DARKTRACE

Enhancing Network Investigations with Deep Endpoint Context

Extend network detection and response with automated forensic investigation and deep endpoint context to move from detection to root cause faster, more efficiently, and with greater confidence.

The investigation gap in modern security operations

Despite significant investment in detection technologies, security teams continue to face a critical gap: **understanding attacks quickly and completely.**

Network detection and response (NDR) solutions provide early visibility into anomalous behavior, while endpoint detection and response (EDR/XDR) tools offer device-level telemetry to better understand why and what is happening inside the device. However, these capabilities remain siloed, requiring manual correlation across tools to reconstruct an attack.

This challenge is amplified in hybrid environments, where visibility is inconsistent, and traditional tools struggle to provide deep forensic insight without added complexity or disruption.

Extending network detection to fully automated investigation

By integrating Darktrace / NETWORK and / Forensic Acquisition & Investigation, teams move beyond isolated alerts to an **evidence-based understanding of attacks.**

Combining network intelligence with deep forensic endpoint context and AI-driven analysis creates a unified investigation layer that connects detection directly to root cause, without adding complexity to the security stack. When anomalous activity is identified at the network layer, an investigation is automatically initiated and enriched with forensic data collected from impacted systems via Darktrace / ENDPOINT or third-party EDR/XDR platforms.

This data enhances the complete incident analysis provided by Cyber AI Analyst with additional depth, speed, and operational efficiency.

At a Glance

Instantly initiate forensic investigation workflows directly from high-fidelity network alerts, eliminating delays between detection and analysis.

Collect high-fidelity forensic evidence, including process, file, and system activity without deploying additional agents.

Automate the collection of device-level telemetry and full attack timeline reconstruction to improve operational efficiency at scale.

Embed forensic investigation directly into current workflows, enabling SOC and incident response teams to operate within a single, unified environment.

Analyze multiple systems simultaneously across on-prem and hybrid infrastructures, increasing investigation capacity without increasing analyst workload.

Safely collect forensic data from contained or protected endpoints without disrupting security controls or introducing additional risk.

Seamless integration with existing security investments

Unlike traditional workflows that require manual pivoting across tools and teams, this integrated approach enables security teams to move from alert to full understanding **within a single, unified workflow.**

This approach is designed to enhance, not replace, existing tools:

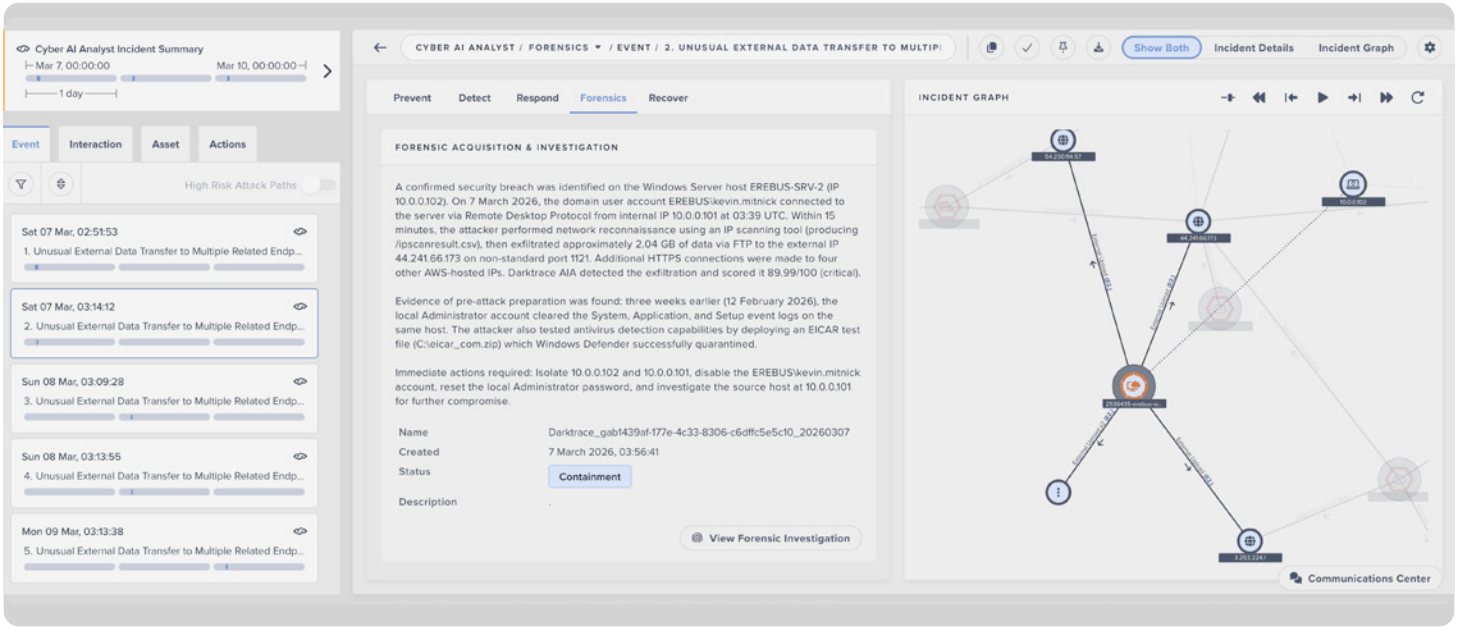
- **Integrates** directly with EDR/XDR platforms to collect forensic data
- **Preserves** existing containment and response workflows
- **Operates** without requiring additional agents or deployment overhead
- **Extends** the value of current investments by adding investigation depth and context

Moving from detection to root cause with confidence

Automated investigations are fueling faster outcomes with complete clarity throughout the end-to-end investigation process, which now takes teams from alert to understanding in minutes **compared to days or even weeks.**

The result is an incident response lifecycle that finally matches the reality of modern infrastructure:

- **Unified** investigations across hybrid infrastructure and a heterogeneous security stack
- **Consistent** forensic depth regardless of asset type
- **Faster** and more accurate root-cause analysis
- **Stronger** incident response readiness
- **Scalable** investigation across hybrid environments



Cyber AI Analyst™ investigation summary combines network and endpoint context with automated investigation and root cause analysis.

SEE HOW DARKTRACE HANDLES THREATS IN ACTION.

Read our 2026 threat report ↗

Request a demo ↗