



# US Law Firm Bolsters Cyber Defense with BlackFog

## US Law Firm

**Industry:** Legal

**Vertical:** Bankruptcy

**Location:** South West, USA

**Size:** Large

## Overview

For this anonymized case study we spoke with the Managed Service Provider (MSP) responsible for IT security at a law firm in the US. The firm, who specializes in bankruptcy law outsources all of its IT security requirements to their MSP.

## The Challenge

As a reputable law firm, protecting client data and maintaining the integrity of their business is a key focus. Bankruptcy data would likely be embarrassing for both clients and the firm if it were to leak via a data breach or cyberattack, so having a robust cybersecurity strategy is important to mitigate those risks.

The pandemic brought additional security challenges as newly remote employees added additional risk.

The firm had the usual tools such as firewalls and antivirus in their security stack, but knew they needed to go beyond the basics to give them the level of protection they needed to stay ahead of cybercriminals. They knew they needed a preventative solution that would act like a 'trip wire', effectively stopping hackers in their tracks before it was too late.

## The Solution

When the firm was selecting a cyber insurance partner it was recommended to them that they bolster their security stack and add next generation cybersecurity tools to prevent cyberattacks, namely ransomware. The insurance partner provided some options for them to investigate further and BlackFog was a recommended solution.

As the firm does not have an internal IT security team, the due diligence fell to their MSP provider. The MSP looked into BlackFog as an option

and immediately liked what the product could offer. "With this customer we had no way of knowing if a device or system had been accessed or if bad actors were up to no good. BlackFog looked interesting to me as it would block attacks automatically, taking a preventative approach rather than just sending alerts which would require me to act on them to block the threat."

## The Approach

BlackFog was tested for around 30 days across several devices. Early in the testing phase BlackFog identified and shut down a phishing attempt which was a key concern for the firm, especially as phishing campaigns continue to increase in sophistication.

The MSP commented "I see the phishing emails coming in, and they are getting better all the time. I've lost count of the number of clients who have had staff rushing out the door to buy gift cards on the back of an impersonated email for example, this particular phishing scam seems to be

gaining momentum and even the most savvy employees can fall for it.

Knowing that BlackFog could prevent these attacks even if an employee clicked on a malicious link was a really strong selling point for us. Every time I get an alert to say someone clicked on a link they shouldn't have, I'd say thank God BlackFog was there to block that connection!" The MSP also noted that other tools were not blocking anonymous networks coming from Tor / dark web sites but noted that BlackFog was. He commented, "there is no one that should ever be connecting to a tor site, yet this wasn't blocked by default with other defense tools, this is something that BlackFog did automatically."

## The Results

The firm decided to purchase BlackFog through its MSP partner and deploy it across all of its devices.

Having BlackFog installed has given them the 'trip wire' they were looking for. The attacker may get in but BlackFog ensures that he's stopped in his tracks and no data will be removed, something that has become increasingly important with the data extortion tactics becoming increasingly popular with ransomware gangs.

BlackFog enables the firm to work more securely without impacting the employees, and perhaps most importantly it provides peace of mind for the team responsible for securing the organization. The MSP commented, "from an IT perspective BlackFog is wonderful, its much easier to get a snapshot of what's happening across the organization which gives me peace of mind and lets me sleep at night. BlackFog has saved me time and I don't need to worry about something bad happening at that organization."

**"Every time I get an alert to say someone clicked on a link they shouldn't have, I'd say thank God BlackFog was there to block that connection!"**

**"from an IT perspective BlackFog is wonderful, its much easier to get a snapshot of what's happening across the organization which gives me peace of mind and lets me sleep at night."**

## About BlackFog

BlackFog is the leader in on device data privacy, data security and ransomware prevention. Our behavioral analysis and anti data exfiltration (ADX) technology stops hackers before they even get started. Our cyberthreat prevention software prevents ransomware, spyware, malware, phishing, unauthorized data collection and profiling and mitigates the risks associated with data breaches and insider threats. BlackFog blocks threats across mobile and desktop endpoints, protecting organizations data and privacy, and strengthening regulatory compliance.

