instantly captures forensic evidence the moment a threat is detected. Full disk and memory can be acquired automatically, including from ephemeral assets like containers or serverless functions that would otherwise vanish before analysts could investigate.

This automation works without agents, reducing deployment overhead and ensuring that collection does not disrupt workloads. Just as important, it isn't limited to Darktrace detections—investigations can be triggered from any signal across the security stack, whether from XDR, EDR, CNAPP, SIEM, or cloud-native tools. By preserving volatile evidence automatically and at cloud speed, the solution eliminates investigation blind spots, giving security teams the forensic clarity they need in minutes rather than days.

“It not only speeds up the process of acquisition and analysis, but it helps us by having more information to dig through and going deeply into the investigation.”

■ Matteo Brunati
CEO - Agorà Security

3 actions

- required by Darktrace / HYBRID NETWORK
Compared to manual cloud evidence collection typically requiring 15-20 steps.

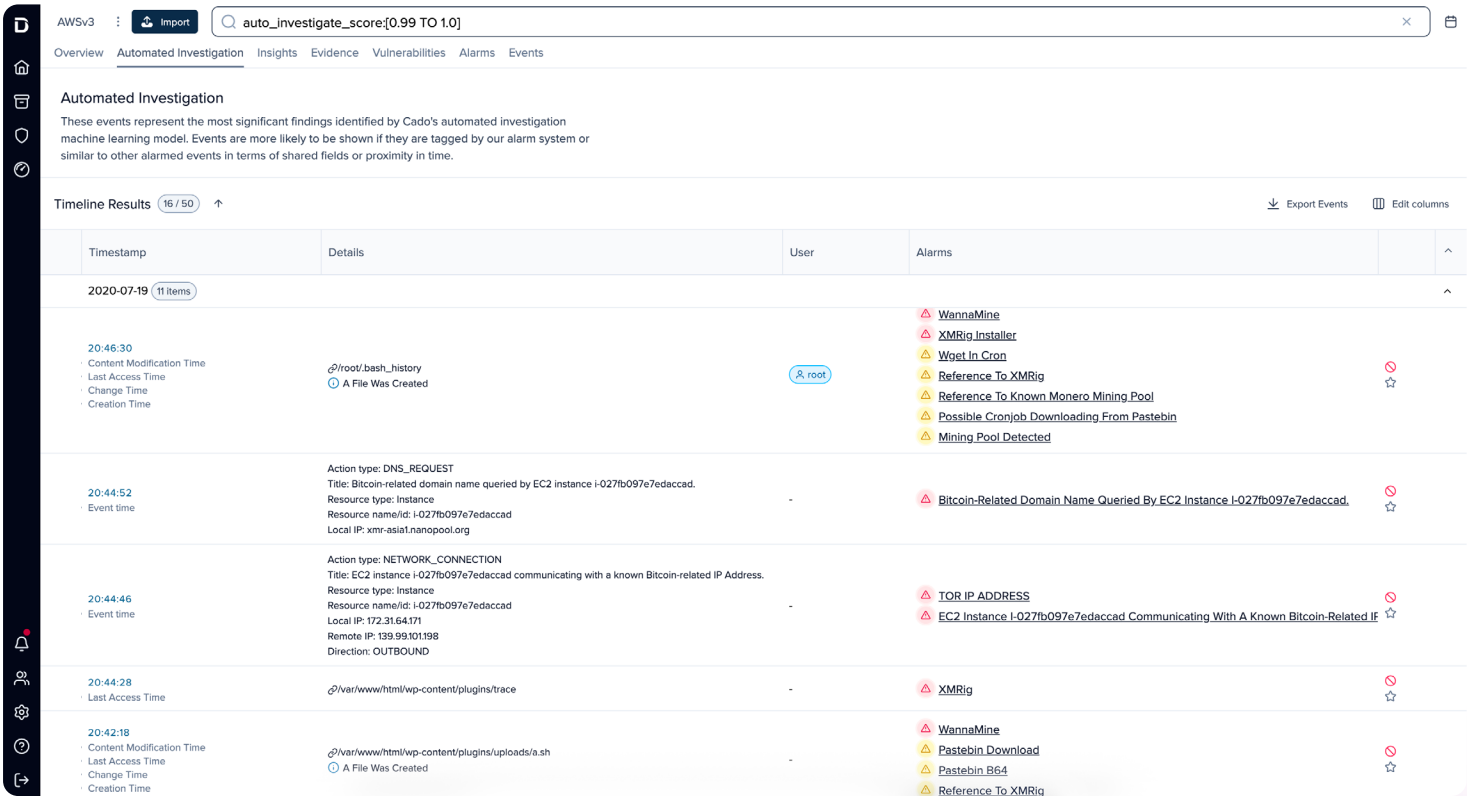


Figure 03: Ability to import data from Cloud, SaaS and on-prem environments



Accelerate time-to-value at scale with rapid and flexible deployment

Every organization’s cloud journey looks different, and so do their operational requirements. Darktrace / HYBRID NETWORK is designed to adapt to your environment, offering deployment models that balance speed, scale, and control.

Whether teams prefer to manage investigations in their own infrastructure or accelerate time-to-value with SaaS delivery, the solution provides the flexibility to meet evolving security needs without compromise.

With flexible deployment options, organizations can align forensic workflows to their existing infrastructure and regulatory requirements, ensuring both deep insight and broad integration.

“After testing out the product, the decision to purchase was a no-brainer. **Darktrace makes things simple.**”

■ **Director, Incident Response**
Large video gaming company

Self-hosted Appliance

Deep Insight. Broad Integration.

For organizations that require maximum control, the self-hosted virtual appliance enables complete forensic investigation at scale across multi-cloud and on-prem environments:

- Complete incident investigation at scale, across clouds
- Preserves ephemeral data for compliance and litigation
- Flexible deployment

SaaS Delivered

Fast Value. Big Impact.

For teams that want quick and easy setup, SaaS delivery provides automated forensic response out of the box. With rapid deployment and minimal overhead, SaaS delivery shortens time-to-value and helps teams stop threats earlier with forensic clarity:

- Respond faster without needing deep cloud expertise
- No heavy setup – automated forensic response out of the box
- Stops threats early by turning detection into action instantly
- Fast deployment

Darktrace Behavioral Defense Platform

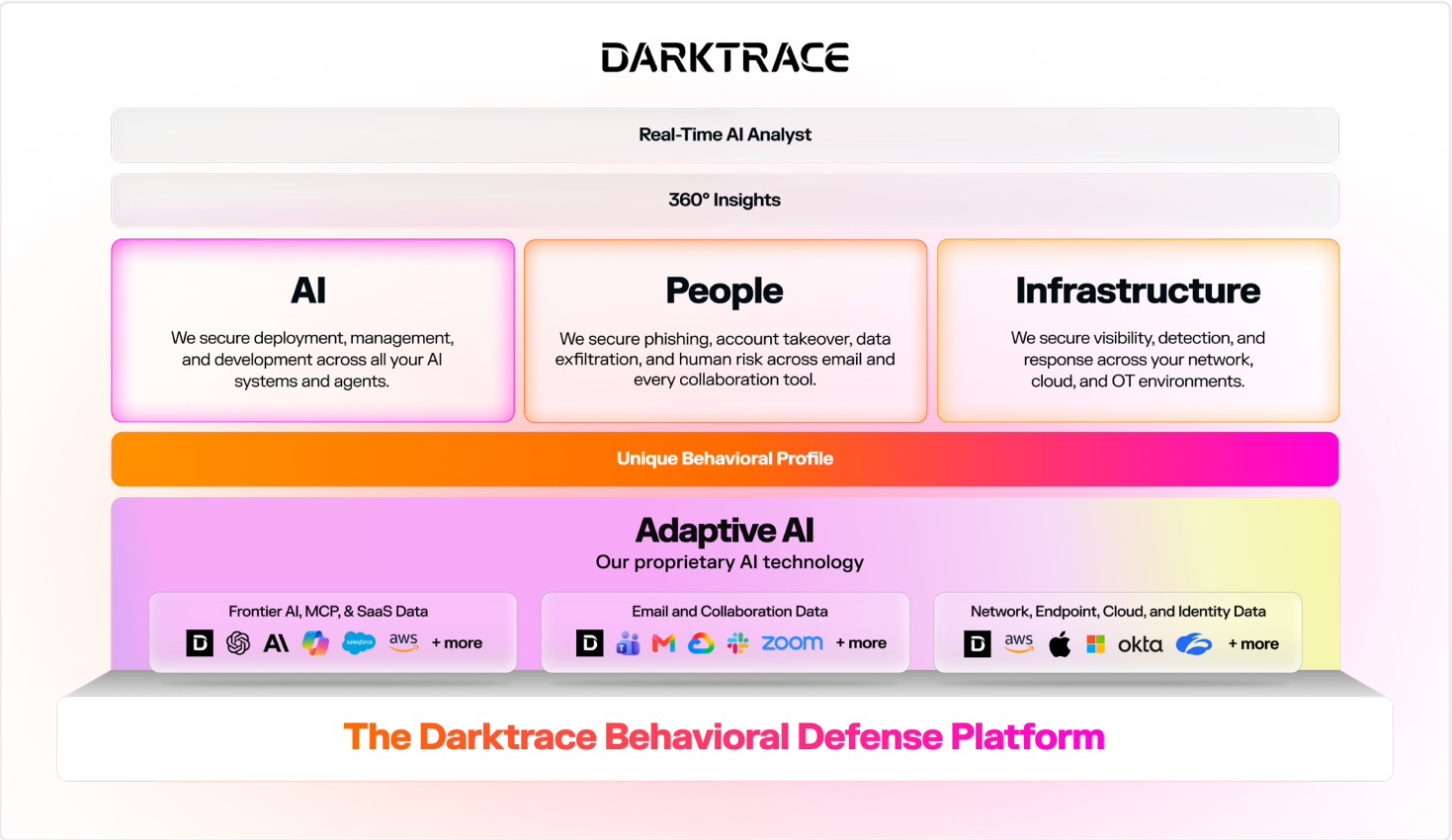
Darktrace / HYBRID NETWORK delivers a powerful end-to-end cloud detection, response, and investigation solution.

Darktrace / HYBRID NETWORK provides real-time visibility and detection of novel cloud-native threats, and Forensic Acquisition and Investigation instantly preserves and analyzes forensic evidence the moment an alert is raised.

This tight coupling ensures that every cloud alert, whether from Darktrace or third-party tools, is enriched with forensic depth and investigation timelines, transforming response from reactive triage into proactive, forensically sound decision-making.

This unified solution give security teams the ability to detect, stop, and investigate cloud threats in one seamless workflow.

Darktrace / HYBRID NETWORK extends its forensic acquisition and investigation capabilities across your entire digital estate with the Darktrace Behavioral Defense Platform. The platform correlates signals across networks, endpoints, identities, SaaS, and email to create a unified understanding of risk. Activity in one domain, such as an anomalous identity action or endpoint process, immediately informs forensic investigations in the cloud, and vice versa. This cross-domain intelligence enables faster detection, enriched context, and smarter autonomous actions, reducing complexity and human overhead.



■ **About Darktrace**

Darktrace secures the modern enterprise by protecting AI, people, and infrastructure with behavioral security. Founded in 2013, Darktrace uses Adaptive AI to understand what is normal for an organization and detect known, unknown and novel threats and respond autonomously in real time. The Darktrace Behavioral Defense Platform delivers unified visibility, continuous behavioral monitoring, and autonomous response across the enterprise. Darktrace protects nearly 10,000 customers across major industries globally, helping organizations defend AI-powered threats across AI and agents, email and collaboration tools, and hybrid networks, while enabling them to innovate with AI securely.