Device Intelligence – Helping Transform Connected Experiences

Table of Contents

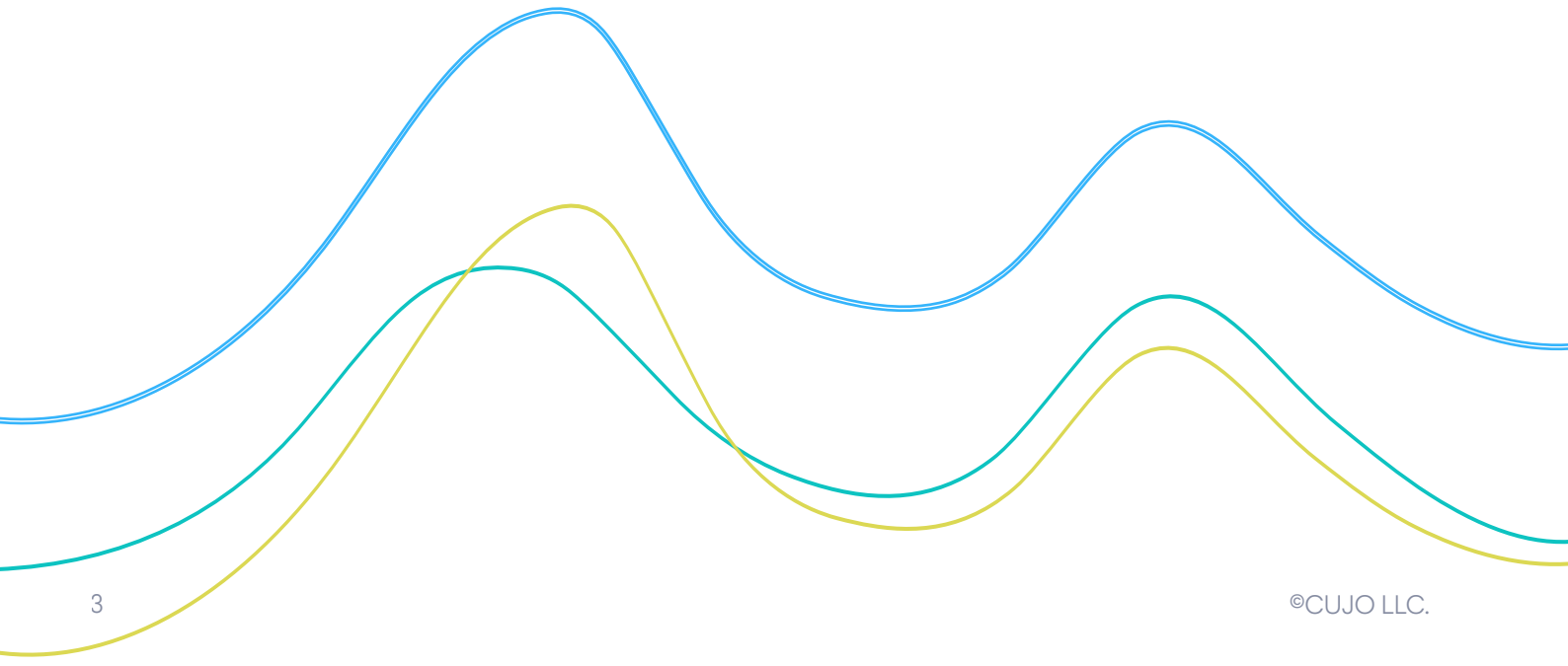
Overview

Consumers are using a larger variety of devices and have a growing need for more personalized and optimized connected experiences. To improve the connected experience inside the home, network service providers (NSPs) leverage an increasing number of tools and solutions.

At the same time, the industry is trending towards improved consumer data privacy, which affects the NSP's operational and value added services, including advanced Wi-Fi services, gaming, parental controls and digital protection.

As devices are increasingly obfuscated, NSPs cannot consistently identify devices and understand their capabilities.

To address these challenges, NSPs need a reliable, scalable, and efficient solution to identify devices and their capabilities.



Network Service Providers Are Between a Rock and a Hard Place

NSPs face several distinct industry trends that are compounding and putting pressure on their operations and cost model.

GROWING AND EVOLVING EXPECTATIONS OF THE CONNECTED EXPERIENCE

Consumers are using a growing number of different devices that require not just more bandwidth, but real-time and personalized, device type-based network optimization, especially on wireless connections.

NSPs are using a growing number of solutions that require device identities and context to optimize their connected experience through more intelligent Wi-Fi connectivity and value-added services.

DEVICE OBFUSCATION

Operating system (OS) providers are making devices harder to detect and identify, impacting NSPs' ability to detect and analyze issues, provide core services, and improve the connected experience for many end-users.

For NSPs, the costs of identifying obfuscated devices are growing, as multiple tools and vendors implement their own solutions.

Market Trends and the Scale of the Issue

Device obfuscation and the evolving expectations of the connected experience have a compounding effect on NSPs: they need device identities and device context to provide great connected experiences for every device, but a significant population of devices are becoming harder to identify.

DEVICE IDENTITY

A unique and anonymized device identifier that is assigned to every device on the network.

DEVICE CONTEXT

A device's capabilities and usage. It can include its type, manufacturer, model, as well as its OS and capabilities (such as 4K streaming or Wi-Fi technology support).

To quantify the scale of the issue, let's examine a few recent trends in consumer connectivity.

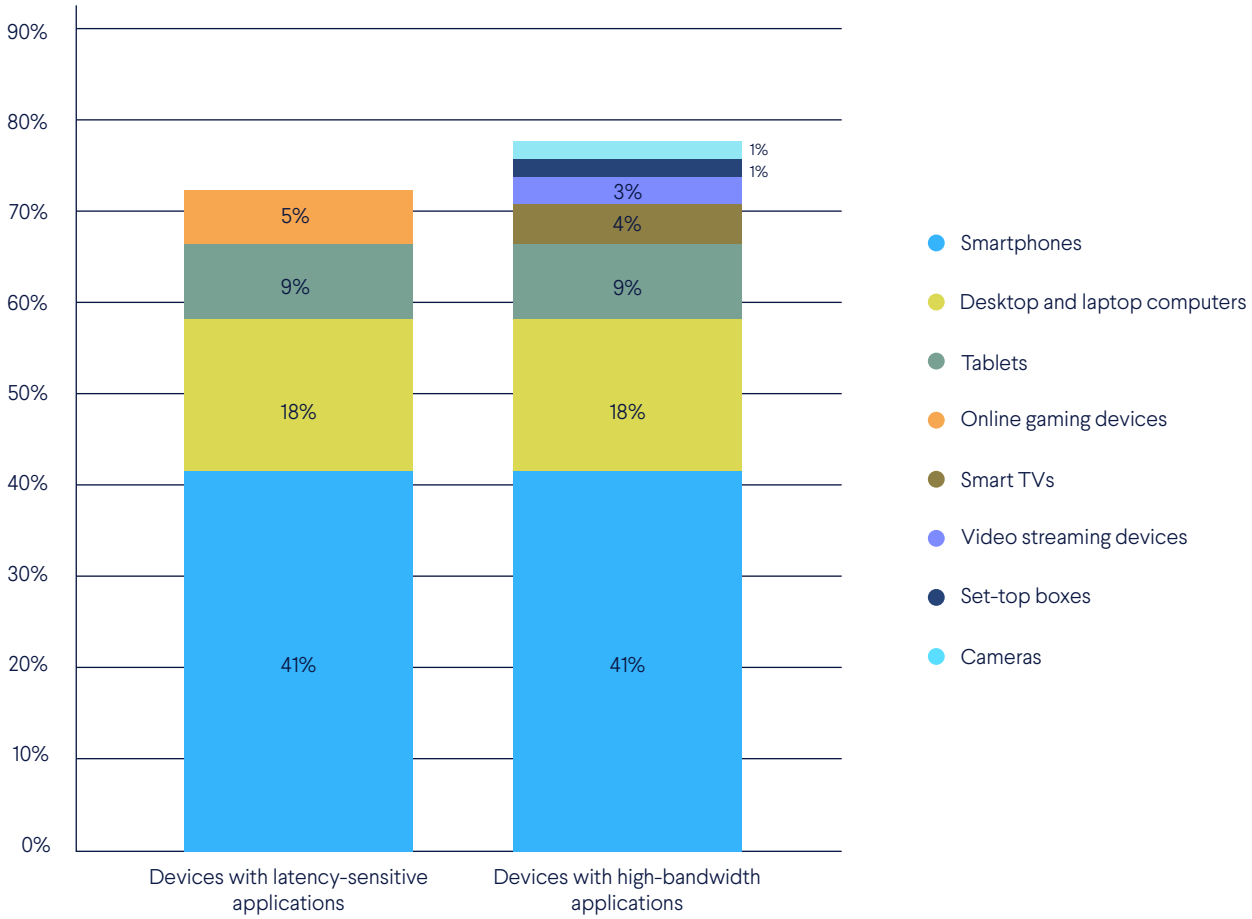
Most devices are used for latency-sensitive and high-bandwidth applications

Latency-sensitive devices increase the customers' expectations for the quality of service (QoS) that NSPs must provide. While end-users can be more lenient towards higher latency when streaming a show, online gaming and video calls cannot tolerate latency without a significant negative impact on the connected experience.

Remote work and education are often accompanied by latency-sensitive connectivity in the form of video conferences, remote presentations, and video conferences. Real-time communication with heavy upstream bandwidth requirements can be extremely challenging and must be a key priority for network service providers.

The shift towards remote work and schooling has also changed the distribution of network loads in residential areas. The Covid-19 pandemic has had a lasting effect on remote work. Our data shows how remote work has a substantial impact on connectivity and threat patterns in North America.

Most devices are used for latency-sensitive and high-bandwidth applications (CUJO AI Labs data, 2022)



Increasing background traffic: Background devices complicate network optimization

BACKGROUND DEVICES *(high-availability, best-effort devices)*

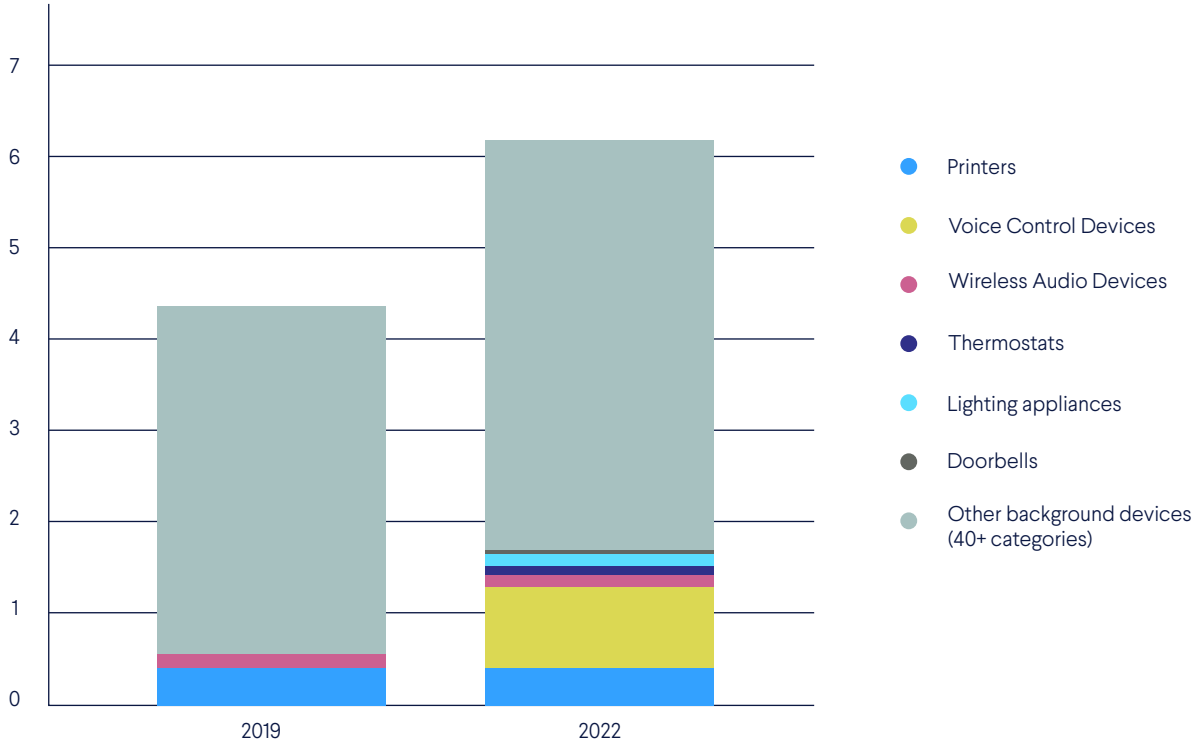
Are predominantly IoT devices that are not latency-sensitive and do not require a lot of bandwidth to provide a fully optimized connected experience for the consumer.

IoT devices, including wearables, already make up around 30% of all connected devices in the West. The Wi-Fi network can be optimized by improving the latency and bandwidth allocation for other devices at the home (for example, by connecting or moving background devices to specific Wi-Fi access points, extenders or the 2.4 GHz wireless band) without any impact on the background device's connectivity.

Wi-Fi optimization, such as band steering, is extremely complex when the network service provider cannot accurately identify background devices. Without knowing the precise context of a device, the NSP may overinvest to provide a great QoS when it is not needed.

Poorly identified background devices draw network capacity away from latency-sensitive devices. This is especially relevant as IoT device adoption is set to double in the next couple of years.

The growth of background devices in an average home (CUJO AI Labs data, 2022)

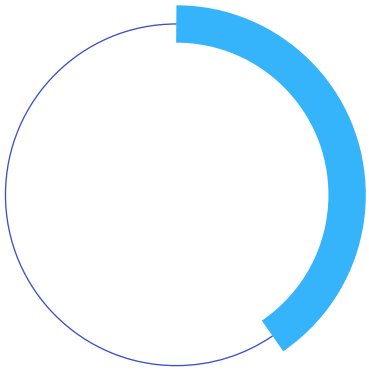


Consumers who have connectivity issues with their devices are **3-5 TIMES MORE LIKELY** to contact customer care agents.

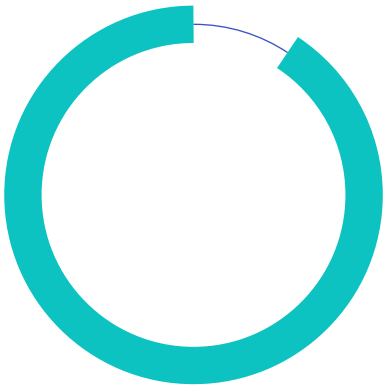
Less reliable network data: decreasing mobile device, laptop, and computer visibility

Smartphones, laptops, and computers make up over 50% of all connected devices. Since they are often used for latency-sensitive applications, such as video conferencing, it is important to monitor and optimize their quality of service. But doing this requires NSPs to identify these devices and distinguish them from IoT or other background devices.

Smartphones, laptops, and desktop computers are being increasingly obfuscated and anonymized for privacy, preventing NSPs from evaluating, analyzing or optimizing their experience.



From 2019 to 2023, the percentage of all new devices that randomized their MAC address grew **from 1% to 40%**



90% of home networks are already impacted by devices obfuscation

CUJO AI Labs data, 2022

Device Intelligence Is a Key Component of the Network Service Provider's Response to These Trends

More than ever, NSPs need to be able to consistently identify a unique device (device identity) and better understand device properties (device context).

This is key for providing great connected experiences for every device, especially when a significant population of **devices are becoming harder to identify**.

Without a reliable device intelligence solution, network service providers:

FACE

... degraded visibility into the device context and not having the data to intelligently set priorities for optimizing device connectivity, resulting in a degraded quality of service for individual devices.

... increased requirements for tech support as more customers engage customer care agents to resolve issues with their growing number of connected devices.

... growing risks of customer churn by failing to meet customer expectations for a connected experience.

SPEND MORE

... time to solve end-user issues and improve the customers' experience.

... money on upgrades and replacements of customer premises equipment.

STRUGGLE TO

... future-proof and improve their business with limited ability to their network for specific device types, such as 4K streaming.

... enforce device-based policies such as parental controls, authentication, or security.

... maintain accurate long-term wifi performance data for connected devices due to MAC address randomization.

Key Aspects of Device Intelligence

There are many factors that determine the ultimate requirements for a device intelligence solution to address the challenges outlined above. It is important to understand the specific use cases and prioritize which ones drive the most value for the NSP.

Here are some requirements that NSPs need to consider when looking at addressing their device intelligence challenges.

The Level of Precision

Device intelligence **goes beyond device identities** and provides useful device context, but how much context an NSP requires depends on the particular use case.

For example, knowing whether a device is an Apple iPhone or an Apple iPhone 14 Pro can be as relevant for both band steering as it is for engaging the end-user during a customer care call.

When optimizing the performance of a specific device, it is very useful to know as much context as possible, for example, which versions of 802.11 a device supports, understanding its capabilities and usage (gaming, video conferencing, streaming, etc.).

Device Identification Speed

How fast a device needs to be identified also varies. A few minutes may be fast enough when engaging the customer or reporting the devices connected to the home network.

But, if the network is trying to apply a policy to the device (e.g., content access controls or managing QoE), the device must be identified quickly (in seconds) at the specified level of accuracy to ensure the customer gets the best experience.

A key thing to consider is the **real-world identification speed** and not the metrics measured in a lab environment, which may not reflect the solution working at scale in a complex production environment.

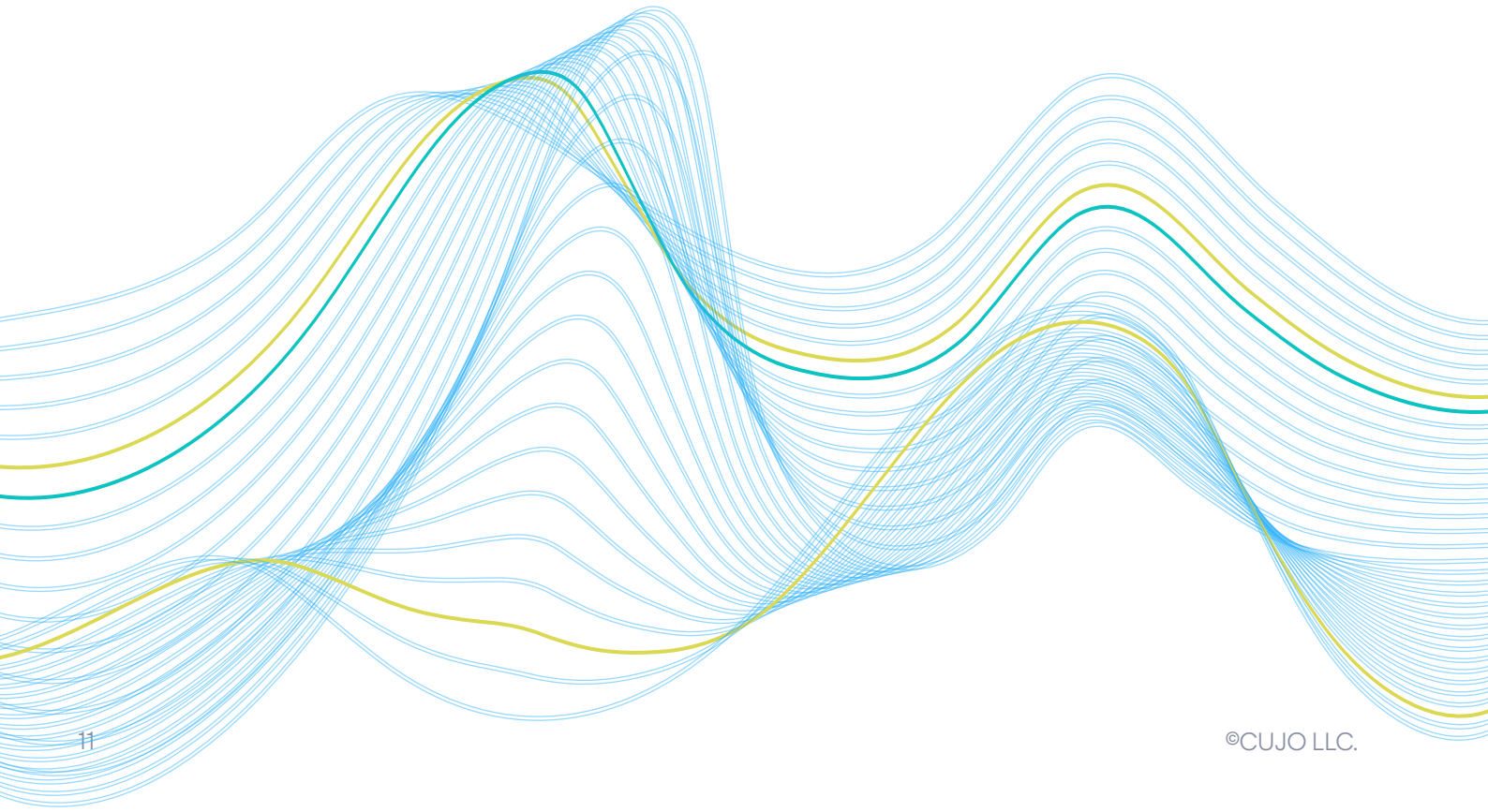
Scalability and Ease of Implementation

When evaluating a supplier of device intelligence, a key consideration is whether it has been deployed elsewhere and on similar CPE platforms. The number of deployments and CPE platforms can tell a lot about the ease of integration as well as the supplier's capability to support the deployments. The scale of those deployments can also act as a proxy for evaluating the cost efficiency of the solution.

Implementing device intelligence into any real-time network service provider's system and data analytics solution requires rapid API access and seamless integration. Thus, the supplier should have experience getting their customers up and running successfully, with projects in production to prove their claims.

Working with suppliers that have not proven that they can scale will add significant risk to any device intelligence project, which is why it is advisable to scope the scale of the partner's existing deployments.

Other considerations for deploying device intelligence should include the costs of data upload, storage, and the potential issue of using multiple non-stand-alone device intelligence technologies.



FIND OUT MORE

CUJO AI Explorer

CUJO AI Explorer is a stand-alone device intelligence solution. It uses machine learning algorithms trained on unmatched real-life data sets to identify devices and provide robust device context for network service providers without any noticeable impact on the connected experience.

Currently deployed on more than 50 million home networks, Explorer detects over 50,000 device models, with around 1,000 new device models added every month.

TO ARRANGE A DEMO and find out more about how device intelligence can help you, contact us at: connect@cujo.com

Media inquiries: press@cujo.com

Learn more: https://cujo.com