binalyze!

novawatch

Fast, Forensic-Driven MDR at Scale

Novawatch accelerates investigations and response with Binalyze AIR

Company overview

Novawatch is a U.S.-based Managed Detection and Response (MDR) provider offering 24/7/365 monitoring, investigation, and threat detection services through a vendor-flexible approach. Their MXDR model is built to extend the reach of security operations across networks, endpoints, and cloud infrastructure—supporting organizations that may not have large internal security teams but still expect high-touch support and rapid response.

Challenges

- Four to six hours per endpoint to gather the right data
- Visibility gaps beyond SIEM and EDR
- Hard to confirm threats or impact
- Unable to scale investigation
- Lacked structured forensic workflows
- Quickly overloaded during incidents

Scaling investigations, not complexity

As Novawatch's client base expanded and incident volumes surged, the pressure on their investigation workflow mounted. The team needed to go beyond alerting and detection—to deliver fast, forensic-backed answers, consistently and at scale.

While EDR and SIEM tools remained central to detection and correlation, they weren't built for investigations. "We'd know a command ran—but not whether it completed successfully, what else was happening on the host, or who else was logged in at the time," says Andrew Haslett, Director of Security Services. "It raised more questions than it answered."

This lack of context beyond the alert made it difficult to confidently advise customers on what to do next. "We'd escalate and they'd ask, 'Should we activate our IR retainer?' Sometimes we couldn't say for sure. We just didn't have the depth of visibility."

Attempting to close those gaps manually was both time-consuming and unsustainable. Analysts had to run one-off scripts, collect logs, and piece together fragments of information across systems. "It could take four to six hours per endpoint just to gather the right data—and that was before we even started the analysis. It became exponentially time-consuming with every new system," Andrew recalls.

Compounding the issue was internal capacity. As customer numbers grew, the number of escalations followed. When a significant incident required deep investigation, it tied up senior analysts for days, leaving the team stretched and unable to fully support additional cases that came in during that time.

Junior analysts, while capable, didn't have the tools or experience to independently support those investigations. The result: more pressure on the top tier, slower turnaround, and the constant risk of bottlenecks.

The outcome wasn't just internal strain—it impacted customer experience. "We'd escalate something and the client would expect answers. And we'd have to say, 'Sorry, we can't really tell you what happened.' That's a hard conversation to have when they're relying on you," says Andrew.

With growing scale, increasing investigation volume, and the expectation of quick, conclusive answers, Novawatch needed to rethink how they approached investigations.

Customer
Novawatch

Industry
Managed Detection and Response Provider

Region
US

Founded
2020

Employees
50-100 employees

Headquarters:
Scottsdale, Arizona, USA

Website
https://novawatch.com

Success Highlights:

- **Doubled customer count** without expanding the team (2x customers, same team)
- **Collection time reduced** from hours per endpoints to minutes for entire estates
- **Up to 70% time savings** on data collection
- **40% time-saving** on time to insights
- **Forensic data gathered** concurrently at scale
- **Structured workflows** accelerate time to answers

The solution: AIR in Action

To overcome these challenges, Novawatch deployed Binalyze AIR—bringing structure, scale, and speed to their investigation workflow.

"With AIR, when an incident happens, we get the answers. It's as simple as that," says Andrew Haslett."

For each client, Novawatch can either pre-deploy or rapidly activate AIR's lightweight Responder, a standalone package that acts like a virtual incident responder. The Responder connects to the AIR platform to execute targeted forensic collection and investigative tasks including triage and analysis, providing wide coverage with minimal resource use.

Once active, AIR enables rapid, targeted and remote collection of forensic data across an organization's assets. Investigations typically begin with AIR's automated Compromise Assessment capability—powered by DRONE and supported by built-in evidence analyzers. This feature helps Novawatch quickly surface indicators of suspicious activity and automatically prioritizes findings, guiding analysts to the most relevant investigative leads.

If deeper analysis is required, Novawatch can also initiate full disk and memory imaging remotely, with evidence uploaded directly to their S3 bucket. This eliminates the need to walk clients through downloading tools, managing large file transfers, or handling forensic imaging manually.

"Before, you'd spend hours just figuring out what to collect and where to look," says Andrew. "Now, with AIR's acquisition capabilities and Investigation Hub, we have everything we need in a single case view—organized, timestamped, and accessible."

AIR's timeline analysis gives analysts a clear, navigable view of host activity, with tagging, filtering, and bookmarking that accelerates both triage and reporting. "Being able to pull all that data and look through a specific time frame of what actually happened, tag and save the results—that's been huge."

Advanced features like InterACT, AIR's live command line interface, and integrated osquery and YARA scanning give Novawatch even more control and context during investigations. "Among other endpoint tools we've worked with, AIR offers a uniquely comprehensive level of investigative functionality," Andrew says. "I'm a big fan of the osquery and YARA rule integration."

Critically, AIR has enabled junior analysts to play a larger role in early-stage investigations. This relieves pressure on senior staff and improves overall capacity. "Instead of having to explain every step, we just say, 'Use AIR.' It gets us what we need, quickly and accurately."

For Novawatch, AIR has transformed investigations from a bottleneck into a business enabler—one that scales with them.

"Now, with AIR's acquisition capabilities and Investigation Hub, we have everything we need in a single case view—organized, timestamped, and accessible." says Andrew.

Raising the bar for MDR

Since adopting Binalyze AIR, Novawatch has significantly enhanced the quality and responsiveness of its investigations. Novawatch now delivers same-day answers at scale, thanks to up to 70% time savings on data collection and 40% time-saving on time to insights, —without compromising on depth or accuracy.

What started as alerting and escalation has evolved into a more responsive service. "AIR gives us the ability to dive much deeper into the forensic artifacts, pull them at scale, and investigate our clients' environments faster," Andrew explains.

Previously fragmented and manual, the investigation workflow is now structured, repeatable, and ready to scale. Analysts can focus on the most relevant leads, deliver faster answers, and provide clear next steps—elevating Novawatch's role from alert triage to trusted investigation partner.

In high-stakes moments, AIR helps validate threats and guide action. "We've used it many times to either prove or disprove that something is in our clients' environment—and we've needed to act fast," says Andrew.

The impact goes beyond the SOC. "We're not just throwing alerts over the fence. AIR lets us deliver clarity. That's powerful in sales conversations—and even more powerful in incidents."

Conclusion

With AIR, Novawatch has strengthened both the substance and perception of its MDR service. The ability to deliver fast, forensic-backed answers—along with clear, actionable recommendations—has become a meaningful differentiator and a driver of lasting client relationships.

Use case: Investigating a Zero-Day

When an admin account at a client's satellite office logged in from the Netherlands, Novawatch flagged the activity. The client confirmed it was unexpected. A zero-day affecting their VPN, combined with shared AD credentials, left the door open—and visibility at that location was minimal.

Novawatch used AIR to gather forensic evidence and quickly assess for malicious activity. A full disk and memory acquisition followed, enabling the team to piece together what happened, what was accessed, and whether the attacker was still present.

"We used AIR to figure out what happened, what was taken, and whether the attacker was still active," says Andrew. "We were able to answer all the key questions—fast."