
AIR
Binalyze AIR
Product Datasheet
b!nalyze

AIR

Capture the “Forensic State” of an endpoint remotely in minutes!

Lightning fast, fully automated, all-in-one platform

Why do you need AIR?

Digital Forensics is 40 years old and the traditional method of “Cyber Incident Response” is not sufficient anymore!

Binalyze AIR is the most comprehensive solution in the market:

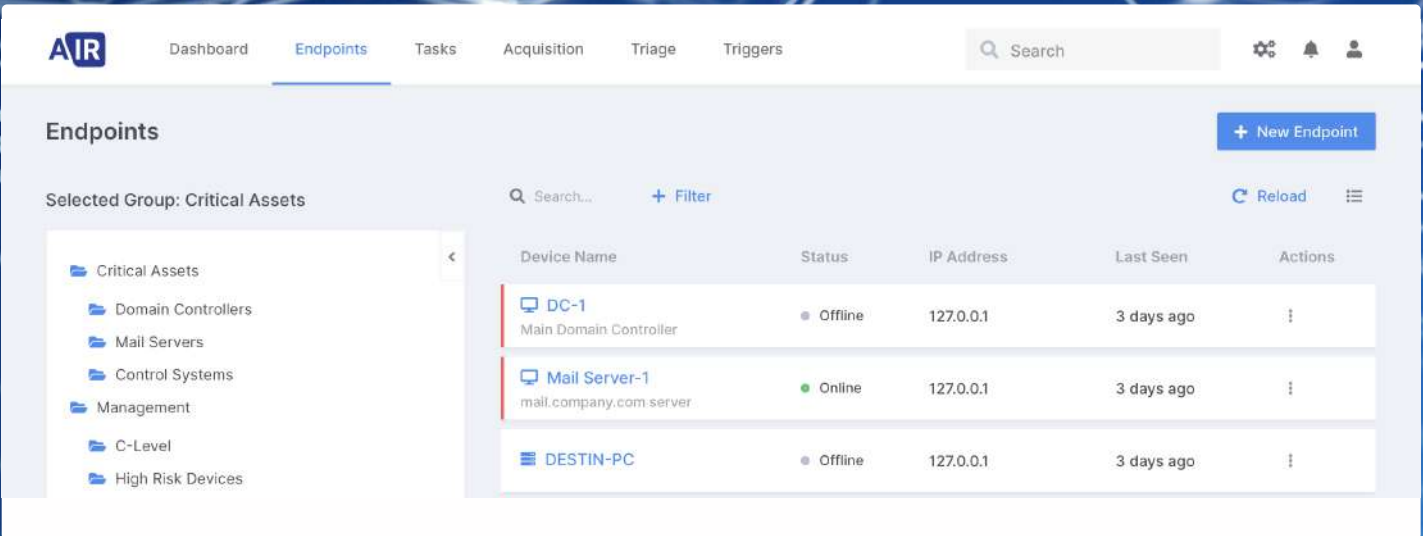
- Decreasing the response time from tens of hours to 5 minutes!
- Integrating with SIEM/SOAR/EDR solutions for automating the response,
- Capturing the “Forensic State” of an endpoint as an HTML file,
- Enriching the alerts you receive,
- Performing a large scale “Triage” using YARA.

100+
Evidence

5-10
Minutes

96x
Faster

> “360° Action Camera for Incident Response”



b!nalyze

Binalyze AIR at a glance

Remote Acquisition
Remotely acquire 100+ evidence type including RAM image, Event Logs, Browser History, and Application Artifacts with a single mouse click.

CASE Reports
Capture the forensic state of an endpoint as an easy to understand HTML report.

Scheduled Tasks
Schedule daily, weekly or monthly tasks for automatically acquiring evidence or performing triage on your critical assets.

Triage with YARA
Search YARA rules both in memory and file-system at scale.

RESTful Triggers for SIEM/SOAR
Easily integrate AIR into your existing SIEM/SOAR solutions with webhooks.

Acquisition Profiles
Create acquisition profiles based on your needs.

Compatible
Fully integrates with Active Directory and Syslog.

Use Cases

“Integrating with your SIEM for acquiring evidence in a fully automated manner.”

“Investigating CTI Alerts regarding stolen credentials being sold on Darkweb.”

“Validating pre-cursors received from your SIEM/EDR for determining false positives.”

“Capturing the forensic state of endpoint for further investigation.”

“Escalating the investigation by forwarding CASE reports to more experienced analysts.”

“Running SIGMA rules across the forensic state of an endpoint for compromise assessment.”

b!nalyze

Features

Evidence Types

- Clipboard Contents
- Crash Dump Information
- Recycle Bin
- System Restore Points
- System Drivers List
- Processes and Modules
- Window Screenshots
- Antivirus Information
- DNS Servers
- Proxy Lists
- Downloaded Files List
- Autoruns
- Prefetch Files
- Activities DB
- AmCache.hve
- RecentFileCache.bcf
- Jump Lists
- LNK Files
- Installed Applications
- Firewall Rules
- Volumes List
- Master Boot Record
- RAM Image
- Page File
- Swap File
- Hibernation File
- Browsing History
  IE, Chrome, Firefox, Opera
- $MFT (CSV and Binary)
- $MFTMirr
- Important Event Records
- Event Log Files
  Evt, Evtx, Etl
- Windows Index Search
- Superfetch
- WBEM
- Registry Hives
- Shellbags
- AppCompatCache
- DNS Cache
- TCP Table
- UDP Table
- ARP Table
- Routes Table
- Network Adapters
- Network Shares
- Hosts File
- WMI Scripts
- IconCache
- Powershell Logs
- ThumbCache
- SRUM Database
- INF Setup Logs

Application Artifacts

- Active Directory Logs
- Apache Logs
- DHCP Server Logs
- DNS Server Logs
- IIS Logs
- Microsoft Exchange Logs
- MongoDB Logs
- MSSQL Logs
- Cortana History
- Microsoft Calendar
- Microsoft Maps
- Microsoft Photos
- Microsoft Mail
- Microsoft Outlook
- Mozilla Thunderbird
- Skype Databases
- Skype Media
- Teamviewer Logs
- Whatsapp Desktop Cache
- Whatsapp Desktop Cookies
- Live Mail User Settings
- Zoom Databases
- Zoom Media Files
- Facebook Cache
- Evernote Databases
- Evernote Drag and Drop
- Evernote Logs
- Search Everything History
- Notepad++ Sessions
- OpenVPN Config Files
- Sublime Text Sessions
- iTunes Backups
- VMware Config
- VMware Drag and Drop
- VMware Logs
- VMware Config

Features (continued)

Application Artifacts (continued)

- Microsoft Sticky Notes
- Microsoft Store Apps List
- Microsoft Voice Record
- Start Menu Search History
- Notification History
- Discord Desktop Cache
- Google Drive DBs
- Linkedin Cache
- Spotify Cache
- Spotify Recently Played List
- Twitter Cache
- Twitter Databases
- Dropbox DBs, Logs, Cache
- Facebook DBs
- Github Desktop Cache
- Github Desktop DBs
- Github Desktop Logs
- Github Desktop Cache
- Tortoise Git Logs
- WSL Files
- Filezilla Sessions

Custom Content Collection

You can also create “Custom Acquisition Profiles” by providing wildcard patterns based on your needs.

Evidence Repositories

Collected evidence can be saved either
- Locally on the endpoint,
- A removable drive attached to the endpoint,
- A network share (evidence repository) protected with a username/password.

Triage with YARA at scale

- Create YARA rules with EditIR - an advanced rule editor for YARA with auto-complete support,
- Scan YARA rules accross your environment either in
  - File System
  - Memory
- Automatically perform actions on “matching” endpoints such as
  - Acquire Evidence
  - Shutdown the endpoint

Requirements and Deployment

Management Console

- Web based management console
- Windows 7 or a newer OS
- 4GB+ RAM
- 1GB Free Disk Space

Endpoints

- Supports both server and workstations
- Works on Windows XP to latest
- Ultra lightweight, **passive agent**
  - 8MB installer
  - 30MB run time memory footprint
- SCCM or manual deployment
- Can be deployed and uninstalled on demand

b!nalyze

Licensing

For Companies (1 to 3-years subscription)

	SMB Edition	Enterprise Edition	SOC Edition
◦ All Evidence Types	✓	✓	✓
◦ Application Artifacts		✓	✓
◦ Custom Content Collection		✓	✓
◦ Active Directory Integration		✓	✓
◦ Syslog Integration		✓	✓
◦ SIEM/SOAR Integration			✓
◦ Triage with YARA			✓

For Consultants / MSPs (15 to 45-days)

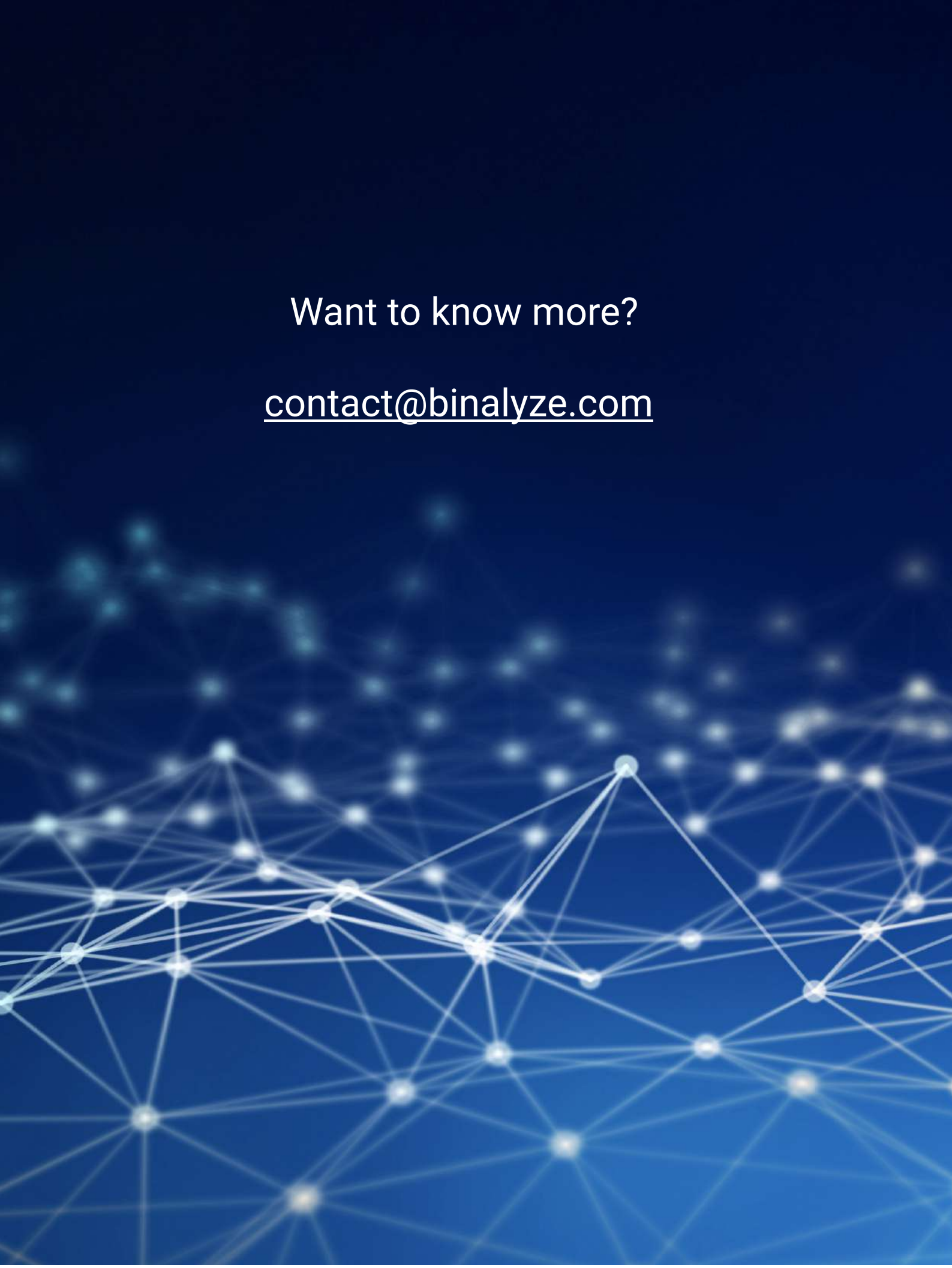
◦ Provides the exact same set of features with SOC Edition,
◦ Depending on the requirements of an investigation service provider could either choose:
  • 15-days license,
  • 45-days license.

Pricing

◦ Prices are calculated per endpoint and the minimum amount of endpoints is 50.
◦ Please contact sales@binalyze.com for further information.

Want to know more?

contact@binalyze.com



b!nalyze