DARKTRACE

Automated Cloud Forensics Explained

Step into the modern era of cloud investigations

At a glance

Cloud investigations are mission-critical, but manual methods can’t keep up with cloud speed and complexity. This e-book explores the transformation from slow, manual investigations to automated workflows that reduce hours of manual work to minutes.

Cloud investigations are vital but increasingly difficult

Modern businesses run on distributed, dynamic cloud environments. Each workload, container, and microservice adds investigation complexity. Security teams need visibility across systems that evolve in real time.

Manual methods fail to capture short-lived workloads

Traditional methods, like manual log collection or VM snapshots, miss evidence when workloads disappear within minutes. Investigators are left with blind spots that attackers can exploit.

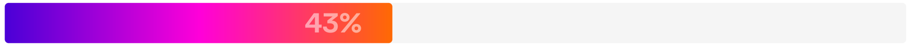
Automating cloud investigations will redefine cloud security

Manual investigations are slow, inconsistent, and labor-intensive. Automated forensics flips the script – evidence is captured instantly, workloads are analyzed at cloud speed, and hours of work shrink to minutes.

Cloud investigations are broken

89% of organizations suffer damage before containing and investigating incidents

Darktrace survey



43% of organizations have experienced significant damage from a cloud incident alert that didn’t get investigated.

Darktrace survey

> “ Ten years ago, breaches due to cloud misconfiguration weren’t even a categorized threat. Today, the cloud and the data in it are **a prime target.** “

IBM & Ponemon Institute Cost of a Data Breach 2025

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**.

The before scenario
Manual cloud investigations

Manual cloud investigations are slow, fragmented, and inefficient

Security teams spend most of their time collecting and stitching together evidence instead of analyzing threats. By the time the investigation is ready to begin, key evidence has often vanished, and attackers already have the upper hand.

The reality of manual investigations

Over 1/3 of cloud alerts are never investigated

ESG Report, Organizations Demand a New Approach to Digital Forensics

82% of organizations use multiple platforms and/or tools to perform forensic investigations

Darktrace survey

80% of investigation time is spent on collection and prep, not analysis

Mark Scanlon, Increasing Digital Investigator Availability

Alert triggered
SOC team receives an alert from monitoring tools.

Triage & assign
Case routed to an analyst; initial scoping begins.

Manual evidence collection
Logs, snapshots, and access records gathered by hand.
(Delay point)

Handoff between teams
Evidence passed to other teams/tools for enrichment.
(Delay point)

Data stitching
Spreadsheets/scripts used to correlate fragmented data.
(Delay point)

Evidence gaps discovered
Ephemeral workloads already vanished; blind spots remain.

Analysis begins
Hours/days later, SOC team starts reviewing the case.
(Major delay point)

Incident closed
Often rushed, incomplete, or too late to prevent damage.

Common pain points

Step-heavy, labor-intensive workflows

SOC teams follow dozens of manual steps to gather logs, snapshots, and access data – work that eats up time and drains resources.

Investigations take hours or days

Delays in collecting and correlating data give attackers critical lead time.

Multiple tools, constant handoffs

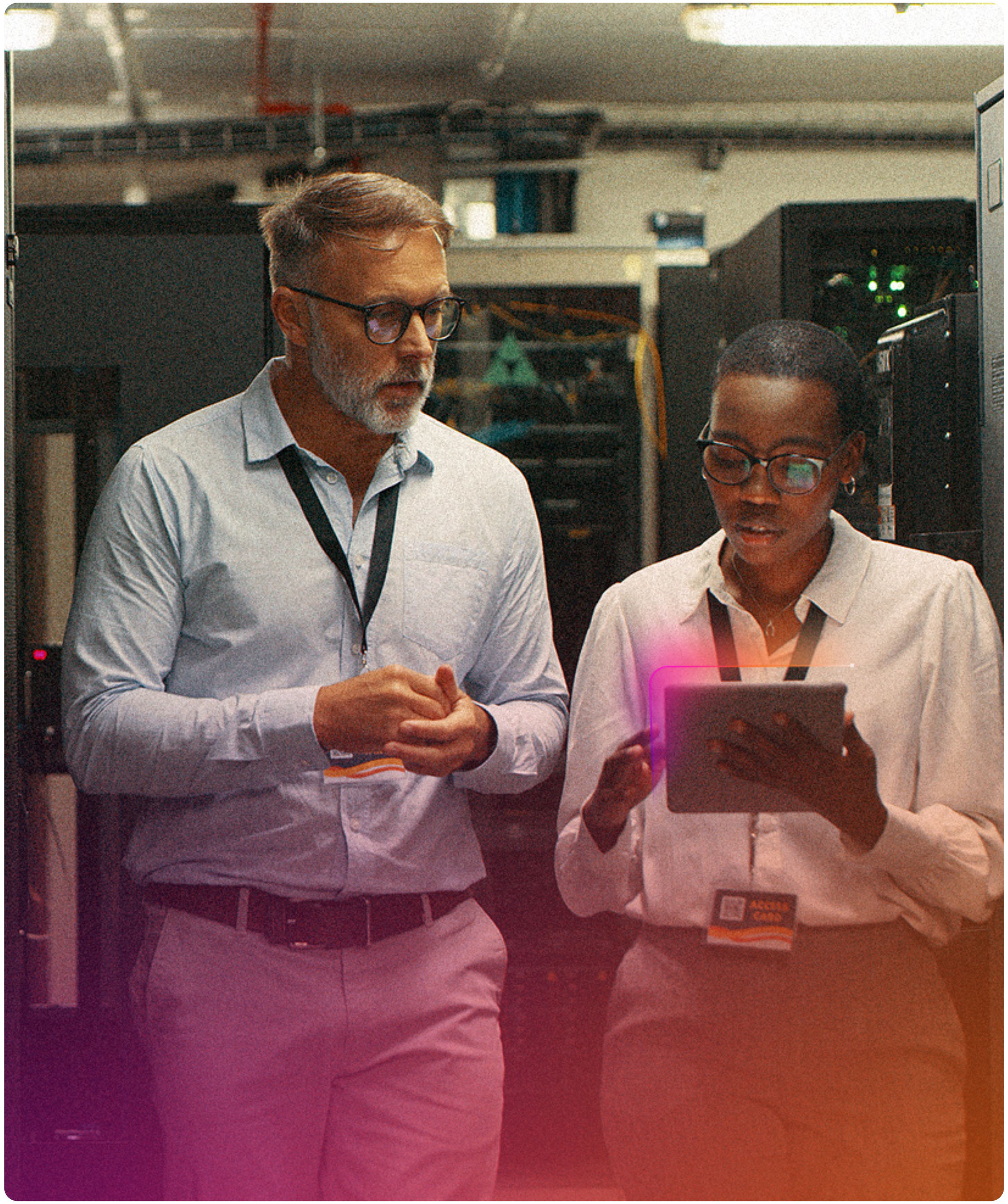
Analysts juggle spreadsheets, scripts, and point solutions, often passing cases between teams, slowing investigations even further.

Ephemeral workloads vanish before capture

Short-lived cloud instances disappear before evidence is collected, leaving blind spots in the investigation.

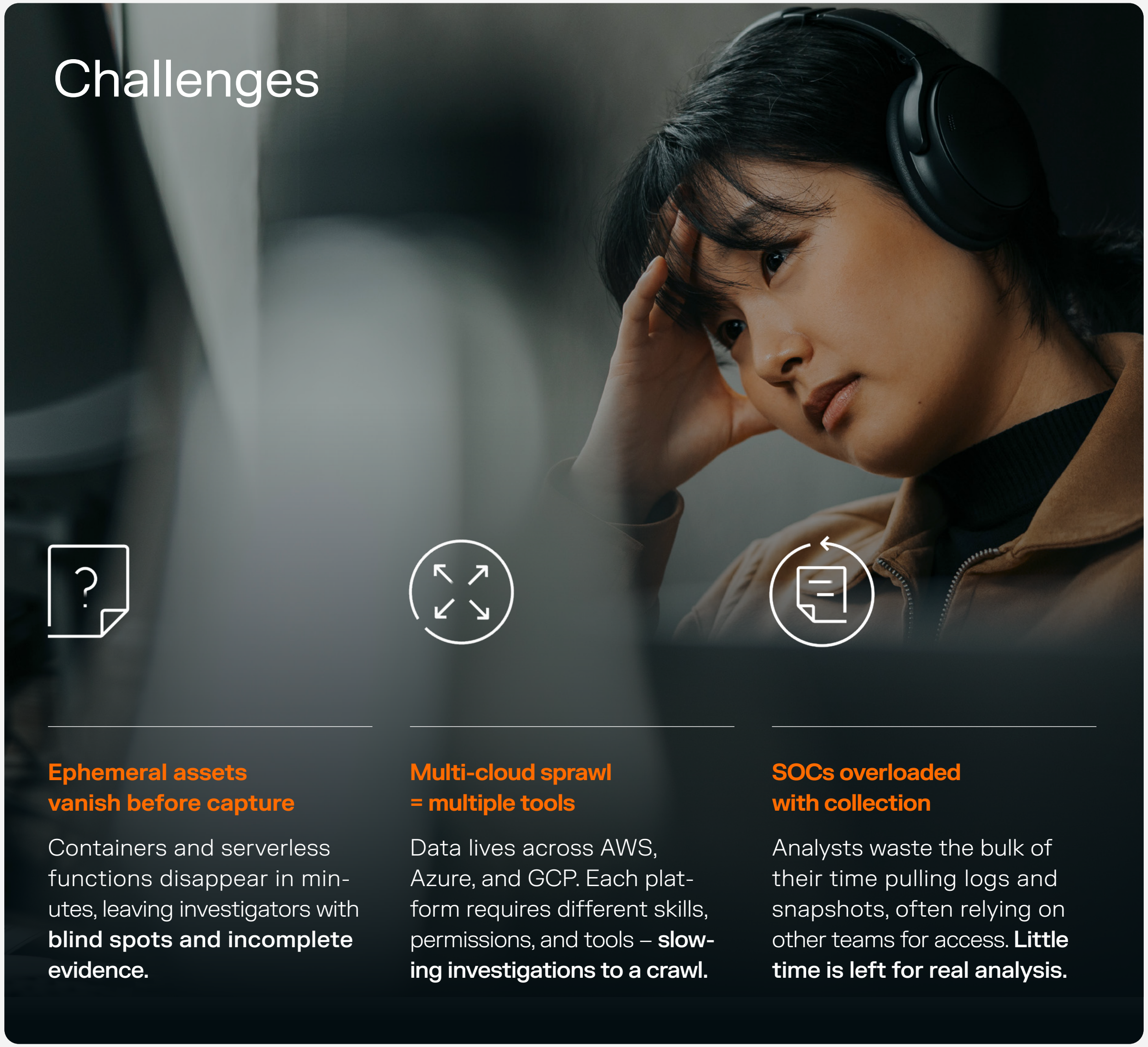
65% of organizations spend approximately 3-5 days longer when investigating something in the cloud vs on-prem

Darktrace survey



The breaking point

Why traditional methods fail in the cloud



Challenges

Ephemeral assets vanish before capture

Containers and serverless functions disappear in minutes, leaving investigators with **blind spots and incomplete evidence.**

Multi-cloud sprawl = multiple tools

Data lives across AWS, Azure, and GCP. Each platform requires different skills, permissions, and tools – **slowing investigations to a crawl.**

SOCs overloaded with collection

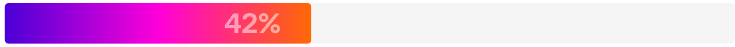
Analysts waste the bulk of their time pulling logs and snapshots, often relying on other teams for access. **Little time is left for real analysis.**

Cloud complexity and ephemeral workloads make traditional investigations extremely difficult and time consuming. Evidence is lost, SOC teams are overburdened, and attacks move too quickly for manual processes.

The cost of traditional methods

- Investigating ransomware lateral movement in AWS can take **10+ manual steps** before analysis even begins.
- The cloud forensics market is projected to grow **~16% CAGR**—a direct reflection of these mounting challenges.

Source: PMC Research



42% of organizations report that the main compliance challenge beyond cloud adoption is the lack of visibility into data

The result?

Investigations are too slow, too fragmented, and too resource-intensive to keep pace with the cloud – pushing security teams to the breaking point.

The after scenario
Automated forensic acquisition & investigation

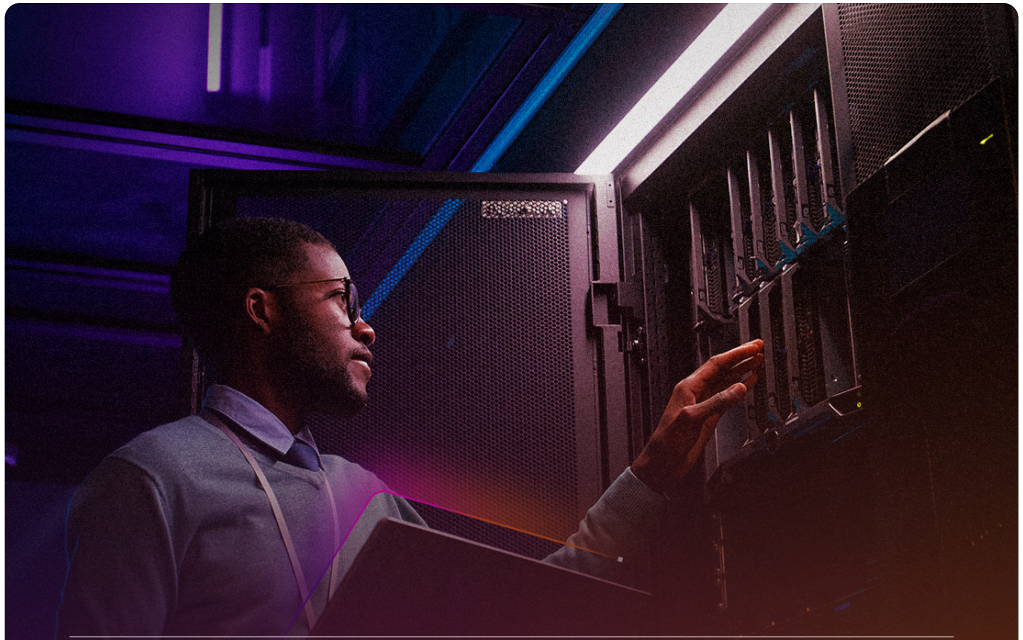
From days to minutes

Automation changes the equation for cloud investigations: evidence is captured instantly, timelines are automatically reconstructed, and investigations start in minutes, not hours.

Evidence preserved at detection
Ephemeral workloads no longer vanish. Automation captures memory, logs, and snapshots instantly.

Attacker timelines auto-generated with context
Tools reconstruct what happened with built-in context, giving analysts clarity from the start.

Workflow cut from 15+ steps to 2–3 streamlined steps
Manual collection, handoffs, and stitching are eliminated. Analysts can move directly to investigation and response.



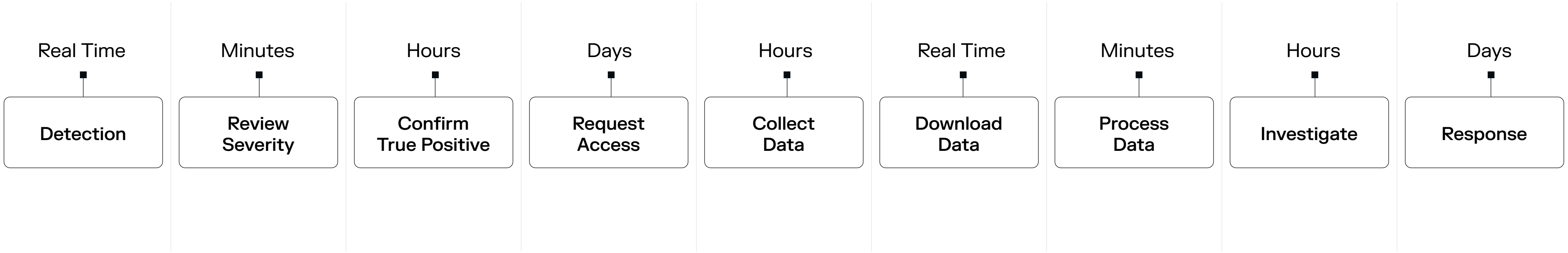
6x

Forensics investigations are up to 6x faster with Darktrace / Forensic Acquisition & Investigation when compared with a leading digital forensics product

Internal research

Before

Days and Manual



Real Time — Detection

Minutes — Review Severity

Hours — Confirm True Positive

Days — Request Access

Hours — Collect Data

Real Time — Download Data

Minutes — Process Data

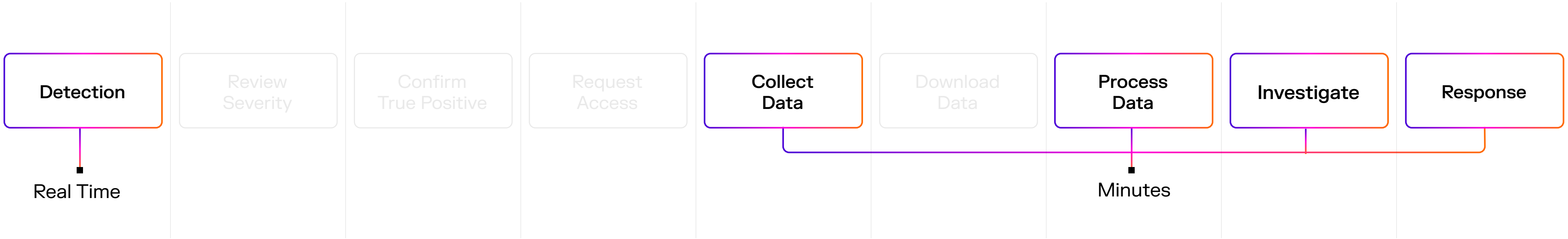
Hours — Investigate

Days — Response

Traditional investigation methodology

After

Minutes and Automated



Detection — Real Time

Review Severity

Confirm True Positive

Request Access

Collect Data

Download Data

Process Data

Investigate

Response

Collect Data, Process Data, Investigate, Response — Minutes

Darktrace / Forensic Acquisition & Investigation

Business impact
What this means for the SOC

Automation transforms how SOC teams spend their time. Instead of wasting hours collecting and stitching evidence, analysts can focus on high-value work.

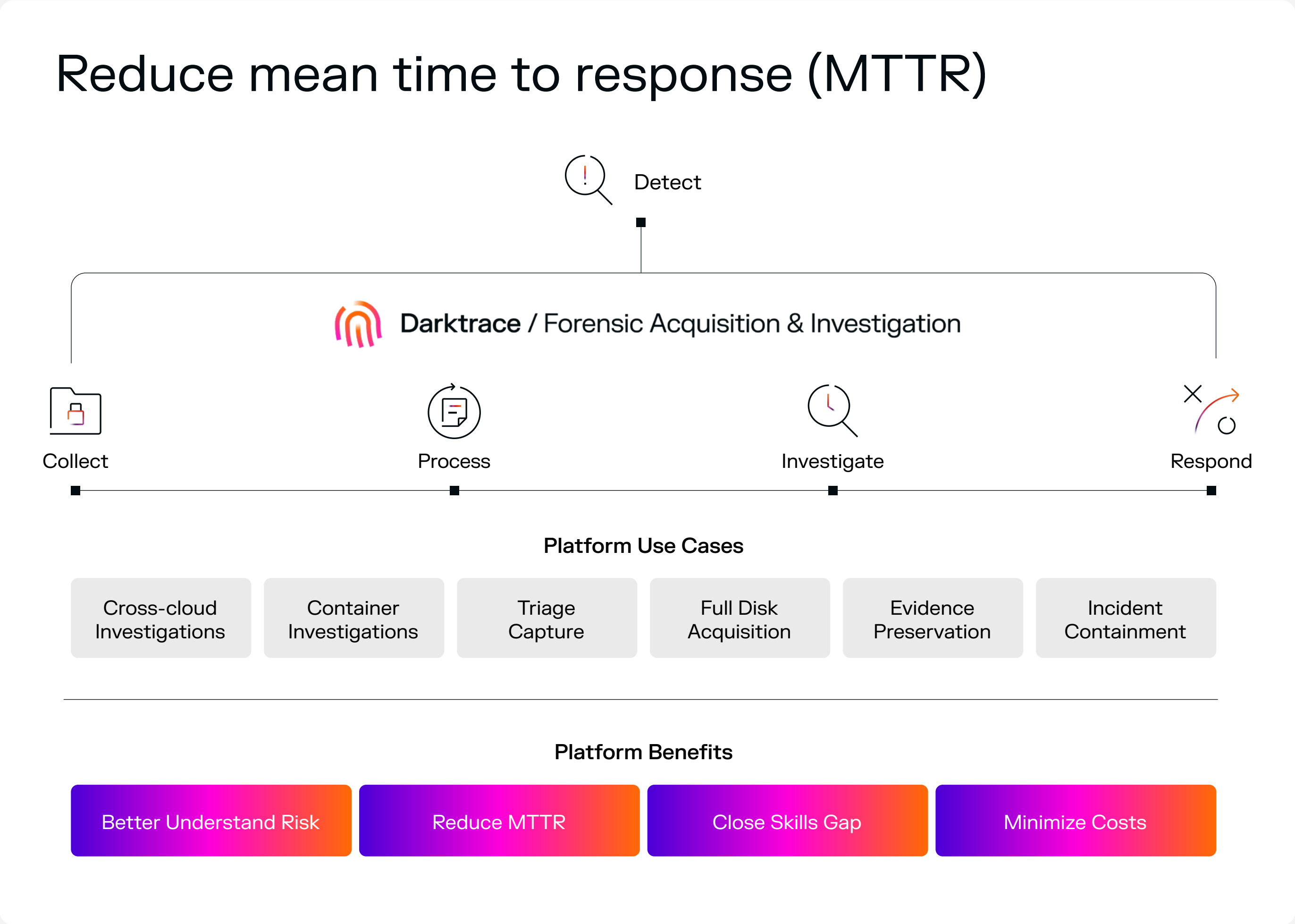
The result is better visibility, faster action, and more confidence in decision-making.

Key benefits

Time savings
Analysts shift from manual data wrangling to real-time response.

Visibility
Ephemeral workloads and fleeting evidence are preserved automatically.

Confidence
Complete attacker timelines reconstructed to provide clarity for quick, defensible decisions.



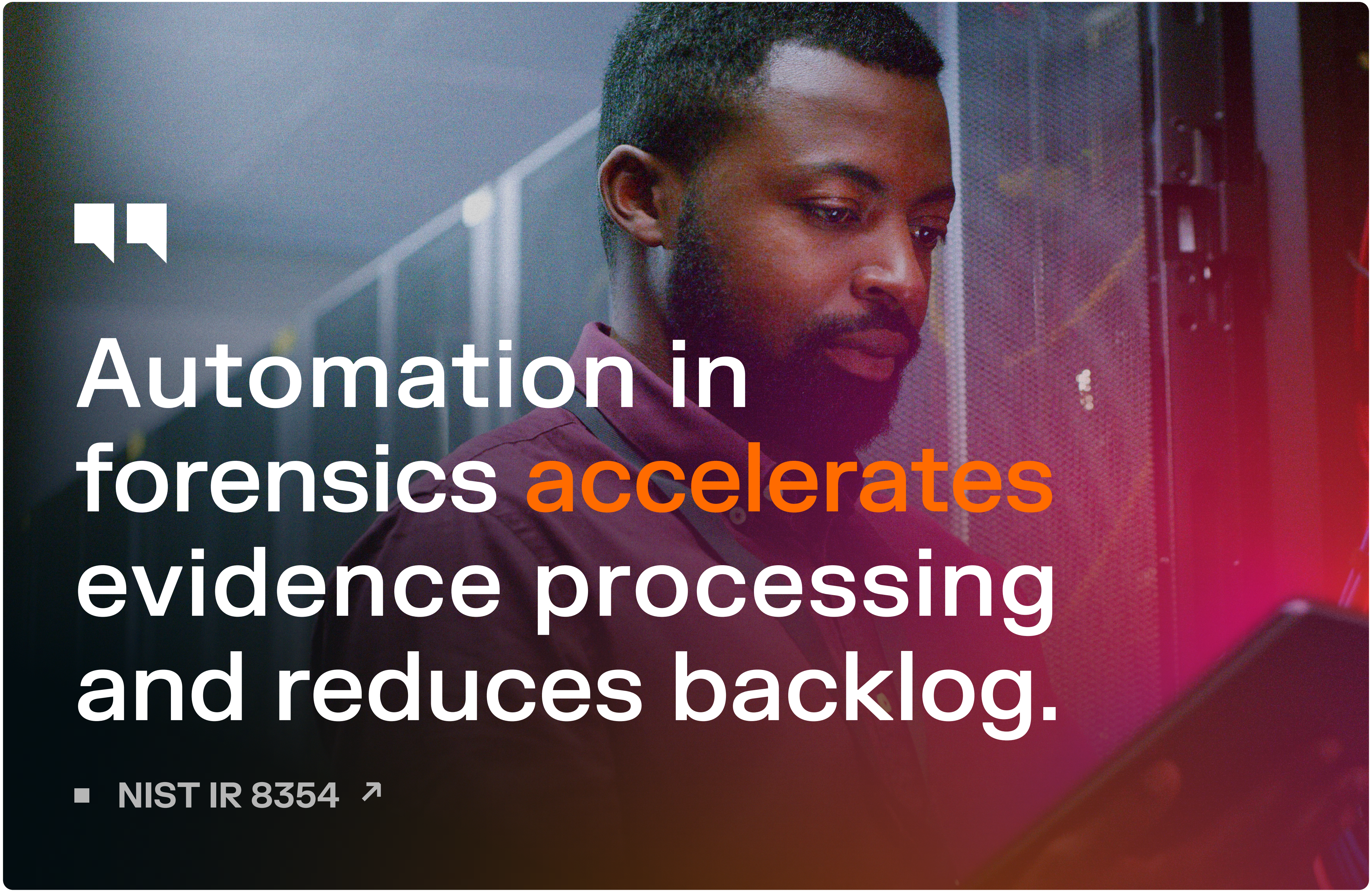
Reduce mean time to response (MTTR)

Platform Use Cases

Cross-cloud Investigations · Container Investigations · Triage Capture · Full Disk Acquisition · Evidence Preservation · Incident Containment

Platform Benefits

Better Understand Risk · Reduce MTTR · Close Skills Gap · Minimize Costs



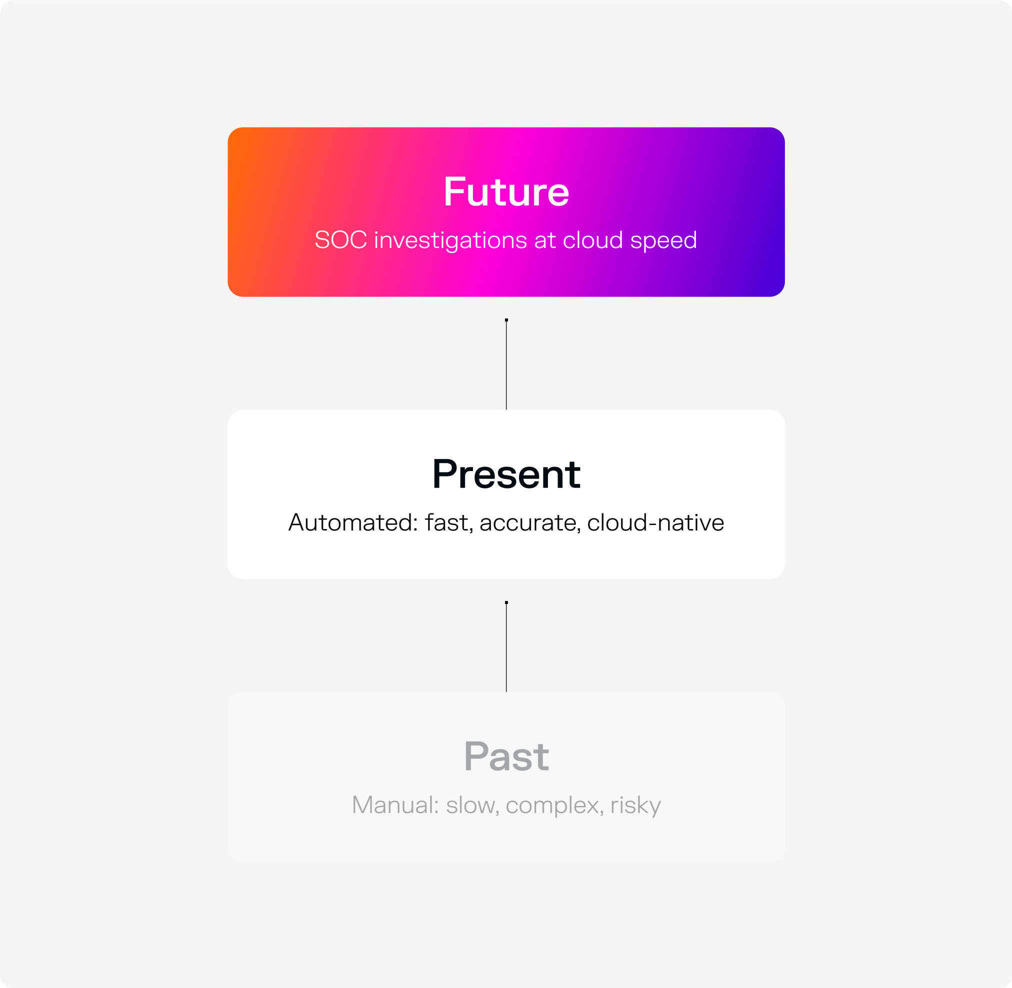
> Automation in forensics accelerates evidence processing and reduces backlog.

■ NIST IR 8354 ↗

Automated forensics, purpose-built for the cloud

In short, manual forensics are too slow for the cloud. Only automation delivers investigations at cloud speed – capturing ephemeral evidence, generating attacker timelines, and empowering security teams to respond faster than ever before.

Cloud threats move fast, your investigations should move faster.
Welcome to the next frontier in cloud security.



Future

SOC investigations at cloud speed

Present

Automated: fast, accurate, cloud-native

Past

Manual: slow, complex, risky

Let's recap the benefits.

Better risk management
Effortlessly gain forensic-level depth and context to understand threats.

Faster response times
Streamline every step—from capture to analysis—cutting hours to minutes.

Close the skills gap
Automation removes complexity, enabling every analyst to investigate like an expert.

Reduce costs
Minimize reliance on external services by bringing cloud forensics in-house.

Check out

Darktrace Forensic Acquisition & Investigation Solution Brief

Download brief ↗

Get a demo

in your cloud environment

Book a demo ↗