binalyze!

TRANSAM

From Detection to Decision:
Boosting TransAm Trucking's Operation Efficiency with Binalyze AIR

Company overview

TransAm Trucking is a prominent transportation and logistics company based in North America, employing over 550 staff members. Specializing in freight and logistics services, TransAm operates with a strong focus on efficiency and reliability. The company's extensive fleet and advanced logistics network enable it to serve various clients across the region.

Facing cybersecurity challenges, including insider threats, data exfiltration, and ransomware attacks, TransAm adopted Binalyze's AIR to bring in improved forensic capabilities and visibility to enhance threat response abilities.

Challenges

- Needed to safeguard sensitive data and ensure continuous operations
- Faced a complex security landscape with multiple threats
- Capacity and resourcing challenges
- Limited IT and security team size compared to large operational scope
- Needed a solution that could integrate with existing tools
- Experienced a previous ransomware attack highlighting vulnerabilities

The need for more efficient security

TransAm faced a complex security landscape characterized by multiple threats, including insider risks and external attacks. As a major player in the transportation and logistics industry, the company had to safeguard sensitive data and ensure continuous operations.

Protecting personally identifiable information (PII) is a top priority for TransAm. Implementing effective Data Loss Prevention (DLP) measures was essential to detect unauthorized data transfers and safeguard customer trust. Data exfiltration by malicious actors posed a persistent threat. Furthermore, the company also needed to address insider threats where employees could potentially misuse their access to sensitive information.

In addition to data protection, as a logistics company, TransAm also needed to prioritize operational resilience, as a disruptive attack could have a severe impact on its fleet. The organization had experienced a previous ransomware attack that highlighted the vulnerabilities in its security infrastructure.

Dane Zielinski, Information Security Manager at TransAm, explained: "We have over 500 employees and we have vehicles out over half the country, but our IT and security teams are small. So, it's absolutely essential for us to have security solutions that can identify threats and let us move quickly before things get out of hand."

He continued: "Transportation is a slim profit margin industry, and a few days or potential week-long outage and the resulting degradation in operations can have millions of dollars in impact that is difficult and possibly impossible to recover from as a business."

.

Customer
TransAm Trucking

Industry
Transportation and logistics

Region
North America

Founded
1987

Employees
550

Website
www.transamtruck.com/

Success Highlights:

- **Reduced downtime** with faster response times to security incidents
- **Higher confidence** in removing threats and stopping kill chains
- **Automated evidence acquisition** and initial analysis completed in under 15 min
- **Enhanced ability** to bring forensic data to SOC investigations
- **Seamless integration** with existing security tools
- **Maintained high** oversight and control with reduced internal resource strain

Why Binalyze AIR was the only choice

As part of on-going efforts to strengthen its security, TransAm brought in various outsourced solutions for endpoint detection and response (EDR) and 24x7 Security Operations Centre (SOC) capabilities. However, Dane also wanted to level up TransAm's digital forensics and incident response (DFIR) in-house to resolve more issues before calling on external partners for deep-dive investigations.

He explained: "Deep-dive analysis for a company like ours, where we don't have an in-house CSIRT/DFIR team, means spending additional money for the investigation. Also, working with MDR forensics teams isn't usually quick and efficient, and you're sometimes sitting and waiting to find out about critical actions - do we isolate, un-isolate, rebuild a system, change service accounts, and so on? This is an important part that forensics answers."

Binalyze AIR was Dane's immediate choice for the job, thanks to his positive experience with the platform at his previous position and employer.

"I helped bring in Binalyze at my previous employer," he explained. "That was a very different proposition to TransAm, because I was working with a large team there, versus a much smaller security operation here. But I knew from my experience that AIR was highly effective and would be exactly what I needed to get forensic details at the bat of an eye."

He added: "Binalyze is basically my default for addressing these kinds of needs. If I were to go anywhere and build a new security stack and defensive layer methodology, I know Binalyze AIR is going to be part of it."

AIR's advanced evidence acquisition capabilities enable it to collect over 500 types of artifacts with a high level of speed and accuracy. The platform is highly automated, enabling users to combine evidence acquisition and initial analysis into a single process using AIR's automated compromise assessment capability, DRONE.

Dane explains: "DRONE is an integrated APT (Advanced Persistent Threat) scanner that allows our team to sift through the hundreds of artifacts, putting my team on target - it's our magnet in finding the needle in the proverbial forensic artifact haystack".

Leveraging extensive integration capabilities. Binalyze AIR was seamlessly integrated with existing tools and services, including their endpoint protection and MDR provider. This integration streamlined workflows, automating forensic evidence acquisition and analysis in as little as 15 minutes, provided key information and prioritized insights without any manual intervention to speed the start of the investigation.

" If I were to go anywhere and build a new security stack and defensive layer methodology, I know Binalyze AIR is going to be part of it."

– Dane Zielinski,
Information Security Manager

binalyze!

TransAm

How Binalyze became a security cornerstone

Implementing Binalyze significantly bolstered TransAm's security infrastructure. The company saw marked improvements in its investigation and response capabilities, allowing for rapid identification and mitigation of threats. Before Binalyze, the team had no in-house forensics or ability to YARA hunt, relying on EDR logs, findings provided by their MDR provider and manual virus scanning.

Dane commented: "One of our big priorities was to incorporate standardized forensics as part of our security operations, and this is really what Binalyze does best. It's very reliable and means we always have that insurance of being able to answer the questions of 'Who, What, When, Where, Why, and How' when it comes to an investigation. I've called it 'forensics for the common man' – it's very easy for analysts to access and understand the data."

Binalyze enabled TransAm to quickly conduct thorough forensic investigations, providing detailed insights into security incidents. This capability was crucial in understanding the nature and scope of threats, leading to more effective responses.

Binalyze's forensic approach, along with its speed and reach, were some of the most beneficial factors for TransAm.

Dane explains: "The ability to pull forensics data on a dime is very useful, but the fact it can even pull over the internet is huge. Right when I implemented Binalyze at my previous company, we had the beginning of COVID. And so of course, we didn't have a way of forensically pulling data from people's houses without physically traveling to every location while they were working remotely. This way we also save on huge delays due to shipping and receiving equipment needing a forensic investigation.

But with AIR, we implemented it through the internet and our private network, so as long as the agent has internet connectivity, we can pull forensic data immediately. It was a huge innovation at the time and it's still extremely useful now."

The deployment of Binalyze streamlined TransAm's security operations, including reduced mean time to verify threats, by providing the informed decision support that allowed the team to get systems back into operational production sooner and with confidence. It also granted the internal team a much greater sense of visibility and control, enabling them to easily verify and follow up on reports coming in from outsourced services like the SOC. As a result, TransAm maintained high oversight while freeing up internal resources for strategic initiatives.

The Insider Threat Use Case

In addressing a perceived insider threat, TransAm leveraged Binalyze AIR to hunt for specific files they suspected were compromised. Binalyze AIR's capabilities allowed them to perform a deep dive into their systems that other security tools could not, to verify the security of their data. "Although the threat was less significant than we feared, this incident showcased the critical role of Binalyze in quickly identifying and resolving potential internal security issues before they become a major problem."

> **"While I can't guarantee a breach will never occur, my goal is to ensure that any compromised data is of minimal significance—a security stance many companies currently lack. Forensics visibility plays a crucial role in achieving this."**
>
> – Dane Zielinski,
> Information Security Manager

Conclusion

By leveraging Binalyze, TransAm has significantly improved its security posture, achieving faster response times and integrating forensic visibility in their security operation. Binalyze has become an integral part of TransAm's security strategy, demonstrating its value in helping the company evaluate threats and make informed, complete decisions. Looking ahead, AIR will continue to be a mainstay of TransAm's security capabilities and Dane is excited to see the platform continue to develop and add new features.