Home Network Security For Network Operators

CUJO AI

75.4 billion connected devices are expected to be online by 2025[1]. Technology giants like Amazon, Apple, Google focus on smart home and connectivity[2].

Leading companies are seeking to offer unique and habit-forming solutions in smart home automation, driven by Artificial Intelligence (AI). With a combination of hardware and AI, the tech leaders are aiming to create value, control data, and offer marketing solutions derived from home automation.

Why is Home Network Security a Primary Risk?

Homes Are More Connected. The amount of smartphones, laptops, tablets, gaming consoles, cameras and smart gadgets in our homes is growing rapidly.

Devices Are Insecure By Design. There is no security standard for smart home devices. Manufacturers prioritize low cost and speed-to-market over security.

Cyber Threat Landscape Grows. Cybercriminals use more sophisticated methods and release 100 000 new malware samples each day to target kids on their smart devices.

The lack of security is a massive risk for home users, but it is also a tremendous opportunity for Network Operators. They are in a unique position. They already have the hardware (broadband routers) deployed across millions of homes and can provide the necessary security for home users.

Network Operators can deploy AI solutions to control home automation, collect valuable insights, and implement new business models.

[1] https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016

[2] https://www.fastcompany.com/40474585/how-apple-facebook-amazon-and-google-use-ai-to-best-each-other

Protecting the Home Users

Securing home networks require several main steps. First, all devices on the network must be identified to make sure they all get the required protection. Then, preventive measures must be taken: troubleshooting ensues to find such vulnerabilities as open ports.

If any suspicious activities start to happen on the network (i.e., someone outside the network tries to access an IoT device), the connection gets blocked. And finally, the home user must be informed about the current status of their network to protect them against the future threats.

Using Network Security features, Network Operators can:

Increase Customer Retention. By reducing the possibility to get hacked and lose money, time or simply their internet speed, the customers will get a better service and experience.

Maximize Adoption Rate. With additional layers of security that clearly benefit their daily lives, the customers will be more likely to purchase premium services.

Lower the Costs of Service. Including endpoint and operating system intelligence, corrective security, security profiling and critical device offline alerts would would help various Network Operators' departments reduce costs and deliver value to their customers.

The Ultimate Solution Powered by AI

The CUJO AI Network Security service is designed to analyze and block online threats. The service uses predictive algorithms powered by Artificial Intelligence. It monitors metadata from the gateway, analyzes it in the Network Operator's cloud environment, and ensures a safe internet experience in real-time.

CUJO AI Security provides:

- **Security for all devices at home and on the go.** Protection from malware, phishing, ransomware, remote access for home and mobile devices.
- **Personalized WiFi Experience.** Blocking and whitelisting specific websites, prioritizing bandwidth and more.
- **Proactive protection from known and new threats.** Machine learning algorithms detect unusual device behavior and potentially harmful websites

Find out more about the service and get a full white paper at **cujo.com**

Contact our team for more information: **isp@getcujo.com**

Seamless & safe connected experiences with CUJO AI