



4Sight Chooses BlackFog ADX to Prevent Data Exfiltration

Company Bio

4Sight Holdings Limited

Industry: Technology Services

Location: South Africa

Partners: 600

Employees: 370

 4sight.cloud

The 4Sight Channel Partner (CP) Cluster is a partner-focused ecosystem that supports value-added resellers across Africa, the Middle East, and Central Europe. It enables the distribution of 4Sight's integrated solutions, including Sage and Microsoft cloud applications, through the Microsoft Indirect Cloud Solutions Provider (CSP) and Independent Software Vendor (ISV) channels. With dedicated sales, marketing, technical, and support resources, the CP Cluster empowers resellers to deliver high-quality solutions globally. For more information, visit [here](#) or contact channel@4sight.cloud.

The Challenge

The challenge for 4Sight was twofold. Firstly, the group comprises four diverse Clusters formed and structured in 2020 with the new strategy. As with any diverse business, creating standards relating to legacy policies, procedures and products was a high priority.

The group needed to focus on standardizing practices across the group, as well as ensuring that information was secure. To ensure compliance, they also needed to be able to easily manage and report this across the group.

Secondly, as leaders in digital transformation, 4Sight is responsible for providing best-of-class solutions to their customers. With cybersecurity playing such a big part in their solutions portfolio, utilizing technologies that would secure data, was critically important.

The Solution

The concept of looking beyond perimeter defence and focusing on preventing exfiltration was interesting, and although some other providers concentrate on elements of that, no one was providing data exfiltration prevention to the full extent that BlackFog was," commented Rudi Dreyer, Chief Business Environment Officer at 4Sight.

As a digital company with a focus on data and data management, 4Sight also needed to ensure they had the best cybersecurity practices across the group when they were in the process of obtaining their ISO 27001 certification. Adding an extra layer which would prevent any unauthorized data exfiltration, was an important part of that strategy.

The Approach

Initially the intention was to provide BlackFog to their customers, but they decided to use the solution

internally over a six-month period. BlackFog was deployed across several company devices. “Initially we really liked the fact that BlackFog was an on-device solution that would help us secure our devices, no matter where our employees were based. It was easy to use with a really intuitive console. We also really liked the Threat Hunting module, being able to detect suspicious activity and investigate it to determine the root cause and address it, was a very appealing feature”, said Rudi.

During the proof-of-concept process, it was evident that BlackFog would be of benefit to their customer base. “When working with customers, our transformation team looks for gaps so we can deploy technology solutions where appropriate. We felt that BlackFog would add significant business value for several of our customers and it made sense to add it to our end-to-end cybersecurity solution.

“ADX provides an extra layer of defense, and there is no such thing as enough defence when it comes to cybersecurity as it’s such a fastmoving target. For example, we have a customer in the mining industry who relies on chat functionality to communicate with partners in Russia and China.



During a POC BlackFog picked up the communication that was going to restricted geographies, in this instance someone was chatting with a business associate in China but in actuality the data was going to Russia or Serbia.”

Rudi Dryer, Chief Business Environment Officer, 4Sight

“During a POC BlackFog picked up the communication that was going to restricted geographies, in this instance someone was chatting with a business associate in China but in actuality the data was going to Russia or Serbia when it shouldn’t have been. BlackFog put a stop to it, meaning the company could continue to do business

with associates in those countries safely with the unauthorized data exfiltration being blocked. We’ve also seen BlackFog pick up ransomware attacks during POCs. When we see these types of events happening it really makes sense to add BlackFog as an extra security layer for of our customers,” added Rudi.

The Results

Following the trial period and evaluation, 4Sight decided to deploy BlackFog to all of its company devices, in addition to adding it to their solutions portfolio for their customers. Rudi concluded, “As a company we are committed to helping our customers future proof their businesses through digital transformation.

“Adding an anti-data exfiltration solution to our security stack means we are providing our customers with nextgeneration cybersecurity solutions to ensure our data and that of our customers is as secure as it can be.

“I would definitely recommend BlackFog to other organizations. Most companies have a data exfiltration problem, they just don’t know it yet. BlackFog provides peace of mind, so much so that I even have it on all of my personal devices.”

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.