CASE STUDY FOCUS | COMMERCIAL & RESIDENTIAL SECURITY

# American Alarm Moves From Reactive Security To Proactive Data Protection With BlackFog

Learn how one of New England's largest independent security systems integrators transformed its cybersecurity strategy, closing the data exfiltration gap after a network incident and laying the foundation for secure enterprise AI adoption.

| INDUSTRY | LOCATIONS | EMPLOYEES | SOLUTIONS | WEB |
|---|---|---|---|---|
| **Commercial & Residential Security** | **9 across New England** | **300** | AIDX Protect<br>AIDX Vision | **americanalarm.com** |

CUSTOMER STORY

## From "Not If, But When" To Proactive Security

"A few years ago, cybersecurity was all about 'not if, but when,'" says Derek Arsenault, Vice President of IT. "You assumed you were going to get hacked and focused on recovering as quickly as possible."

That philosophy reflected the reality facing many organizations. American Alarm had invested in leading security technologies, including SentinelOne and Cato, yet those solutions were designed to detect and respond. They could not stop sensitive information leaving the business.

Everything changed after a network incident. Although the company recovered quickly, one question lingered: had customer or company data already been exfiltrated?

"We worried about what data got exfiltrated. We were fortunate on that front, but we didn't want to take that chance again."

THE TURNING POINT

## Putting BlackFog To The Test

When BlackFog first called, Derek wasn't convinced. "I was skeptical."

Instead of accepting the claims at face value, American Alarm embarked on a six-month technical evaluation. Independent cybersecurity consultants challenged BlackFog's engineers, explored the architecture and tested whether anti data exfiltration protection could genuinely complement the company's existing security stack.

"We brought in outside cyber companies we worked with to question BlackFog and meet BlackFog's sales engineers. We grilled them. It really satisfied the need."

The outcome wasn't that BlackFog replaced EDR, it filled the missing layer. For the first time, the organization had a way to proactively prevent data leaving endpoints before attackers could exploit it.

> **"We brought in outside cyber companies we worked with to question BlackFog and meet BlackFog's sales engineers. We grilled them. It really satisfied the need."**
>
> **DEREK ARSENAULT** · VICE PRESIDENT OF IT, AMERICAN ALARM

THE MISSING LAYER

## Completing The Security Stack

The decision came down to more than technology. BlackFog changed the way American Alarm approached cybersecurity.

Instead of preparing for the inevitable breach, the team could begin preventing one of the most damaging outcomes – data exfiltration.

Looking back, Derek reflects: "I don't know why I took the cold call, but it was one of the best decisions I made."

PRIMARY OUTCOMES

**› Proactive protection › AI governance › Operational simplicity › Peace of mind**

THE DEPLOYMENT

## Simple To Deploy. Easy To Trust.

BlackFog was deployed across every endpoint across the organization and became mandatory for network access. After minor tuning during the initial rollout, it settled into everyday operations with almost no administrative burden.

"It's a set it and forget it solution." Its simplicity was initially surprising. "In fact, it's so easy to use it's hard to believe it's working."

For a lean IT team supporting hundreds of employees, one console and very low false positives translated into greater efficiency without sacrificing protection.

AI GOVERNANCE

## Preparing For Enterprise AI

As the business began evaluating ChatGPT, Microsoft Copilot and Grok, BlackFog's role expanded. ADX Vision gave the team visibility into AI usage, allowed licensed and unlicensed users to be managed differently and provided the evidence needed to create sensible governance policies.

"It gives us a barometer of what we need to establish our AI policies going forward."

Rather than slowing innovation, American Alarm is using visibility to enable AI adoption with confidence.

THE RESULTS

## A Shift From Reactive To Proactive Security

REACTIVE TO PROACTIVE

**BlackFog fundamentally shifted American Alarm from preparing for cyber incidents to proactively preventing data exfiltration.**

OPERATIONAL SIMPLICITY

**A small IT team benefits from one console, minimal management overhead and consistently low false positives.**

FUTURE-READY SECURITY

**The same platform now supports both ransomware resilience and enterprise AI governance.**

> "I sleep much better at night. Before BlackFog I would be up a lot of nights worrying about what the next attack vector could look like. BlackFog and our other solutions mean it's much less of a worry for me."

**DEREK ARSENAULT** · VICE PRESIDENT OF IT, AMERICAN ALARM

A TRUSTED ADVOCATE

## Sharing The Experience

Today Derek regularly recommends BlackFog to fellow security professionals through the NetOne community, a network of 30 security companies across the U.S. and Canada. His advice to organizations evaluating proactive data protection is simple:"They should have deployed it yesterday."

That endorsement carries weight because it comes from someone who was once the sceptic in the room. After rigorously testing the technology, living through a network incident and expanding into AI governance, American Alarm now sees BlackFog as a foundational part of its cybersecurity strategy.

ABOUT BLACKFOG

## Real-Time, On-Device, Data Exfiltration Prevention

BlackFog helps organizations reduce modern cyber risk by stopping data exfiltration, the common factor behind ransomware, insider threats, zero-day attacks, and Shadow AI exposure. Our anti data exfiltration (ADX) platform delivers real-time, on-device prevention. It stops sensitive data from leaving endpoints and networks without authorization and blocks ransomware communication, data theft, and AI driven leakage before damage occurs. By focusing on prevention instead of just detection, BlackFog helps organizations strengthen compliance, protect privacy, and improve operational resilience.