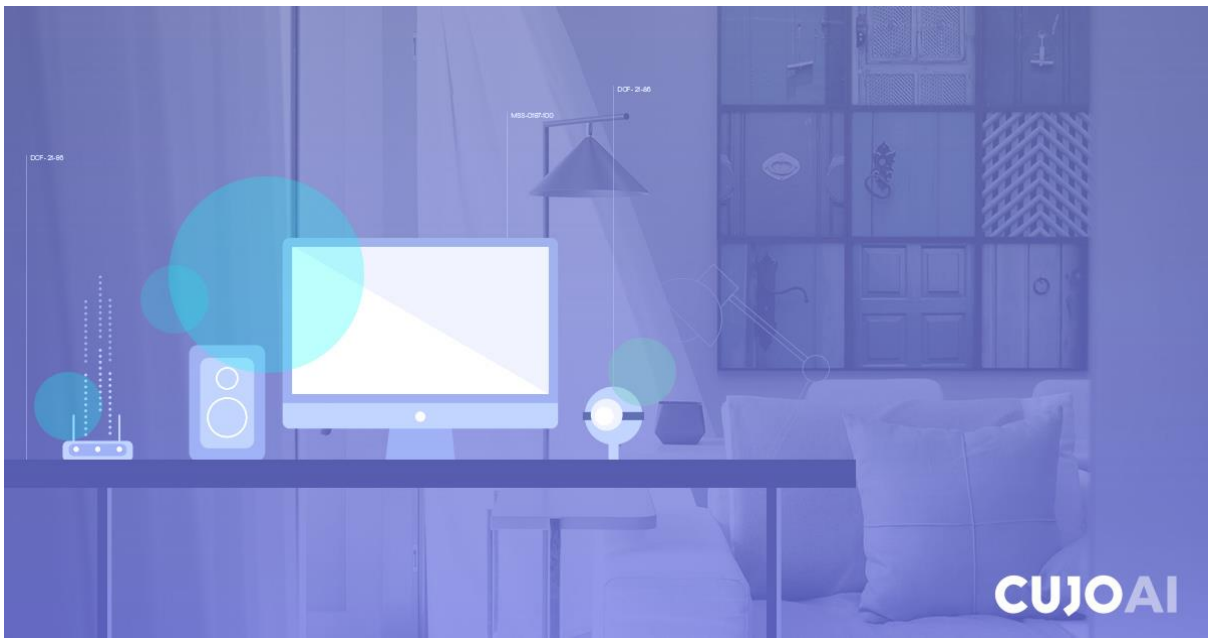
Why Identifying Your Network of Devices Is Key to Improving Security



The modern reality is an ever-growing network of IoT devices. Gartner predicts no less than 20.4 Bn of IoT devices worldwide by 2020. This high level of connectivity also poses a lot of new risks.

Simple IoT devices become easy entry points to the network that hackers mercilessly exploit. Home users are becoming more and more aware of the modern threat context, and no less than 83.3% of the CUJO AI survey respondents prefer to get full information about device vulnerability to threats.

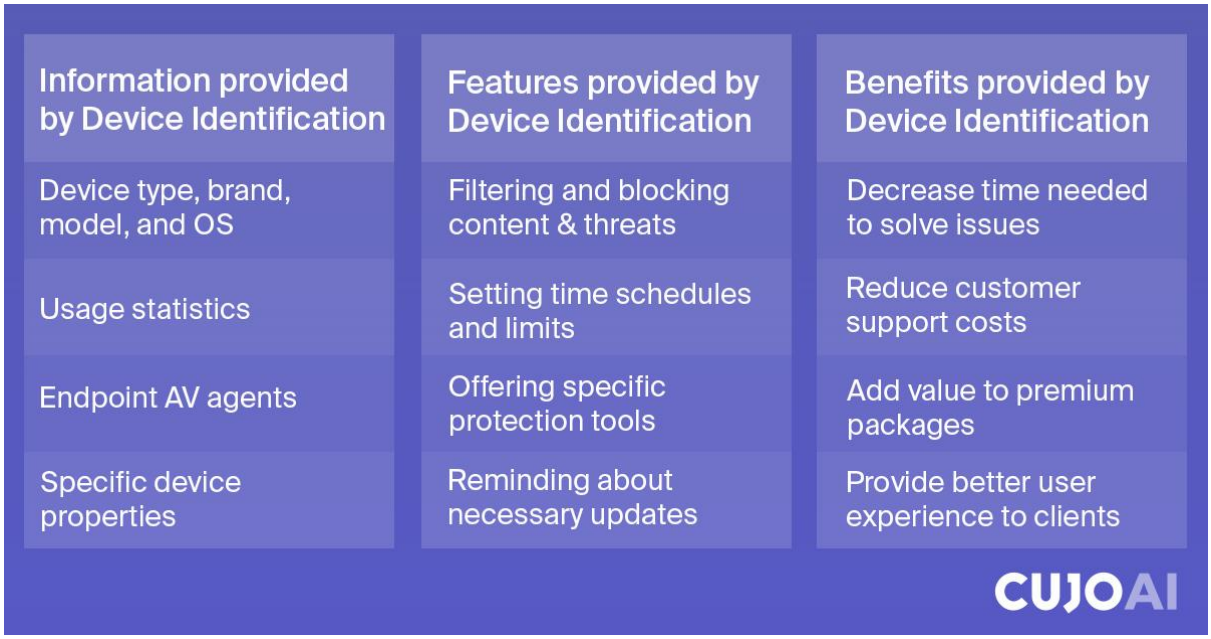
The aforementioned CUJO AI survey included 2600+ respondents and spanned over the period of two months this summer.

The Invisible Network Devices: Mapping with AI

In order to provide home users with precise information on their entire network and the devices in it, device identification is imperative. While that is the obvious solution, it is not an easy task to find a solution that can do this job accurately and quickly.

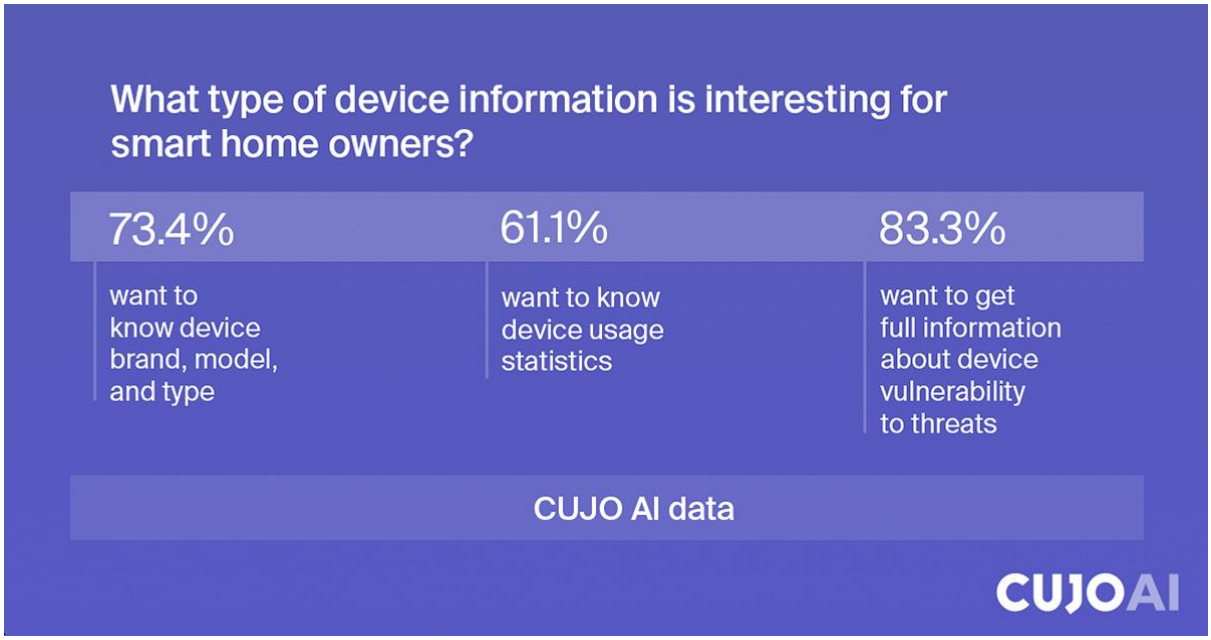
Good user experience is vital in today's market. Incorporating artificial intelligence in device identification tools can help guarantee that. Device identification is important to the customer from the safety perspective: correct device identification is crucial in identifying specific device vulnerabilities as well as setting up a strong security foundation.

Device identification is also useful for the end user since it provides information about the devices at home and the unknown devices that might be connected, hence allowing customers to stop any unwanted access to their personal devices. It also provides deeper insights of network usage.



The identification part can work on a few levels. On a more generic level, it detects a generic device type, brand, model, and OS. However, it can dive deeper and precise endpoint AV agents, as well as to inform of specific device properties and display very detailed information about the device (i.e., MacBook Pro Retina, 13-inch, 2012-2013).

Device identification uses predictive algorithms powered by AI to analyze a broadband home network and determine what devices are connected to it.



CUJO AI data shows that 73.4% of respondents want to know device brand, model, and type of the devices in their network. A slightly smaller amount - 61.1% want to know device usage statistics. Security remains a priority, as 83.3% of the respondents prefer to get full information about device vulnerability to threats.

Once a network operator is equipped with more information, it can go on offering additional features, such as filtering content, blocking it, or scheduling to help with time management. Knowing the exact device properties also allows offering better protection tools that can work specifically for that gadget, and even reminding to update outdated software.

Building Value with AI-Based Device Identification

Seamlessness is critical when it comes to smart homes. Today, users tend to have a variety of IoT gadgets and a lack of control over them or their network. AI-based solutions can help patch bridge this gap and offer not only a more clear overview but a sense of confidence to home users. That is especially relevant when more and more IoT hacking incidents come to light.

With technology becoming so natural and necessary at an average household, home users are becoming more aware of both the risks and the potential value that the vast IoT network brings. While that can be a challenge, it is also a rapidly growing market that requires a lot of new solutions, powered by the latest advancements in technology.

The data from the CUJO AI survey shows a clear interest to the specifics of device activity on home networks. Users are starting to value additional information in conjunction with premium services, and using AI-based tools can help provide exactly that.

Getting more precise data on their users is very valuable to network operators, too. It can dramatically decrease the time needed to solve issues, which can reduce costs, not to mention offering a much more attractive package of services to their users.

In conclusion, better network visibility is very important both to the provider of the service, and the client. The current IoT is hard to identify and even harder to manage properly, however, as technology evolves, artificial intelligence solutions that can fix that are being deployed this very second.

About CUJO AI:

CUJO AI is a nextgen artificial intelligence company that provides cybersecurity and device management solutions for network operators worldwide.

We personalize and secure connected experiences. CUJO AI platform solutions are delivered as a SaaS for all home network devices. It analyzes vast amounts of local network data and then uses proprietary machine learning algorithms to power the features.

CUJO AI platform includes:
- Advanced Device Identification
- AI Security
- Digital Parenting solutions

CUJO AI:
- Recognized as a Technology Pioneer 2018 by the World Economic Forum
- Listed as a “Vendor to Watch” and a “Cool Vendor in IoT Security” by an acclaimed research company Gartner.
- Official Member of Forbes Los Angeles Business Council.

In May 2018, the company has closed a strategic Series B round, led by Charter Communications, valuing the company in excess of $100M. For more information about CUJO AI, please visit https://www.cujo.com/