b!nalyze

AIR

Reimagining Incident Response

Binalyze AIR is a comprehensive Investigation and Automation Response platform that enterprises and MSSPs rely on to deepen their investigations and speed up incident response processes.

Binalyze AIR maximizes incident visibility by acquiring and investigating over 350 forensic evidence types in minutes with unrivaled coverage for on-premise networks and private/public cloud computing platforms.

Modern incident response teams face increasing challenges. Binalyze AIR eliminates or alleviates...

- Difficulties acquiring evidence at speed and scale
- Time–consuming root cause analysis processes
- Fragmented toolkit to identify, analyze and remediate
- Shortage of experienced DFIR professionals
- Alert noise and fatigue from other security systems
- Lack of complete and forensic level incident visibility
- Increasing volume, velocity, and sophistication of attacks
- Limited remote data acquisition and digital investigation capability
- Risk related to increasing dependence on cloud storage and services

Automated decision support

Binalyze AIR's Triage and DRONE features use proprietary analyzers, YARA, Sigma and osquery to scan assets and evidence. Uncover compromised assets and guide the IR team to the key evidence data quickly.

For rapid triage at scale, import YARA, Sigma and osquery rules or develop and validate new rules with the embedded rule editor.

Evidence–driven threat hunting

Binalyze AIR helps teams find the root cause of any cyber event by providing full forensic visibility and evidence in minutes for end–to–end threat hunting capability.

With scheduled and proactive compromise assessment features, enterprises and MSSPs can minimize the risks associated with attacks, decrease dwell time and improve security posture.

Accurate and fast incident response

Incident responders need fast, integrated, automated and actionable security data insights to keep up with today's cyber criminals.

With remote, accurate and scalable evidence acquisition, collaboration, automation and smart baseline acquisitions, Binalyze AIR unlocks the power of forensics. Thanks to AIR's forensic-level data, the modern SOC can fulfill its granular visibility requirements in various new use cases.

b!nalyze

AIR

Lightning fast evidence acquisition

Collecting digital forensic evidence from any asset on your network takes a few clicks and is completed in minutes.

- Windows, Linux, macOS, ChromeOS, ESXi & Cloud
- Acquisitions in minutes
- Remote and scalable
- Over 350 evidence types
- Compression, encryption & timestamping
- Scheduled evidence acquisition

Consolidated, efficient investigations

Comprehensive visibility and context to efficiently manage, progress and prioritize your investigation from a single pane of glass.

- Collaborative case overview across all assets
- Aggregate data from AIR and other sources
- Focus efforts with MITRE ATT&CK mapping
- Prioritize with intelligence-driven verdicts and scores
- Comprehensive event timelines
- Filter and search large data sets

Cut through the noise of cybersecurity data

Progress incident response investigations quickly and confidently with a full suite of capabilities.

- Live YARA, Sigma and osquery scanning
- Rapid keyword searches
- Event scoring
- Secure remote shell
- Auto asset tagging
- Baseline comparison

Automated and collaborative forensics

Work smarter, not harder. Eliminate low value manual tasks and make teamwork easy and consistent.

- SIEM, SOAR and EDR integrations
- 24/7 task triggering
- Webhooks and API integration
- Granular access control
- Incident timeline for full visibility

AIR covers Windows, Linux, macOS, ChromeOS, ESXi & Cloud

Binalyze is the developer of AIR, an innovative Investigation and Response Automation platform powered by digital forensics.

Binalyze empowers incident response and SOC teams to accelerate the time to close threat investigations with end-to-end investigation capabilities. AIR provides the powerful combination of forensic-level visibility, automation, alongside an easy to use, collaborative interface.

AIR delivers speed, efficiency, and accuracy that elevates the investigation experience and enables teams to more effectively and proactively respond to cybersecurity incidents improving response outcomes and bolstering cyber resilience.

AIR's suite of capabilities includes remote evidence acquisition and automated intelligence-driven evidence analyzers. Its core Triage, Timeline, and interACT remote shell features speed up investigation and remediation efforts. The AIR Investigation Hub sits at the heart of the platform to provide an integrated view of case-related evidence and insights to seamlessly and consistently manage investigations.