binalyze!

From MDR to full-scale Incident Response

How Thrive powers faster, clearer investigations with Binalyze AIR.

Company overview

Thrive is a leading provider of NextGen managed services, delivering secure, scalable, and innovative solutions to small and mid-sized organizations. With a dedicated 24/7/365 Security Operations Center (SOC), Thrive offers robust Threat Detection and Response services, including Managed Detection and Response (MDR) and Managed EDR, to ensure continuous protection and visibility. In addition to proactive monitoring, Thrive supports its customers with tailored incident response and remediation capabilities designed to minimize disruption and accelerate recovery.

Challenges

- Inconsistent customer experience when escalating to third-party DFIR firms
- Growing customer base and incident volumes requiring greater scale and speed
- Limited visibility into root cause using traditional SOC tools (SIEM/EDR)
- Tools that required analysts to work in silos, slowing response

From alerts to answers: the missing link in IR

As Thrive's 24x7 security offerings matured, so did customers' expectations. Having built strong relationships through its MDR services, Thrive increasingly found that customers wanted more than alerting—they wanted answers. Fast.

Previously, when serious incidents occurred, Thrive's SOC would escalate and hand off cases to their customer's third-party DFIR provider. While this approach could get results, it often introduced delays and fragmented the customer experience. The Thrive team, who already understood the customer's environment intimately, had to step aside while an external team started from scratch.

"Our engineers knew the customer environment, their users, their pain points," said Kevin Landt, VP of Product Management at Thrive. "But once a third-party DFIR provider stepped in, valuable time was lost—and that's when customers need clarity most."

Thrive's SOC leveraged powerful detection tooling like EDR and SIEM platforms to support its MDR services. These tools offered high value in alerting and monitoring, but lacked the forensic depth needed to answer key questions—like how an attacker got in, what they did, and how far they moved. They weren't designed for evidence collection or deep investigation at scale.

"We could tell a customer there was malware on a system," said Christopher Clark, Incident Response Team Manager. "But if they asked how it got there, there were times when we could not supply a complete answer with only the logs in our SIEM or EDR."

Clark added, "We do use those tools, but they only give part of the picture. You don't get things like ShimCache or AmCache, or the ability to prove execution on a system or see what files were accessed. They provide a limited data set."

Customer
Thrive

Industry
Next-Gen MSP/MSSP

Region
Global, multiple locations across the US, UK, Canada, Australia, and Asia.

Founded
2000

Employees
1,001-5,000 employees

Headquarters:
Foxborough, MA, USA

Website
https://thrivenextgen.com

Success Highlights:

- **Key findings provided** to customers within 1-4 hours
- **Ransomware case completed** with reporting in under 9 hours
- **Operations restored** across 5 sites over a single weekend
- **99.9% of IR work done** in single investigative solution
- **IR retainer now** among fastest-growing services

It became clear that Thrive could close that gap. As demand grew, the leadership team quickly realized they needed tooling that could help them own more of the investigation process—faster, and at scale. They explored open-source and commercial platforms, but many came with trade-offs: steep learning curves, slower time to value, and workflows that forced analysts to work in isolation.

Building a faster, smarter response capability

With a clear goal to close the investigation gap and deliver a more seamless experience for customers, Thrive launched its Incident Response Retainer—an add-on service for existing managed customers. Designed to extend their 24x7 security operations with complete response services powered by Binalyze AIR.

The team uses AIR to collect artifacts, create and assess timelines, identify indicators of compromise, and conduct detailed triage and threat hunting across impacted systems. AIR's unified Investigation Hub brings the entire workflow—detection, analysis, and reporting—into a single interface. This has helped Thrive streamline investigations, accelerate time to insight, and elevate the consistency and quality of reporting delivered to customers.

"We're often able to provide key findings within an hour," said Clark. "Even with customers who aren't pre-deployed, we're usually delivering solid insights within four hours." This speed allows Thrive to de-escalate tense situations quickly—often well before third-party DFIR providers, brought in by customers as part of their cyber insurance policies, begin their work.

One of AIR's standout capabilities is its ability to surface conclusive evidence that enables the team to validate execution, trace attacker movement, and confidently report findings. Thrive also makes extensive use of AIR's Triage engine to extend investigations—applying custom rules based on threat intelligence and case-specific indicators to hunt across systems and close out any lingering gaps.

"Our findings have stood up to review by third-party forensics teams," Clark explained. "In some cases—especially when insurers are involved and bring in their own DFIR vendor—those teams have reviewed our collections and chosen to use them rather than start over."

AIR's remote shell capability, interACT, is another critical feature. Thrive uses it frequently for post-compromise access, particularly when adversaries have changed credentials or restricted normal access. It's become an essential tool for conducting AD audits, executing tools, and regaining visibility in compromised environments.

Thrive's use of AIR has powered successful outcomes across a wide range of incidents, enabling quicker investigations, stronger reporting, and more resilient responses."

Use Case: Ransomware recovery across five sites before Monday morning

A customer with existing managed services was hit by ransomware early Friday morning. Thrive responded immediately, delivering critical insights within two hours, including confirmation on data exposure. By 6 PM the same day, the team had built a complete attack timeline and shared findings with the customers and their insurer.

The third-party DFIR provider ultimately relied on Thrive's collections, validating their accuracy and skipping redeployment of their own tools. With coordinated effort and deep visibility from Binalyze AIR, Thrive helped the customers restore operations across five sites before the start of the business week—reducing a potential week-long outage to just days.

Use Case: Rapid ransomware response for a Midwest credit union

When a small federal credit union with a single-person IT team was hit by ransomware, Thrive moved quickly to contain the threat. Artifact collection was completed within 15 minutes of notification, and full incident reporting was delivered in under 9 hours. Using Binalyze AIR, Thrive investigated 99 systems with complete coverage and surfaced the forensic insights needed to support both remediation and regulatory response. The case was successfully transitioned to a third-party IR firm using Thrive's structured reporting—streamlining coordination and compliance under pressure.

Use Case: Proactive onboarding reveals hidden ransomware

During the onboarding process for a new customer, Thrive used Binalyze AIR to run an initial compromise assessment across the environment. While validating connectivity and readiness, the team also uncovered artifacts from a ransomware incident that had occurred years prior—unknown to both the current IT leadership and the customer's security team. By surfacing these dormant indicators of compromise, Thrive helped the customers understand and address a lingering threat, closing a critical visibility gap that had persisted undetected through previous tooling and handovers. With Binalyze AIR's automated triage, Thrive can now efficiently deliver these in-depth assessments as part of onboarding for all Incident Response Retainer customers—providing proactive visibility that was previously out of reach due to time constraints.

Outcomes: From deep investigations to faster recovery

Binalyze AIR has transformed how Thrive delivers incident response. AIR empowers the team to investigate more thoroughly, respond faster and operate with greater assurance.

For customers, the difference is immediate: faster answers, clearer communication, and reduced downtime. Thrive now delivers key findings within hours of an incident, compressing timelines that previously stretched into days—especially in cases involving external DFIR providers. Clark explained, they're "not just telling customers there's a problem—we're showing them exactly what happened, how it happened, and what to do next."

That clarity accelerates the path to recovery. AIR helps Thrive move swiftly from investigation to remediation, arming customers with conclusive evidence and structured reports that streamline communication with legal, compliance, and insurance teams. EVP of Security Operations at Thrive, Audy Bautista, shared that they'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."

Internally, AIR has also allowed Thrive to scale more efficiently. The success of the IR Retainer has expanded the company's footprint with existing customers and unlocked new growth opportunities. What started as a capability gap has become one of Thrive's fastest-growing service lines. "This has been one of our most successful launches," said Landt. "Our customers remember how we showed up when it mattered most."

> **"This has been one of our most successful launches," said Landt. "Our customers remember how we showed up when it mattered most."**

Conclusion

Thrive's partnership with Binalyze has redefined how incident response is delivered at scale, delivering conclusive analysis and rapid execution to meet the demands of today's customers. With AIR embedded in its IR Retainer, Thrive has turned a critical capability gap into a high-growth service line that's delighting customers and driving business momentum.

"Our team continues to be better prepared, faster, and more effective," said Bautista.

> **'Our SIEM and EDR give us alerts and telemetry, but Binalyze AIR gives us visibility. With AIR, we get the full picture—what executed, what moved, what was accessed—and that's what helps us close investigations with confidence.'**
>
> – Christopher Clark, Incident Response Team Manager

Use Case: Working with Cyber Insurance Companies

Thrive's incident response team regularly works alongside third-party forensics firms brought in by their customers' cyber insurance providers. In many cases, these teams have validated the completeness and quality of Thrive's investigations—sometimes even opting to rely on Thrive's AIR-based collections instead of redeploying their own tools.

This growing trust is a testament to the maturity of Thrive's processes and the depth of forensic insight delivered through AIR. While third-party engagement is often required by insurers, these teams can typically take 24 to 72 hours to onboard, deploy tooling, and begin collection. In contrast, Thrive is already in the environment—often delivering key findings within the first hour. That head start provides customers with faster clarity and helps guide early decisions while maintaining full alignment with insurer processes. For customers, this dual support structure offers the best of both worlds: insurance compliance backed by validated forensic reporting, and a trusted response partner who can act immediately to limit disruption and begin the recovery journey.