AIR

Enterprise Forensics Suite

b!nalyze

www.binalyze.com

AIR ENTERPRISE FORENSICS SUITE

Delivering Cyber Resilience with Enterprise Forensics

The exponential growth in the volume and velocity of attack vectors, the enterprise attack surface and the amount of data to be managed has led to an acknowledgement within enterprise cyber security that 100% breach prevention is no longer a realistic expectation.

These challenges are driving a trend towards blending traditional cyber security strategies with cyber resilience to ensure that, when a breach occurs, the organisation has the tactical tools in place for a fast and effective incident response.

Enterprise Forensics is a new category of digital forensics that is fast, remote and scalable across the corporate network and is pushing forensic readiness toward the centre of the security stack.

Binalyze is the leader and innovator in Enterprise Forensics solutions.

DIGITAL FORENSIC EVIDENCE ACQUISITION

Lightning Fast Evidence Acquisition

ACQUIRE

Get our FREE acquisition & case reporting tool from binalyze.com today.

Built on our proprietary IREC engine, collecting digital forensic evidence from any endpoint on your network is just a few clicks within the AIR management console, and is completed in minutes.

Acquisitions in minutes

Evidence acquisition is completed in under 10 minutes (average) instead of hours or days using traditional tools.

Remote & scaleable

Once deployed across your network, endpoint tasks and actions can be run concurrently and at scale.

Compression & encryption

Acquired evidence can be compressed to save storage resources and encrypted to AES-256 military-grade encryption standards.

Evidence respositories

Evidence can stored on the local machine, an attached removable drive, a network location, an SFTP server, SMB share or Cloud repository on Amazon or Azure.

Forensically sound

AIR's unique features ensure acquired evidence is timestamped and ransomware shielded to maintain forensic integrity.

Proactive posture

Make digital forensics proactive by scheduling evidence acquisition and triggering tasks from other security systems.

Windows 10

Windows XP and later

Linux

Debian / RPM versions

macOS

* Coming Q4 2021

COMPREHENSIVE CASE REPORTS

Structured, Complete & Simple-to-Share Case Report

Over 120 different evidence types, parsed and presented in a single report. AIR's case report is a self-contained HTML/JSON file that can be easily shared between analysts or with the client.

Custom evidence types

In addition to the 120+ evidence types collected, custom content profiles (path/pattern based) can be defined for specific evidence requirements.

Custom acquisition profiles

AIR provides granular control of evidence acquisition through the creation of unlimited acquisition profiles.

Report preparation & sharing

Individual events of interest within AIR's case report can be flagged as significant and provided as a PDF report.

65 evidence types

- System Evidence
- Disk Evidence
- Memory Evidence
- Browser Evidence
- NTFS Evidence
- Registry Evidence
- Network Evidence
- Event Logs Evidence
- WMI Evidence
- Process Execution Evidence
- Miscellaneous Evidence

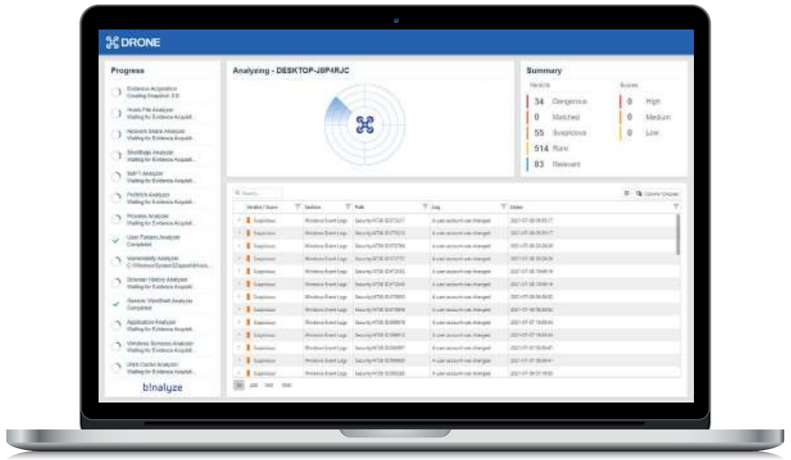
59 artifact types

- Server Artifacts
- Microsoft Applications Artifacts
- Communications Artifacts
- Social Artifacts
- Productivity Artifacts
- Utility Artifacts
- Developer Tools Artifacts
- Cloud Artifacts

TRIAGE WITH YARA

Remote Triage at Scale

Move seamlessly from forensic evidence acquisition findings to rapid Triage across your network directly from the AIR management console.



Search with YARA

Create or import YARA rules within the AIR platform and share them between analysts. Triage tasks can be sent to an endpoint in seconds to scan both memory and file system.

Rule builder & validator

AIR's YARA rule builder and validation features make YARA rule creation and management efficient and error-free.

Fast, concurrent scanning

From the AIR management console Triage can be performed remotely and at scale across multiple endpoints concurrently.

Auto Actions

When a Triage rule match is detected on the endpoint why wait to take action?

Our proprietary Auto Actions and interACT technology allow the remediation process to begin automatically to prevent unnecessary delays that extend the threat window, while also removing laborious and time consuming manual tasks.

Define the following actions from directly within your YARA rules...

- Isolate the machine
- Acquire evidence
- Create a timeline
- Dump a process
- Delete a file
- Run a command (interACT)
- Reboot
- Shut down

INVESTIGATION TIMELINES

Collaborative 1-click Timelines

Create comprehensive event timelines in a single click and just a few minutes. Expand the scope of your timeline as the investigation proceeds to reach the correct conclusions quicker.

Automated timelining

With a single click AIR creates a comprehensive timeline of a single or multiple endpoints in minutes.

Event flagging

Flag events of interest with a severity scale and collect flagged events for streamlined customer reporting.

Real time collaboration

Collaborate remotely and in real time with other analysts directly on the AIR platform.

Enrich with milestones

Add anecdotal evidence obtained during the investigation process i.e. HR intelligence, timings of real world events etc.

Import CSV data

Use AIR's 4-step, format agnostic CSV importer to enrich your timeline with mapped data from Cloud systems, firewall logs and much more.

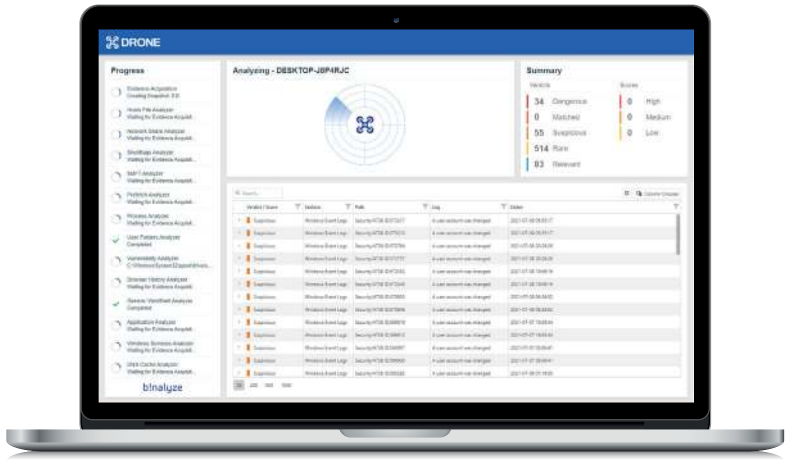
Add additional endpoints

Easily add additional endpoints to your timelines as your investigation progresses and lateral movement is identified.

INVESTIGATION AS A SERVICE

Compromise Assessment

Find the relevant events in your digital forensic evidence quicker and with less resources using DRONE, AIR's rapid, assisted compromise assessment module.



Modular forensic analysers

DRONE's modular architecture passes forensic evidence through a number of relevant analysers to find the anomalies for you.

Findings, verdict & scores

Our proprietary scoring algorithms deliver findings, verdicts and scores to guide your decision making processes and significantly speed up the investigation.

Live YARA & Sigma scanners

DRONE has embedded YARA scanning capabilities and, uniquely, Sigma scanning capabilities on the live endpoint.

Rapid keyword searching

DRONE's flexible keyword searching capabilities provide powerful compromise assessment in just a few minutes. Search for domains, IP addresses, file names, hashes and much more.

Enriched acquisition reports

In just a few minutes DRONE enriches the evidence acquisition report flagging events of interest on a scale of severity.

Zero config deployment

Rapid and simple zero config deployment directly from the AIR management console, over SCCM or manually on the endpoint as a standalone product.

INTEGRATIONS AND PARTNER ECOSYSTEM

Automated Forensics

With our flexible integration features you can automate your forensic digital evidence capabilities in minutes to deliver genuine enterprise-grade functionality.

SIEM, SOAR & EDR integrations

AIR support Splunk and QRadar SIEM solutions by default.

Webhooks integration

Simple and fast Integration with any service that is compatible with webhooks.

24/7 task triggering

Respond instantly to alerts and incidents regardless of the time of day or available analysts.

Innovating in Enterprise Forensics

Binalyze's Enterprise Forensics solutions are providing innovative new ways to incorporate digital forensics into the corporate security posture.

Critical asset scanning

AIR automatically identifies the critical assets on your network such as Domain Controllers, Mail & File Servers and Enterprise Application Management Servers.

Scheduled tasks

Perform scheduled and proactive forensic actions on your critical assets to identify any anomalies that may have gone unreported.

Diffing a golden image

Dramatically reduce evidence load and investigation time by diffing an endpoint against a golden image (Coming Q4'21).

ENTERPRISE FEATURES

Enterprise-grade Cyber Resilience Platform

AIR is an enterprise solution and has enterprise-grade features to facilitate its management in line with your corporate policies and security requirements.

Global policies

AIR has a system of cascading policy definitions. Global policies are created as defaults to define acquisition profiles, evidence repositories, CPU usage, and more.

Custom policies

Policies at the organisation, group or individual endpoint can be created where it is necessary to override the global policy.

Active directory

Integration with Active Directory automatically creates and maintains your organisational structure within AIR.

SSO & 2FA

Access to the AIR management console can be securely controlled using Single Sign On and 2 Factor Authentication.

Organisations

AIR's native Organisations feature allows for additional business structure definition and access management.

Users, roles & permissions

AIR includes a highly granular roles and users definition system, with more than 80 different variables, to tightly control access permissions throughout your security team.

Professional Services

Our professional services compliment your investment in the cyber resilience delivered by AIR to maximise your return on investment.

Assisted deployment

Our solution sales engineers can join your project team after procurement, using their experience and in-depth product knowledge to guide and inform the deployment and configuration phase.

Accredited training

We provide a number of training programs via our Future Forensics Academy to develop the investigation capability of your security analysts on the AIR platform.

Advanced SLA support

If you require advanced levels of support that meet a specific service level agreement, that is outside of our standard support, we can provide enhanced support services.

On premise & SaaS

AIR can be delivered as an On Premise (inc. offline), Private Cloud or SaaS based solution.

Lightweight, passive agent

AIR's endpoint agent is passive making it extremely lightweight on resource usage at just 0.01% CPU and 14MB RAM.

Auto backups

Configuration of backup locations and scheduling of auto-backups can all be configured in the AIR management console.

Auditing & Syslog integration

Extensive, tamper-proof audit logs are kept by the AIR platform locally and can also be integrated with your Syslog servers.

Endpoint isolation

AIR's endpoint isolation feature allows you to remotely isolate a machine from the network, in seconds, while still performing actions from the AIR management console (acquisition, triage, timeline etc).

Reboot & shut down

Endpoints can be remotely rebooted or shut down from the AIR management console.

Binalyze is the world’s fastest and most comprehensive enterprise forensics solution. Our software remotely, securely and automatically collects more than 120 digital forensic artifacts in under 10 minutes.

With evidence collected, our Timeline, Triage and Drone product modules help you analyse, collaborate and complete incident response investigations quickly to dramatically reduce dwell time.

Binalyze saves you time, reduces cyber security operational costs in your SOC and helps you prevent financial and reputational losses associated with cyber attacks.

Arrange a demonstration today online at www.binalyze.com

Binalyze OÜ
Narva mnt 5, 10117
Tallinn
Estonia

info@binalyze.com
www.binalyze.com