

Blackpanda Scales Incident Response and Democratized Cyber Resilience for Customers of All Sizes with Binalyze AIR

Company overview

Blackpanda is Asia's leading cybersecurity incident response firm, dedicated to making digital forensic and incident response (DFIR) expertise accessible to organizations across the region. It offers a subscription-based IR service, IR-1, that provides unlimited incident response support to businesses of all sizes, making high-quality cybersecurity accessible and affordable.

Founded in 2015, the company's mission is to democratize cybersecurity resilience by providing affordable, high-quality incident response services tailored to the Asian market. This commitment to set a high-water mark in effective incident response has led the company to implement Binalyze's Automated Investigation and Response (AIR) platform.

Challenges

- Needed to scale amid rising and demanding ransomware cases
- Manual evidence collection was highly resource and time-consuming
- Investigations took 6-8 hours per machine, limiting capacity
- Needed to streamline operations without compromising quality
- Faced varying regulatory compliance requirement across multiple countries

Challenges in Scaling Incident Response

As Blackpanda rapidly grew, it faced challenges in scaling its incident response operations to manage the increasing volume of ransomware cases, which represented the majority of the cases impacting their customers.

This was because traditional methods were proving too time-consuming and resource-intensive. The manual nature of evidence collection and analysis, often involving multiple tools and disparate systems, became a significant bottleneck. Investigations were time-consuming, and limited the number of cases the team could handle concurrently.

George Trikoilis, Director of Incident Response at Blackpanda, explains: "We were looking for a solution that would allow us to scale our operations irrespective of the number of systems we had to investigate.

We needed to respond in a timely manner, no matter how large the scope of the incident."

The team recognized the need for a solution that would enable them to scale their operations without sacrificing speed, and more importantly, quality. They wanted a platform that could streamline evidence acquisition and analysis, foster collaboration, and address the unique regulatory challenges of operating across different countries in Asia. Aligned with Blackpanda's mission, the solution needed to be cost-effective and scalable to support their diverse client base, from small businesses to large enterprises. It also needed to be user-friendly, easy to learn and manage, so it did not only cater to the high-level technical experts within the organization.

Customer

Blackpanda

Industry

Cybersecurity
Incident Response

Region

Asia (Hong Kong, Singapore, Japan, Philippines)

Founded

2015

Website

www.blackpanda.com

Success Highlights:

- **Improved overall case** investigation times by 30%
- **Reduced investigation time** per machine from 6-8 hours to 1-2 hours
- **Increased capacity and efficiencies** through technology rather than stretching or increasing workforce
- **Improved case collaboration** among team members through a unified platform
- **Improved ability to meet** cross-border data residency requirements
- **Removed the need for multiple** time-consuming recapture for missing artifacts

'Ransomware cases demand the most immediate support and the allocation of many resources since clients want to get back to business as quickly as possible. As we cannot securely restore systems until we have figured out how things have broken down, it's essential our investigations are very fast and accurate,' says George.'

George further emphasized the importance of finding a technological solution rather than merely expanding the workforce: "We started looking for solutions that did not just involve throwing more people at it. The right platform would facilitate incident response, because it does so many things for you. It highlights what you should look at and investigate first, significantly helping less experienced users to effectively support their organization."

Adopting Binalyze AIR for Efficiency and Collaboration

Blackpanda turned to Binalyze AIR, an automated investigation and response platform powered by digital forensics, to address their scaling challenges. The team initially heard about AIR from an ex-employee who recommended the solution. They conducted a free trial and found AIR to be highly efficient in accelerating investigations.

In 2023, with the launch of its IR-1 model, Blackpanda evaluated Binalyze AIR along with two other solutions. The team conducted competitive analysis and proofs of concept (POCs) before deciding on Binalyze AIR, highlighting its comprehensive features across acquisition, processing, analysis, and collaboration as key factors in their decision.

AIR's unified platform provided Blackpanda with a single pane of glass for evidence acquisition, analysis, and collaboration, streamlining their entire incident response investigation workflow.

Guo Yan, DFIR Specialist at Blackpanda, highlights the impact:

'Before Binalyze AIR, we spent about 6-8 hours investigating each machine. With AIR, we have reduced that to 1-2 hours per machine.'

Binalyze AIR's automated evidence collection and analysis tools significantly accelerated investigations. Its collaboration features enhanced team communication and knowledge sharing, boosting overall efficiency.

"When it comes to collaborating or sharing findings, you need to hand over the work efficiently. Before having a solution that centralizes everything, you had to figure out how to transfer data between colleagues in different locations, like from Singapore to Hong Kong. With Binalyze AIR, everyone can access the same data without screen shares or waiting for colleagues to be available," explained George Trikoilis.

The platform's automation features further enhanced Blackpanda's efficiency. By automating time-consuming tasks such as evidence collection and preliminary analysis, AIR freed up the team's valuable time to focus on higher-level tasks, such as threat hunting and strategic decision-making. The BlackPanda team can now quickly complete evidence collection directly rather than waiting for the client's IT team, making for a faster and smoother process. Additionally, AIR's ability to acquire a wider range of artifacts in a single pass significantly reduced the time and effort required for evidence gathering.

Most notably, AIR's comprehensive coverage across Windows, Linux, and Mac OS platforms enabled Blackpanda to streamline their incident response processes, ensuring efficient and thorough investigations regardless of the operating system involved.

"When conducting our competitive analysis, we found that Binalyze AIR offered a more complete solution by providing support across Windows, Linux, and Mac OS platforms. This comprehensive coverage allowed us to tackle acquisition, processing, and analysis in a unified manner, unlike other tools that focused solely on Windows for example. The broad support ensured we could efficiently handle investigations across various operating systems, which was crucial for our diverse needs," said George Trikoilis.

A transformative partnership

Binalyze AIR has become a cornerstone of Blackpanda's incident response operations. The platform's efficiency gains, streamlined workflows, and collaborative features have enabled them to scale their operations effectively. Incidents now typically require just one responder each, enabling the team to handle a larger volume of cases while also delivering timely and comprehensive support to their clients.

The solution also proved instrumental in meeting stringent cross-border data residency requirements, a crucial factor for Blackpanda's operations in Asia. The platform's flexible deployment options allowed them to comply with local regulations while maintaining the speed and efficiency of their investigations. This alignment with regulatory requirements, combined with the platform's scalability and cost-effectiveness, directly supported Blackpanda's mission to democratize cybersecurity by making high-quality incident response services accessible to businesses of all sizes.

Conclusion

"The support and speed of action on feedback from the Binalyze team have been stellar," says George. "The immediate support we get is exceptional, and the rapid implementation of our feedback into new releases has made a significant difference. These prompt responses have deepened our relationship, making Binalyze AIR an invaluable asset for our team."

Blackpanda's success with Binalyze AIR exemplifies how the platform can empower incident response teams to overcome scaling challenges, improve efficiency, and deliver high-quality cybersecurity services to a broader range of organizations.