



HFS Hot Vendor: CujoAI

Coverage initiated: Q4 2018

Introduction

The HFS Hot Vendors are an exclusive group of emerging players, each with a differentiated value proposition for the HFS OneOffice or HFS OneEcosystem. HFS analysts speak with numerous exciting startups and emerging players.

We designate a select group as HFS Hot Vendors based on their offerings' distinctiveness, ecosystem robustness, client impact, financial position, and the impact in our OneOffice and/or OneEcosystem Frameworks. The HFS Hot Vendors may not (at the time of writing) have the scale and size to be featured in our Top 10 reports, but they have the vision and strategy to impact and disrupt the market.

Author: Elena Christopher

CUJO AI wants to help network operators bring enterprise-grade network security to consumers to protect their proliferating range of connected devices and things. Founded in 2015, the firm got its start with a smart firewall product sold directly to consumers through big-box retailers. The product, which connected directly to in-home routers, enabled CUJO AI to establish a business in the emerging niche of home network security and, critically, to start collecting data about the threats facing connected consumer devices. This collection and processing of network metadata enabled CUJO AI to train machine learning algorithms focused on ensuring consumer cybersecurity and determining relevant network threats.

As so many consumers source their routers directly from their internet providers, in January 2018, CUJO AI officially pivoted to a business-to-business (B2B) focus and began exclusively targeting broadband network operators with its AI-based platform.

Today, CUJO AI offers its AI-enabled platform on a white-label basis to network operators for local area networks (LAN) and wireless communications (mobile networks and public wi-fi). The SaaS-based platform currently comprises the following services:

- **Device identification:** According to CUJO AI, a typical household has about 18 devices. To protect these devices, a consumer needs to understand what's connected to a home network. CUJO AI offers discovery of all devices in the connected home with easy-to-understand naming conventions beyond MAC or DHCP host addresses.
- **AI security:** CUJO AI protects against malware, phishing scams, and other threats with dedicated security algorithms for all devices, from laptops and smartphones to IoT and cameras.
- **Content controls:** CUJO AI provides content filters, schedules, content blacklisting, and configurable profiles to monitor, manage, and protect online activity.

Each solution can be implemented as a carrier-branded service offering. Operators can choose to implement the entire suite or select services. The CUJO AI platform integrates into the operator's cloud and customer premise equipment (CPE) infrastructure, assuring the safety and privacy of the operator's data. CUJO AI is currently deployed in approximately 16 million homes and protects more than 200 million devices worldwide.

CUJO AI closed a round of series B funding in May 2018, led by Charter Communications. It is using the infusion of funds to scale its business internationally, to expand its team with an emphasis on sales and marketing, and to support continued investment in its technology. The investment by Charter, which does not have a separate corporate VC fund, represents critical support from its targeted client base.

In our reference interviews with multiple operators using CUJO AI, we heard that operators selected CUJO AI based on its strong mix of capabilities, the fact it's deployed (not slideware), and its nimbleness.

On the capabilities front, all operators interviewed indicated that CUJO AI's approach of using machine learning rather than deep packet inspection or DNS filtering made it appropriate for its consumer-focused business given innate privacy concerns. Its ability to integrate with operator firmware and function effectively using the limited processing and memory on gateways was critical. Additionally, its device identification is purported to be the best on the market, returning successful and descriptive device identification about 90% of the time versus 40% from other tools, which often supply only IP addresses.

HFS' take

HFS has designated CUJO AI as a Hot Vendor because of its innovative use of machine learning AI to help solve the growing problem of privacy and cybersecurity protections for consumers. The proliferation of connected consumer devices is so vast that no company could employ enough security analysts to evaluate and render decisions on all potential threats. Existing enterprise-grade solutions such as deep-packet inspection are not appropriate for consumer data due to privacy concerns. CUJO AI's use of machine learning algorithms to support threat detection coupled with its intuitive device identification abilities has created a range of value-added services that both help end-consumers safely manage their connected existence and help network operators elevate the role of customer experience.

As the provision of communication and connectivity services continues to commoditize, network operators are

challenged to both shore up existing revenue and identify new sources. As such, many are placing big bets on elevating customer experience (CX). CX is a broad concept, however, and it has too often been code for cost-savings initiatives such as self-service instead of genuine efforts to improve CX. While each network operator that works with CUJO AI customizes how its end-customers access and interact with CUJO AI's services, all efforts are squarely aimed at improving CX. Some services, such as device identification, are being offered as part of existing service subscriptions and others, such as security protection or content controls, are available for a nominal fee. These services also offer network operators the potential silver lining of lowering support costs; accurately identified connected devices help eliminate problems by making systems more secure and making it easier to diagnose issues.

While CUJO AI has high potential, it is still a young company in a new market. There are always growing pains when small companies start working with large and often siloed businesses such as network operators. Its clients, while very happy from a technology standpoint, cite a strong need for the development of enterprise-grade processes and enhanced knowledge of the speed and culture of network operators. While these needs are critical to meet, they are typical of fast-growing companies like CUJO AI. The other areas for development are with technology relevance—ensuring it stays focused on its core strength of data science to ensure its algorithms scale with device and threat proliferation.

Additionally, CUJO AI would do well to help educate the consumer market on the very threat it protects against—cyber threats for consumer connected devices. Enterprise hacking and issues such as election tampering are current headline issues, but they don't have a consumer face to them. CUJO AI and its network operator partners can help educate the market on the benefits of consumer-focused cybersecurity, perhaps from a threat avoidance perspective such as protection against identity theft or assurance of financial privacy.

Vendor factsheet

- Founded in 2015
- Headquartered in Mountain View, California with locations in Brazil, Hungary, Lithuania, Finland, the United Kingdom, Malaysia, Hong Kong, and the Philippines
- Key executives include Einaras von Gravrock (co-founder, CEO) and Yuri Frayman (co-founder, Chief Strategy Officer, and serial tech entrepreneur)
- Number of employees: ~175
- Financial backing by investors including Charter Communications and KPN Ventures
- The company is working with Tier 1 network operators in the US, Europe, and APAC
- Recognized as a "Technology Pioneer 2018" by World Economic Forum

Solution portfolio

CUJO's AI platform consists of the following services. Each solution can be implemented as a carrier-branded service offering. Operators can choose to implement the entire suite or select services:

- **Device identification:** CUJO AI offers discovery of all devices in the connected home with easy-to-understand naming conventions beyond MAC or DHCP host addresses
- **AI security:** CUJO AI protects against malware, phishing scams, and other threats with dedicated security algorithms for all devices, from laptops and smartphones to IoT and cameras
- **Content controls:** CUJO AI provides content filters, schedules, content blacklisting, and configurable profiles to monitor, manage, and protect online activity

Industry coverage

Telecommunications

Partnerships

Technicolor: CUJO AI is working with Technicolor to integrate AI and machine learning technologies to customer premises equipment (CPE) platforms used by network service providers.



About HFS

Insight. Inspiration. Impact.

HFS is a unique analyst organization that combines deep visionary expertise with rapid demand side analysis of the Global 2000. Its outlook for the future is admired across the global technology and business operations industries.

Its analysts are respected for their no-nonsense insights based on demand side data and engagements with industry practitioners.

HFS Research introduced the world to terms such as “RPA” (Robotic Process Automation) in 2012 and more recently, the HFS OneOffice™. The HFS mission is to provide visionary insight into the major innovations impacting business operations such as Automation, Artificial Intelligence, Blockchain, Internet of Things, Digital Business Models and Smart Analytics.

Read more about HFS and our initiatives on:
www.hfsresearch.com or follow
[@HFSResearch](https://twitter.com/HFSResearch)