binalyze!

DARK RHIINO SECURITY
INVESTED IN OUTCOMES

Dark Rhiino Enhanced Security Operations with **Binalyze AIR**

Company overview

Dark Rhiino is a leading MSSP dedicated to providing comprehensive security services to businesses of all sizes. Its mission is to ensure robust cybersecurity for clients through advanced technology and expert service with a Defense-in-Depth approach.

Founded in 2017, Dark Rhiino has grown to become a trusted partner for businesses seeking reliable and effective security solutions. The company offers a unique insured guarantee of up to $1m for all clients subscribing to its Defense-in-Depth, enabling them to secure a higher deductible on their cyber liability insurance coverage.

Manoj Tandon, Co-Founder and COO at Dark Rhiino, explained: "Plenty of other companies sell security services, but what makes our market claim so strong is that we actually back it up. We're in the business of selling outcomes."

Challenges

- Needed to improve the efficiency of its security capabilities.
- Manual processes were time-consuming and resource-heavy.
- Required increased visibility into customer systems.

Challenges in expanding security operations

As Dark Rhiino pursued an ambitious growth strategy, it faced several challenges as it expanded its operations. When the team took on more customers worldwide, it faced a greater variety of operational needs as well as a greater volume of incidents to address. At the same time, they needed to maintain a high level of security assurance for all customers and meet their $1m security guarantee.

With an increase in scope and demand, the team needed more efficient processes and greater visibility that allowed them to identify and address threats proactively.

Tyler Smith, CTO at Dark Rhiino, explained: "One of our customers operates in literally every country on Earth. So, at that scale, it's very difficult to monitor user endpoints with traditional SIEM technology or endpoint detection and response tools."

He elaborated: "There's also a danger of falling into the 'prevention paradox' - you focus on what you can easily detect and prevent, and the things outside that scope effectively become invisible. So, we needed to expand both the breadth and depth of our visibility into customer systems."

Efficiency was another key factor, as existing processes became increasingly resource heavy.

Investigating and clearing security alerts could take as much as a third of the day for Dark Rhiino's analyst team. Further, with many of those being false positives, all that work could equate to little value.

Tyler explained: "As our client base grew, we needed to find a way to scale our operations without simply adding more manpower. Our existing tool was extremely capable but overly complex and obtuse for our young team to use – it sometimes felt like we were fighting the tool as much as the threats. So, we needed something that was as accessible as it was reliable."

Maintaining high-quality service while operating efficiently was a critical challenge. Dark Rhiino needed to quickly identify compromises missed by prevention activity and achieve the visibility needed for thorough investigations to mitigate the chances of a full-blown incident.

This required a comprehensive platform that integrated a forensic-level approach, enabled proactive compromise assessments and would be easy and efficient to use. At the same time, the solution would need to provide complete remote system visibility with Dark Rhiino's broad customer base.

Customer
Dark Rhiino

Industry
Managed Security Service Provider (MSSP)

Region
North America

Founded
2017

Website:
darkrhiinosecurity.com

Success Highlights:

- **Near elimination of the need** for full scale incident response
- **Reduction in incidents** escalated to L3/L4 analyst
- **Make sense of security alerts** in less than 15 minutes
- **Accelerated false** positive validation
- **Scaled operations and upleveled** existing analyst team
- **Streamlined evidence** acquisition and analysis
- **Increased endpoint visibility** for easier malicious activity detection
- **Standardized processes** across operating systems

binalyze!

CYBERCLAN™
Enterprise Security Human Response

Why Binalyze AIR was the choice for enhanced efficiency

To address these challenges, Dark Rhiino chose Binalyze AIR after evaluating several solutions and finding it to be the most comprehensive and user-friendly. The platform was well-recommended by trusted industry peers, and Dark Rhiino quickly confirmed what it could do through an AIR trial.

Tyler explained: "One important factor was the platform's ability to integrate seamlessly with our existing workflows. The usability won us over very quickly. With our previous solution, we could solve security alerts in 15 minutes, but it would be a frantic 15 minutes as we battled to get visibility of the situation and make sense of it quickly."

He continued: "With Binalyze, we could gain situational awareness and skip all the digging and coding. The information we need is quickly available without needing to be a query wiz. This is so valuable for us - the team can act with greater speed and confidence, and achieve more with less supervision, fewer needs to escalate or interruptions to the workflow."

'One important factor was the platform's ability to integrate seamlessly with our existing workflows. The usability won us over very quickly.'

Binalyze AIR also improved the accuracy of evidence gathering and analysis to add context to alerts. The platform's advanced capabilities ensured the team had ready access to everything they needed to make informed decisions and respond to threats decisively.

The platform provided a single point for all evidence-related tasks helping to streamline workflows. The in-built analysis capability, DRONE, automatically highlights IoCs and ranks findings by severity to aid in prioritization. Meanwhile, AIR's remote shell feature, interACT, provides remote, cross-platform access to Windows, Mac, and Linux devices, allowing for a standardized process regardless of operating system.

This end-to-end investigation workflow capability also means that Dark Rhiino's team could manage a higher volume of incidents without needing to proportionally increase their workforce. The platform's scalability meant that the company could expand its operations and manage more clients efficiently.

'With Binalyze, we could gain situational awareness and skip all the digging and coding. The information we need is quickly available without needing to be a query wiz. This is so valuable for us - the team can act with greater speed and confidence, and achieve more with less supervision, fewer needs to escalate or interruptions to the workflow.'

Tyler added: "The accessibility of AIR was a huge benefit from a resource perspective. Anyone who has had to manage cybersecurity salaries knows that the more expertise a tool requires, the more expensive it is to run because of the skills required. Binalyze is so easy to use that I could get an intern, and they would be an absolute rockstar with it in three hours. It means we can uplevel our team and provide a complete security solution to our customers."

'Binalyze is so easy to use that I could get an intern, and they would be an absolute rockstar with it in three hours. It means we can uplevel our team and provide a complete security solution to our customers.' – Tyler Smith, CTO

binalyze!

CYBERCLAN™
Enterprise Security Human Response

Legitimate Access Use-Case

During a routine monitoring session, Dark Rhiino identified a client's employee who had inadvertently connected to a malicious wireless network in Asia, believing it to be a legitimate hotel Wi-Fi. This led to a DNS corruption that redirected all network traffic to a malicious server, which blocked the employee's ability to use their VPN.

The endpoint was unable to recognize any malicious behaviour, leading to a frustrated employee requesting exceptions to access work tools. Dark Rhiino utilized the Binalyze platform to swiftly investigate the issue. Within 30 minutes, they traced the DNS responses and confirmed the malicious DNS was altering IP addresses, preventing legitimate connections.

Thanks to Binalyze AIR's forensic-level visibility, Dark Rhiino quickly identified that the employee had connected to a fake network mimicking the hotel's Wi-Fi. By instructing the employee to connect to a trusted port or a different network, the team mitigated the threat before any significant damage occurred.

Delivering more value and security to clients

The adoption of Binalyze AIR provided several key benefits that enhanced its managed security operations and enabled the team to better meet the security challenges of Dark Rhiino's clients, and provide more ROI.

As an MSSP heavily involved in cyber liability insurance, capabilities around compliance are critical for Dark Rhiino. The Binalyze platform's comprehensive data collection, tagging and management, and analysis features helped Dark Rhiino meet compliance standards efficiently and accurately. Binalyze plays a crucial role in a 'defense-in-depth' approach, catching threat indicators that may be missed by a traditional prevention-detection approach.

Tyler added: "While we address incidents when they happen, our play revolves very much around prevention. We help enterprises avoid having to go down the costly road of incident response with a very deep level of monitoring beyond what traditional endpoint tools can manage.

"On the occasions where we have an active bad actor, we know AIR will let us see literally everything they've done. We can freeze those files, pull them off the machine, delete them, anything we need to do. Binalyze lets us see all the pieces, put them together into a timeline, and deal with it. This is a hugely valuable capability for us."

'While we address incidents when they happen, our play revolves very much around prevention. We help enterprises avoid having to go down the costly road of incident response with a very deep level of monitoring beyond what traditional endpoint tools can manage.'

'Binalyze AIR has been a huge boost to our ability to proactively identify and stop threats before they do damage. Having so many comprehensive features in one place have been instrumental in enhancing our service delivery, enabling our business model and meting our clients' needs.'

– Manoj Tandon, Co-Founder and COO

Conclusion

"Binalyze AIR has been a huge boost to our ability to proactively identify and stop threats before they do damage," said Manoj. "We can easily sort out false positives, quickly initiate a deep dive on genuine threats, and if necessary, contain an incident with a very rapid host isolation.

"Having so many comprehensive features in one place have been instrumental in enhancing our service delivery, enabling our business model and meeting our clients' needs."

Dark Rhiino's experience with Binalyze AIR demonstrates how the platform can empower MSSPs to overcome operational challenges, improve efficiency, and deliver high-quality security services. This partnership highlights the potential for technology to transform security operations and ensure robust protection for clients.