binalyze!

Forensic-driven, AI-augmented Investigation and Response Automation

Instant Forensic Insights | **Conclusive Answers** | **Stronger Response**

Forensic clarity is the foundation of Binalyze's Automated Investigation and Response (AIR) Platform. Today's cybersecurity teams require rapid, conclusive answers that only forensic evidence delivers. AIR provides deep forensic visibility at speed and scale, making investigations clear and actionable without traditional complexity.

By turning forensic data into investigative momentum, AIR enables faster decisions and collaborative progress. Intelligent automation, embedded expert-level AI, and a full suite of investigative tools — including evidence collectors and analyzers, timelining, remote shell, and forensic comparison capabilities — support both post-breach investigations and proactive threat hunting to accelerate time to insight and strengthen overall security posture.

Overcome key investigation challenges

- Rapidly investigate compromised assets and scale investigations
- Collect forensic evidence across OSs, cloud workloads, and apps
- Empower analysts with built-in automation and expert-level AI
- Eliminate manual effort and shorten investigation dwell time
- Integrate seamlessly with your existing security stack to enrich alerts and enhance workflows
- Improve collaboration with consistent, streamlined investigation experiences

Rewriting the rules of response

AIR disrupts traditional investigation workflows. Instead of reactive, slow processes, AIR proactively combines forensic-level depth with intelligent automation, embedded AI, and built-in expertise. By eliminating bottlenecks that slow investigations, AIR accelerates root cause analysis and dramatically strengthens your response.

Forensic clarity at speed and scale

Gain deep, effective visibility across thousands of assets in minutes. AIR rapidly collects, processes and presents forensic evidence and historical artifacts from Windows, macOS, Linux, ESXi, and ChromeOS, and seamlessly integrates artifacts from cloud workloads into a single investigation view.

- → **Perform flexible remote targeted collections,** full-disk imaging, and offline acquisitions
- → **Maintain evidence integrity** with encryption, compression, and timestamping
- → **Effortless case management** through an integrated single-pane-of-glass interface

Analyst-empowering investigations

AIR automates repetitive tasks, enabling analysts to focus on high-impact investigative work. From initial triage to in-depth threat hunting, embedded expert-level AI and standardized workflows ensure, consistent and efficient investigations at scale.

- → **Trigger tasks on-demand,** scheduled, or via event-driven workflows
- → **Leverage Fleet AI,** AIR's embedded multi-agent assistant, providing specialized insights without replacing analyst judgment
- → **Accelerate triage, compromise assessments, and precision threat hunting** via YARA, Sigma, osquery scans and full-text search at scale

Enhanced workflows, seamless integration

Extend your security stack's capabilities with investigation-ready workflows. AIR integrates deeply with SIEM, EDR, XDR, SOAR, and ticketing systems, bringing forensic depth and investigative control.

- → **Instantly trigger forensic investigations** directly from your existing security platforms
- → **Customize integrations and automate workflows** using AIR's robust API and webhook framework, and MCP support
- → **Strengthen detection-to-response** with enriched context, centralized case management, and ready-to-use investigation data

Why Binalyze AIR?

Binalyze AIR revolutionizes investigation and response—transforming what traditionally takes days or even weeks into comprehensive investigations completed in just hours. With forensic-level visibility, intelligent automation, and embedded AI, AIR enables your team to achieve faster, more accurate decisions and dramatically strengthen your cyber resilience.

Visit us at: binalyze.ai