binalyze!

BINALYZE FOR SECURITY SERVICE PROVIDERS

TURN INVESTIGATION INTO YOUR ADVANTAGE

THE PROBLEM

YOUR CUSTOMERS EXPECT ANSWERS. FASTER.

When a potential incident hits, customers don't just need to know that something happened. They need to know what happened, what was affected, and what to do next. Whether you're an MSSP, MDR provider or incident response firm, they need those answers quickly to meet the reporting demands of leadership, regulators, insurers and other stakeholders.

Yet thorough investigation has traditionally been difficult to deliver at the speed and scale incident response demands. Detection gives teams a place to start, but not the answers customers need. Fragmented tools, manual collection and analysis, complex workflows and scarce specialist time can force action before teams have the evidence-backed understanding to know exactly what happened.

THE PLATFORM

TURN BETTER INVESTIGATION INTO BETTER BUSINESS.

Binalyze AIR is a cloud-native, multi-tenant Investigation Platform that gives security service providers a forensic-grade investigation layer for delivering services across customer environments. Acquire, analyse, investigate and report — across Windows, macOS, Linux and cloud in a single platform, at scale.

01 ACQUIRE

Remote, targeted collection across hundreds of artefact types, chain of custody built in.

02 ANALYSE

Automated analysis with MITRE ATT&CK mapping and severity-ranked findings.

03 INVESTIGATE

One shared hub across thousands of assets, with per-tenant isolation.

04 REPORT

Client-ready findings for stakeholders, insurers and regulators.

WORK WITH THE TOOLS YOU ALREADY USE

Integrate AIR with the EDR, XDR, SIEM, SOAR and other security tools you already use to bring forensic-grade investigation into the workflows that power your services.

MOVE FASTER.

Streamline collection, analysis and investigation to get from incident to insight and reporting sooner.

INCREASE CAPACITY.

Reduce repetitive work and handle more investigations without scaling headcount at the same rate.

PROTECT MARGIN.

Reduce the operational effort surrounding every case and make valuable investigator time more productive.

STAND OUT & RETAIN.

Differentiate your services through speed, forensic depth and evidence-backed answers customers can trust.

PROVEN IN SERVICE DELIVERY

10× FASTER

Evidence acquisition and triage

Across entire estates.

1-4 HOURS

To key investigative findings

Deliver actionable findings to customers within hours, instead of days.

2× CUSTOMERS

With the same team

Deeper investigation at managed-service scale without doubling the team.

> ‘WITH BINALYZE, WE’RE NOW ABLE TO GO DEEP INTO INVESTIGATIONS AND, IN A SHORT TIME, GET TO THE POINT WHERE WE’RE TALKING ABOUT RECOVERY AND REMEDIATION. THAT’S REAL VALUE - FOR THE CUSTOMERS AND ACROSS THE BUSINESS.’

- EVP of Security Operations, Thrive

MORE WAYS TO DELIVER VALUE

ONE INVESTIGATION PLATFORM. MORE WAYS TO DELIVER VALUE.

Strengthen the Services You Deliver Today. Extend Them When You're Ready.

The same investigation foundation can support reactive response, proactive assurance and deeper managed security services, giving you more ways to create customer value and grow the relationship.

RESPOND

Accelerate incident response investigations without compromising the outcome.

Collect and analyze forensic-grade evidence across customer environments, investigate at scale, provide post-incident assurance, and get to the answers customers need faster.

Faster answers. Greater case capacity. Consistent delivery.

ASSURE

Turn point-in-time response into ongoing customer value and recurring revenue.

Extend the same investigation capability for proactive assessments at scale: compromise assessments, threat hunting, health checks and other proactive assurance services.

More assurance. More customer value. More revenue opportunities.

MANAGE

Bring depth to managed security investigations.

Add forensic-grade investigation to ongoing security operations, supporting deeper validation, investigation and smarter escalation when customers need more than an initial response.

Go beyond detection and containment when customers need answers.

BINALYZE ECOSYSTEM

AIR

With AIR providing the forensic-grade evidence that grounds investigations in what actually happened, Fleet and Outpost extend how teams put that capability to work.

FLEET AI

Binalyze's agentic investigator gives teams an AI-driven way to work through evidence, test hypotheses and accelerate investigations across customer environments — while keeping investigators in control.

OUTPOST

Binalyze's free browser extension brings live access to assets into the analyst's workflow, making it easy to pivot from alerts, reports, observables and other signals into deeper investigation with AIR — in seconds.

COMMERCIAL MODEL

BUILT FOR YOUR SERVICE MODEL

Your commercial model should work the way your services do. AIR offers three ways to consume the platform: from case-driven response and retained customers to continuous managed security.

	REACTIVE IR	RETAINER IR	MDR+
FOR	Reactive, case-driven incident response investigations	Retained customers requiring reactive and ongoing health and assurance services.	Service providers running continuous detection and response at scale.
BILLING MODEL	Base Licence + per case fee	Base Licence + per retainer customer fee	Per endpoint subscription
FLEET Binalyze Agentic Investigator	Add-on, per user fee	Add-on, per user fee	Add-on, per user fee
ASSET/SCOPE	Unlimited assets per case. Scale with the needs of the case over 30-day periods.	Pre-deployed across each retained customer's estate.	Per managed endpoint
SUPPORT	Included	Included	Included
MULTI-TENANT	**Included** Multi-tenant is included across every model — manage multiple customers, each with its own isolated entity, while benefiting from shared resources.		

CUSTOMER CASE STUDY

INVESTIGATION CAPABILITY THAT CAN BECOME A GROWTH ENGINE

Thrive already delivered MDR services, but serious incidents requiring deeper forensic investigation could mean escalating customers to external incident response providers.

With AIR, Thrive brought that investigation capability into its own service portfolio and launched an incident response retainer — now one of its fastest-growing services.

1-4 HOURS
To evidence-backed insights

99.9%
Of IR work completed in one investigative solution

UNDER NINE HOURS
From investigation to reporting in a ransomware case

Read all our customer stories.

WHY BINALYZE

Binalyze gives security service providers the investigation capability and capacity to deliver meaningful security services efficiently and at scale. Streamlined evidence acquisition, analysis and investigation workflows help teams reach answers faster, increase capacity and deliver consistently across customers — from reactive incidents to ongoing assurance and managed security.

More efficient investigation.
More capacity to deliver.
More value for your customers.

> ‘WITH AIR, WHEN AN INCIDENT HAPPENS, WE GET THE ANSWERS. IT’S AS SIMPLE AS THAT.’

Andrew Haslett, Director of Security Services, NovaWatch