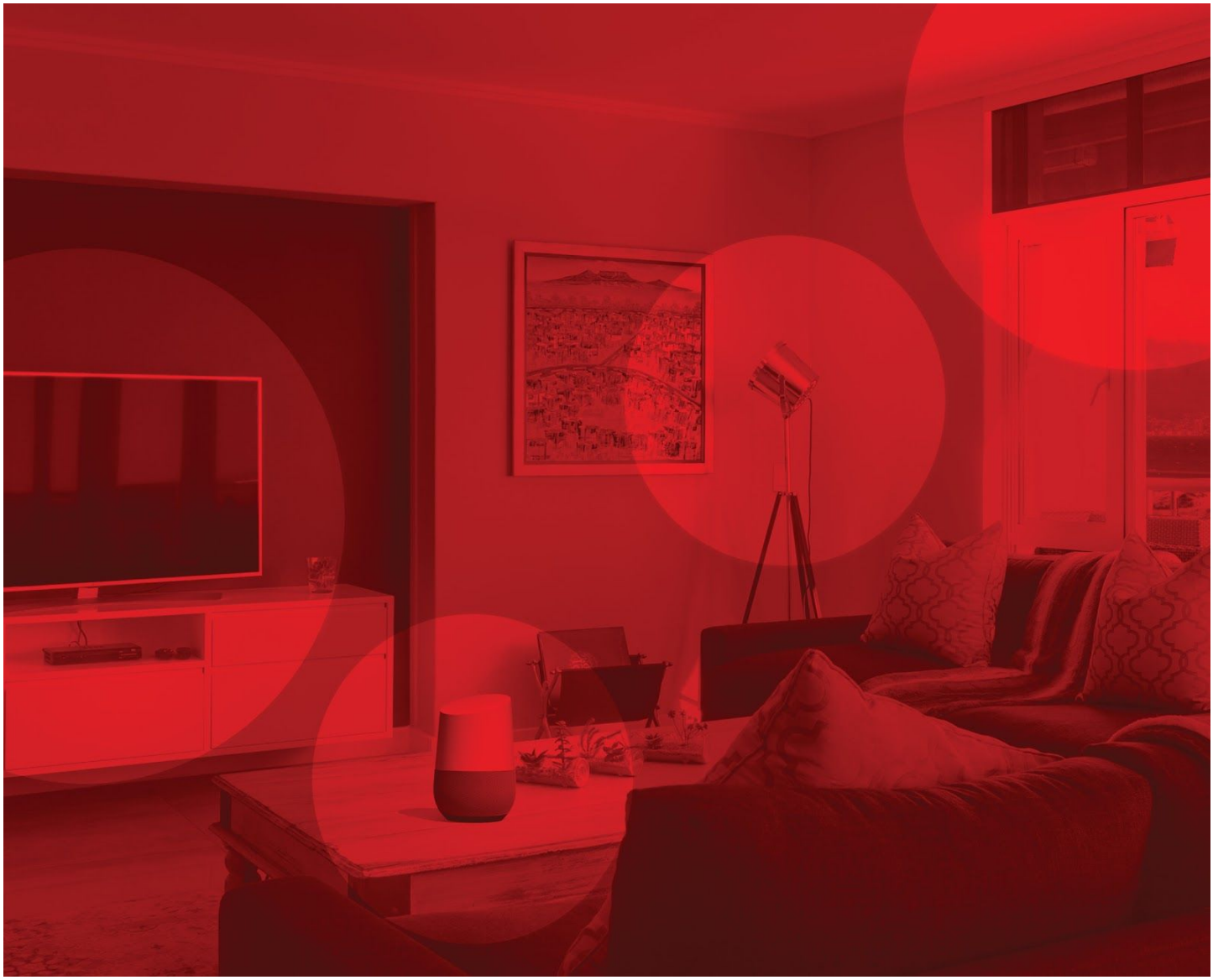
SCALED ACCESS

WHITEPAPER

The 5 Biggest Opportunities Access Management Offers Consumer IoT



Intro

Access management has up till now played an unnoticed role in the consumer Internet of Things (IoT). It's surprising because consumer IoT ecosystems are complex networks, requiring flexible yet secure access management to ensure their smooth running.

Here are the 5 biggest opportunities access management offers consumer IoT:

1. Improve the multi-user experience
2. Secure the device installation and hand over process
3. Secure the IoT infrastructure – device to back-end and device to device
4. Enforce consent and privacy choices in line with GDPR recommendations
5. Provide better insights into the userbase and device use

1. Improve The Multi-User Experience

The multi-user experience is the driving force behind the growth of IoT. People share smart home devices with their family and guests. Improving this experience - both the security and usability - is key to unlocking greater value.

Not all households are equal. Here are some examples how different relationships require different access:

Relationship	**Access level**
Parent - Child	Limited usage of the smart device
Homeowner - Household Staff	Access limited to the weekdays they come to work

Advanced access platforms provide predefined access rights for each relationship type so you don't have to do it all yourself.

“The multi-user experience is the driving force behind the growth of IoT. Improving this experience - both the security and usability - is key to unlocking greater value.”

Access limitations not only depend on relationships. There are other dimensions, such as:

Access Limitation	**Use Case**
Privacy	giving guests anonymous access (e.g. to people renting your home)
Payment	letting a user pay to access your device (e.g. an electric car charger)
Functionality	letting a user regulate smart lighting but not smart heating

2. Secure The Device Installation & Hand Over Process

Modern access platforms secure the device installation and hand over process.

Let’s take smart locks as an example. Currently, installers set up the device, then hand over the device credentials they used to install the device to the owner. This type of installation has two issues:

1. How can the homeowner ensure that only certified installers can install their device?
2. How can the homeowner ensure that the installer will not be able to access the device after they handed over the credentials?

Advanced access platforms solve the first issue by ensuring that the installer has been authenticated and verified as a certified installer before they get to install. These platforms use validation workflows to match the installer's certificates against an authoritative source.

The second issue is solved by giving the installer the ability to invite the homeowner to get access, without sharing credentials. The owner gets a separate administrator account.

As soon as the owner is set up, the installer loses access and can't operate the device without permission from the owner. If the same professional - or a different one - comes back for maintenance, they'll only be able to access the device after being given permission by the owner.

Once the maintenance has been completed, the admin can then easily disable access for the professional from the device, which ensures absolute security.

3. Secure the IoT Infrastructure

Access platforms help secure the ever growing IoT ecosystem and infrastructure. It's a simple, obvious, but definite statement.

Securing the IoT ecosystem is no longer simply about securing the 3-way communication between a user, a device, and the IoT back-end system.

The IoT landscape contains intercommunication between different devices and different back-end systems, and this infrastructure is continuing to expand. Leading research giants, Gartner, has predicted that by 2023 there will be 43 billion connected devices worldwide[1].

[1] Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2017, Gartner, December 2017, gartner.com

Increased growth means increased risk. Put simply: as the IoT ecosystem continues to grow so too does the risk of cyberattacks. Hackers have more entry points and routes to attack.

Info Security Magazine reports that 100 million cyberattacks on IoT endpoints were detected by a security vendor in the first half of 2019 alone[2]. It's worrying, to say the least.

State-of-the-art access management helps secure the landscape and communication between different entities. It provides access tokens to both IoT devices and IoT back-ends.

Using access tokens throughout the ecosystem helps ensure only authentic devices and back-end systems get access to the infrastructure.

The benefits of access tokens goes further, though. They remove the need for an application to require a user's credentials for every access request. This massively reduces the risk of a user's credentials being compromised and their device being targeted by a hacker to gain access to the back-end and attack the infrastructure.

"Access platforms help secure the ever growing IoT ecosystem and infrastructure. It's a simple, obvious, but definite statement."

[2] https://www.infosecurity-magazine.com/news/over-100-million-iot-attacks/

4. Enforce Consent & Privacy Choices in Line with GDPR Recommendations

When multiple people share a device, consent and privacy concerns need tackling:

- Sharing devices shouldn't automatically mean others get to see your personal information without your knowledge. How to enforce users' consent?
- Sharing devices shouldn't automatically mean that others get to see how you use the device. How to let users control this?

Access management tools give people this control. It ensures a user's consent is always enforced before access is given (denied or withdrawn) to their data. For example, a babysitter wouldn't be able to see personal details of the homeowner.

These platforms can also push a user's delete data request to any back-end system that stored personal information about them.

But, it goes further than that. They manage the lifecycle of a users' consent and ensure that a repository of all the recorded consents a user has given or denied over time, exists. Consent receipts can be retrieved, should unlawful data access disputes occur.

Users choose whether others can track how they use the device. The access platform enforces these choices. For example, you don't want your landlord to be able to see how you use devices.

5. Provide Better Insights Into The Userbase & Device Use

Finally, access management platforms help IoT vendors get better insights into how their devices are being used.

Consumer IoT devices, especially smart home appliances, are used by multiple users, yet vendors struggle to see who is actually using their device and how. By unlocking a more accurate userbase, this information can help IoT vendors in two areas: product management and marketing.

Advanced access platforms let device owners share their device with friends and family without sharing credentials. One device may be linked to multiple individual accounts. IoT vendors get to see how many users use their devices and how they actually interact on an individual level. This unique knowledge helps vendors improve their product management, build better products and target their marketing.

Conclusion

Access management within consumer IoT gives enormous benefits to device owners, users and vendors. And, as the consumer IoT continues to develop, so will the opportunities and importance of access platforms.

> **“Consumer IoT ecosystems are complex networks, requiring flexible yet secure access management to ensure their smooth running.”**