Artificial Intelligence Drives the next Generation of Internet Security

CUJOAI

Sam Lee
Regional Director
sam.lee@cujo.com

CUJOAI

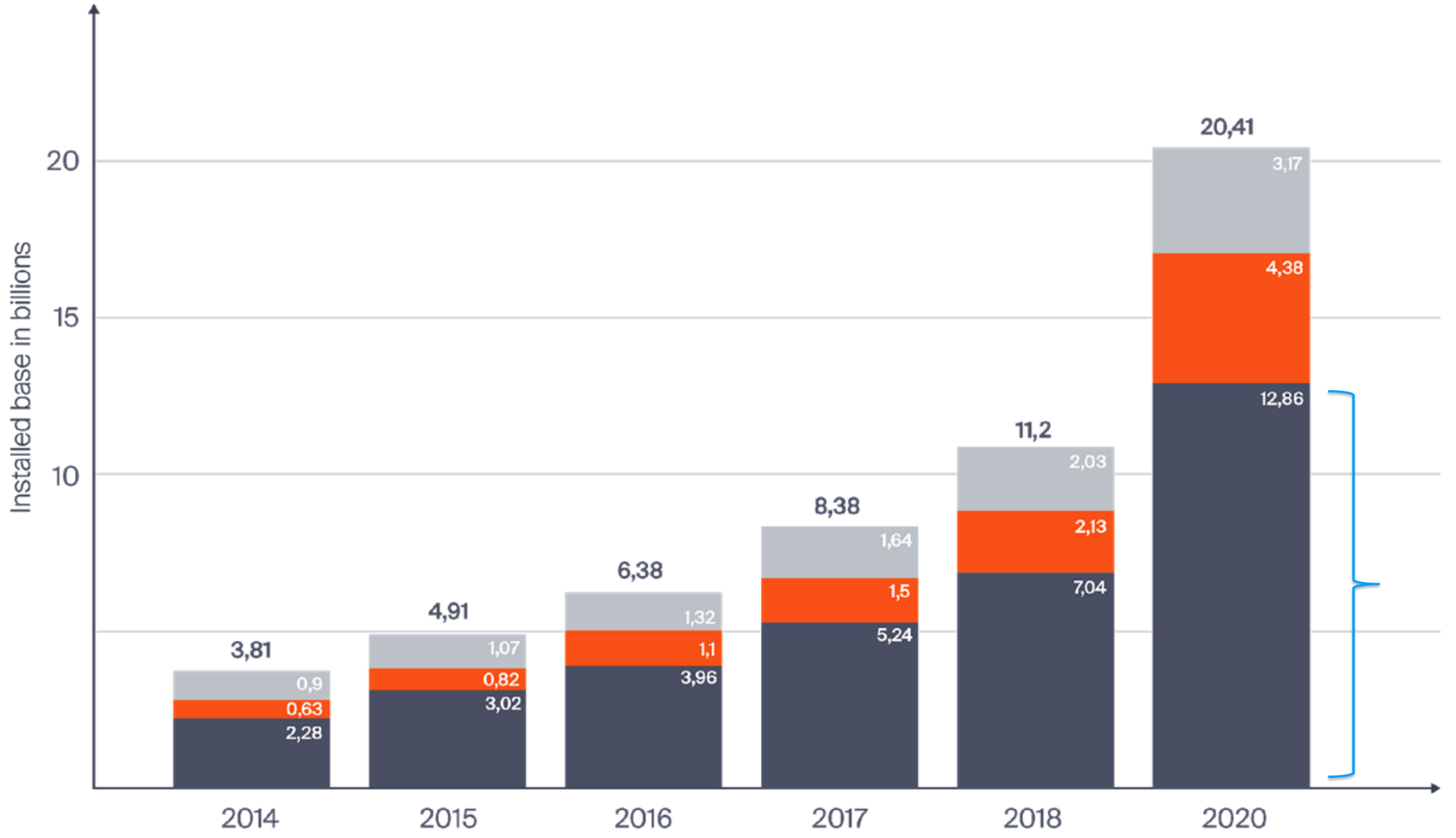

Artificial Intelligence Leads the Way

You Use Services Powered by Big Data and AI Already

Personalized experience, premium services, advanced insights

Growing Internet of Things

The number of connected devices will exceed **20 billion** by 2020



Source: Gartner (January 2017)

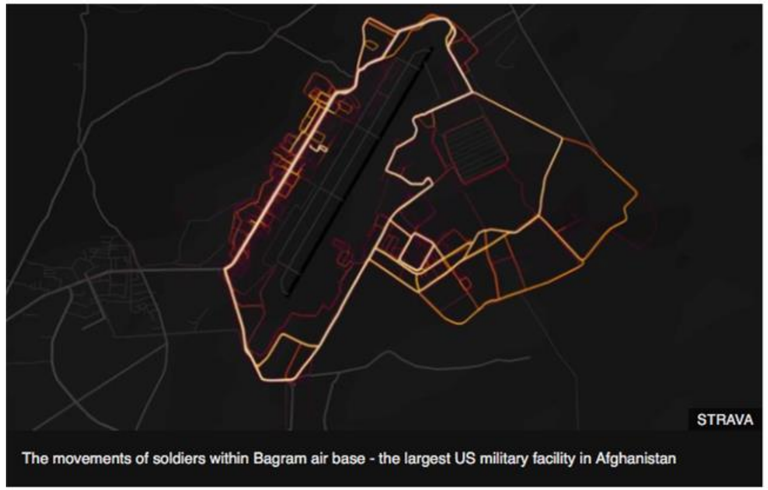
Consumer and SMB IoT is 63% of total

Attack Vectors on IoT

Smart Toys, Kettle Zombies, and Privacy Issues

Fitness app Strava lights up staff at military bases

29 January 2018 Share



The movements of soldiers within Bagram air base - the largest US military facility in Afghanistan

Hackable Holidays: Dangers of toys that spy on kids

By Megan Cloherty | @ClohertyWTOP
November 26, 2017 10:42 pm

Attack of the zombie kettles! How the UK is striking back against cybercrime

share 0

Smart devices - those connected to the internet - can be a new vector for cyber attacks

https://youtu.be/sZcsEweg5f8

AV-TEST
The Independent IT-Security Institute

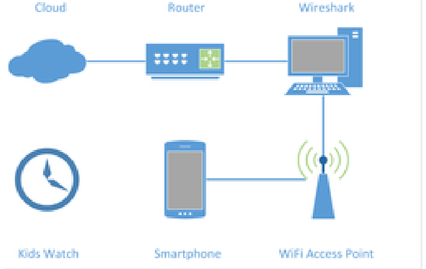
About the Institute | News | Tests | AWARD | Test Procedures | Statistics | Publications | Press | Contact

27th November 2017

Shock around the Clock! 6 children's watches in the test

Children's GPS trackers disguised as smart watches promise parents seamless digital supervision of their offspring. But the evaluation of six of the latest children's watches by the AV-Test Institute uncovered alarming security gaps. Several of them can even endanger children's safety.

Six GPS children's watches put to the test by the AV-TEST Institute.



According to the test configuration , there was an evaluation of the data traffic security, protection from manipulation, as well as handling of user data by the GPS children's watches.

Trust, but verify?

To whom would you entrust the most precious thing you have? When it comes to the safety of their children, parents rightly examine very carefully who appears to be trustworthy and who does not. How about the reputation of neighbors, leaders of children's groups and other people close to the family? The same applies when the question arises as to the freedoms that should be allowed to children: Walking from home to school with classmates, playing with friends outside without parental supervision? In terms of young people's developing confidence, these experiences are milestones, for parents as well, however.

Parents are clearly less critical towards technical tools for monitoring their children. According to the latest studies (in German), already one out of ten are using a GPS tracker. It is indeed true that buyers are primarily using the devices for their own navigation, when on vacation, for example, and for tracking pieces of luggage and house pets. But over 70 percent of those surveyed consider the trackers a good tool for safeguarding the safety of children and checking up on their offspring. A dangerous fallacy, as this test proves. Because none of the six examined tracker watches is immune to attacks, which can be launched without expert knowledge using software freely available on the Web. Yet, these attacks can be extremely dangerous for children.

Parental apps vulnerable to spying attempts

The security of the apps deployed for the communication between parents and children is also decisive, and was precisely evaluated in the lab accordingly. Here as well, two thirds of the watches revealed significant gaps. The app from CAT failed the app test. Among other things, this is due to the fact that it stored the login data unsecured in a log file on the SD card of the smartphone.

Login data captured in this manner offers attackers an additional opportunity to intercept information on the movement of children or to spy on and manipulate the communication. Only the provider Pingonaut, as well as the product from ANIO, were able to convince the testers in this test category. The apps from BELIO, hellOO and MyKi revealed slight vulnerabilities.

Data protection is child protection

In the course of use, the watches collect a large amount, and above all, sensitive data: Starting with the telephone numbers of the child and the people involved, in addition to location data, right down to vital signs. Based on all this information, comprehensive profiles can be created. Therefore, good data protection and an appropriately detailed privacy policy are indispensable. When reviewing the privacy policy and evaluating the apps, however, it turned out that only the providers Pingonaut and ANIO guarantee the data protection of their customers in an acceptable manner. Thus, both privacy policies promise judicious handling of user data. Pingonaut ensures anonymized processing of data and rules out its disclosure to third parties. In the app, and on the servers of the manufacturer, the location movements are also automatically deleted after 30 days. This is in direct contrast to the complete lack of an available privacy policy from hellOO. The remaining three providers were only able to earn a rating of satisfactory in this category. For instance, all three providers make no statement as to the duration of data storage.

Conclusion

The findings of this test are anything but reassuring. Solely based on the vulnerabilities resulting from call ID spoofing alone, the AV-Test Institute cannot recommend any of the tested GPS tracker watches for children.

Apart from this general risk, only the product offered by Pingonaut was able to win over the testers. A two-star rating each was in fact earned by the products from ANIO, BELIO and MyKi. The watches of the manufacturers hellOO and CAT failed due to severe security deficiencies and did not receive any of the three possible stars. Both products exhibited major defects, not only in the test category of external communication. The results of the evaluation of the app security of both providers, along with the lack of a privacy policy from hellOO, were significantly below the standard requirements.

◀ Back

The Internet Was Not Designed for Safety

Rapid growth leads to widespread issues

New threats

1339 data breaches were registered in the US in 2017

ITRC, 2017

Numerous devices

Typical household in the US today has 22 connected devices

CUJO AI data, 2018

Vulnerable networks

Average DDoS attack cost businesses $2.5M

ZDnet, 2017

Risky Connected Experience

Source: HP Fortify

90%

of devices collected at least one piece of personal information via the device, the cloud, or its mobile application

70%

of devices used unencrypted network traffic

80%

of devices along with their cloud and mobile application components failed to require passwords of a sufficient complexity and length

70%

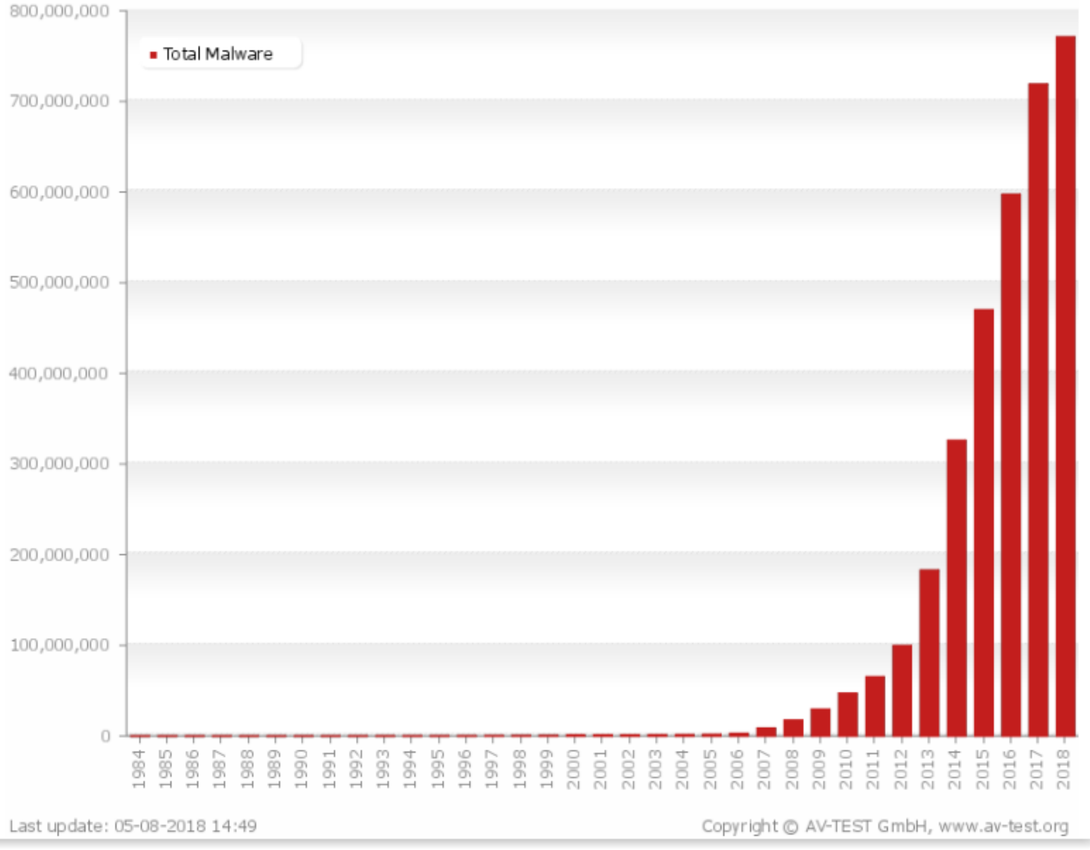
of devices along with their cloud and mobile application enable an attacker to identify valid user accounts through account enumeration

Malware

The AV-TEST Institute registers over 250,000 new malicious programs every day. These are examined using the analysis tools Sunshine and VTEST, classified according to their characteristics and saved. Visualisation programs then transform the results into diagrams that can be updated and produce current malware statistics.

Total Malware

All years | Last 10 years | Last 5 years | Last 24 months | Last 12 months

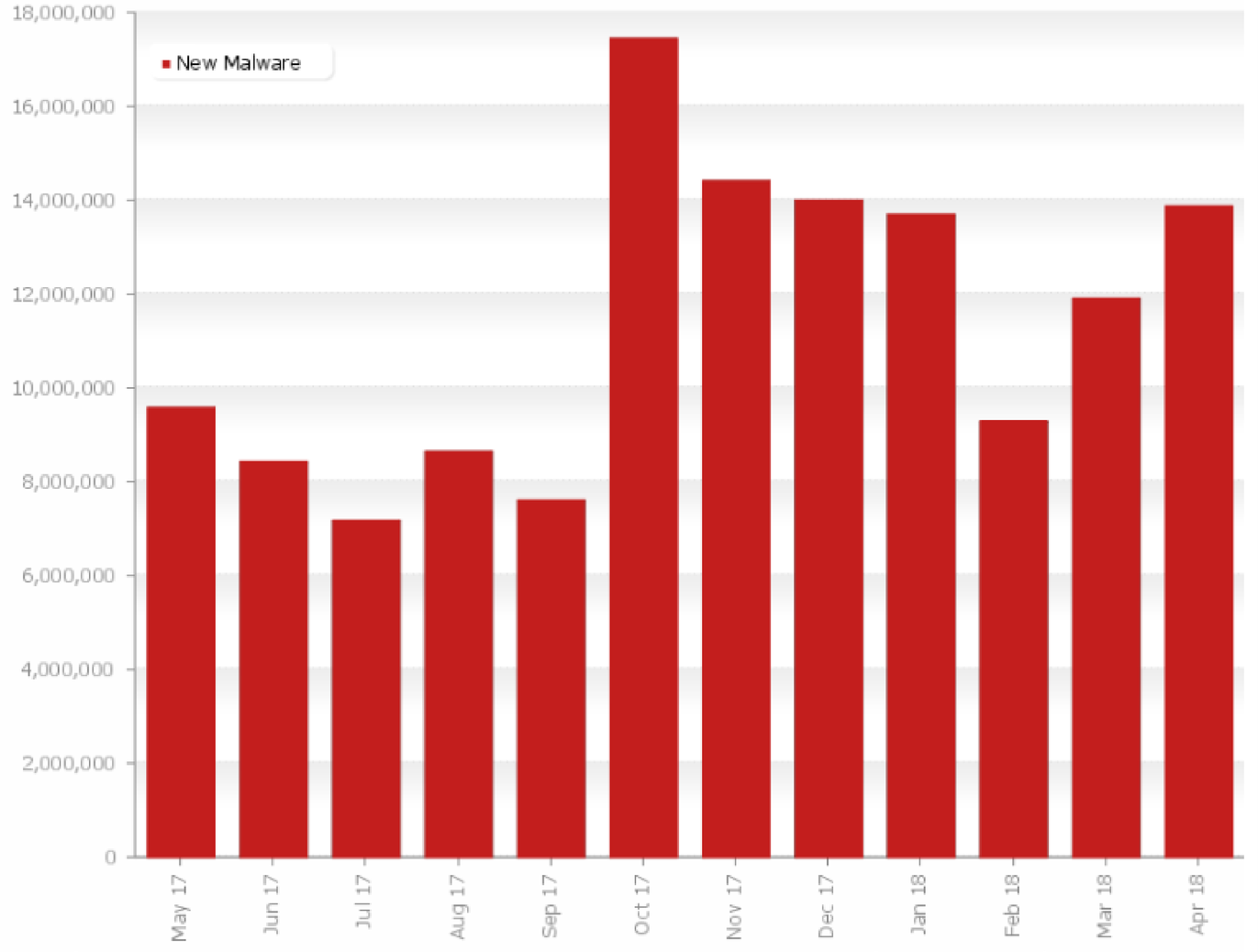


Last update: 05-08-2018 14:49

Copyright © AV-TEST GmbH, www.av-test.org

New Malware

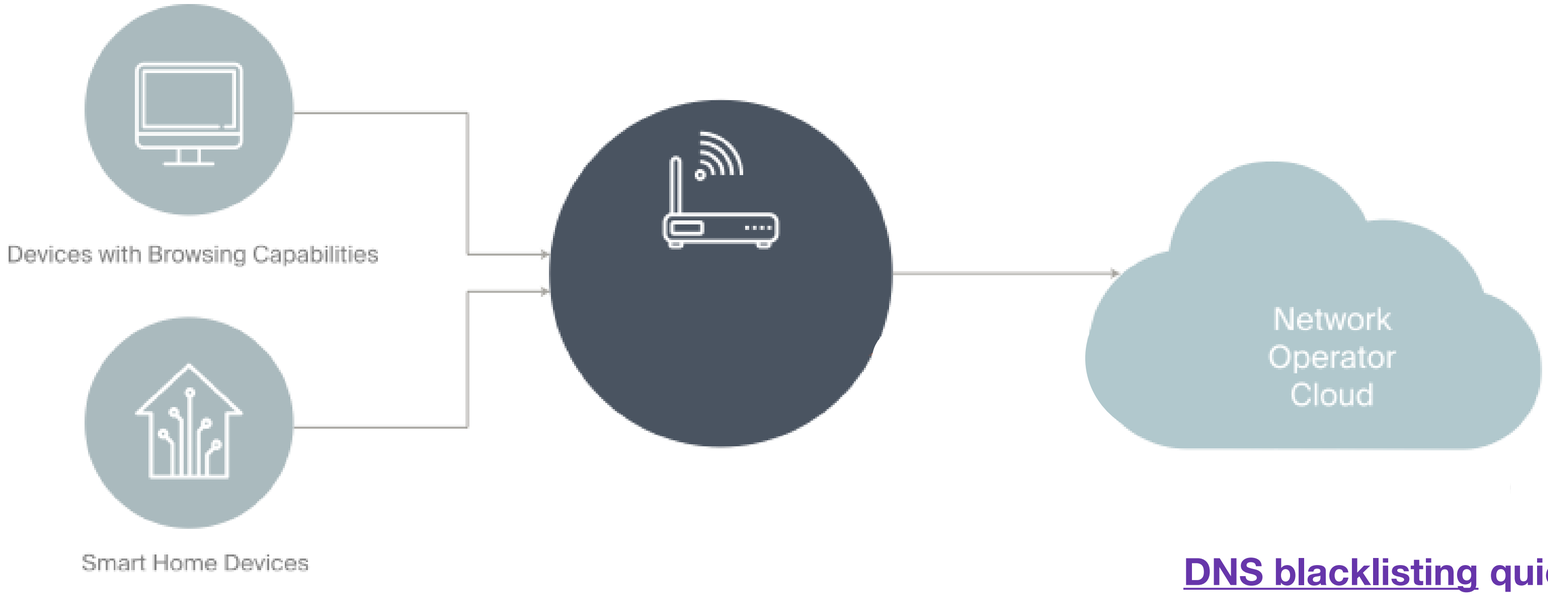
All years | Last 10 years | Last 5 years | Last 24 months | **Last 12 months**



Last update: 05-08-2018 14:49

Copyright © AV-TEST GmbH, www.av-test.org

Legacy Technologies Do Not Suffice When It Comes To Protecting Broadband Homes



Endpoint security solutions do not address risks associated with consumer IoT devices

DPI on firewall at the edge creates privacy concerns and drives up cost of broadband CPE

DNS blacklisting quickly becomes ineffective as a control point with trend towards encrypted DNS

Threat and reputation lists not enough to prevent zero-day phishing threats, ensure safe browsing and thwart IoT attack vectors

CUJOAI

Limitations of Current Technology

Consumer IoT space focus

	Current State of the Art	What is Required
Data Collection	• Honey Pots • Traditional threat intel gathering • Forensic investigations	• Collect data in millions of homes • Accurately identify IoT devices • Model normal behaviors
Threat Detection	• DPI on Firewall at edge of network • Endpoint solutions on LAN devices	• No DPI at the edge router • Leverage cloud-based AI/ML algorithms
Identification Methods	• Reactive • Based on what “bad” looks like • Pattern recognition	• Proactive • Based on what “good” looks like • Recognize anomalous behavior
Key Components	• Smart SecOps team and systems • Threat Lists • Hashes	• AI/ML Algorithms • Real-time analysis/assessment and categorization
Security/Policy Enforcement	• DNS • Endpoint Security • Enterprise-grade firewalls	• Residential Router

Artificial Intelligence, Machine Learning, or Deep Learning

What is the difference?

Artificial intelligence

An umbrella term for all programs that can sense, reason, etc. Intelligence presented by machines.

Machine learning

A subset of AI. Algorithm that makes better predictions when given more data.

Deep learning

A subset of machine learning that uses data to learn using neural networks

AI-Based Solutions

Human analysts cannot comprehend the amount of new data. Algorithms can.

Analyze data

IoT devices and online activities create huge amounts of data

Spot the pattern

ML algorithms can define the patterns from anonymized data

Offer a prediction

After comparing known data with the new data, the algorithm can offer precise predictions

Device Identification with AI

Precisely detecting all devices

Define Device Behavior

Each device has its own network behavior pattern, depending on its category and specific features.

Without knowing the pattern, it is not possible to properly protect these devices

Fingerprint and find the pattern

Fingerprinting all devices allows the ML algorithm to create different behavioral patterns for each device within a network

Offer Personalized Security

Precisely adapt security controls, predict potentially harmful behavior, block threats and get notified

Proactive Network Security with AI

Detecting threats without decrypting DNS traffic

Learn network behavior

Learn network and device behavior from big data sets. Identify which patterns are known-good and known-bad

Create behavioral profiles

After precising which behavior is considered malicious, the ML algorithms can create behavioral profiles for good and bad device or network behavior

Accurately predict threats

Known behavioral patterns are then used to block the threats that are showing malicious features

Contextual Alerts using AI

Detecting threats without compromising user privacy

Learn normal behavior

Learn appropriate and inappropriate content from big data sets. Identify which patterns are known-good (neutral, positive) and known-bad (insulting, negative).

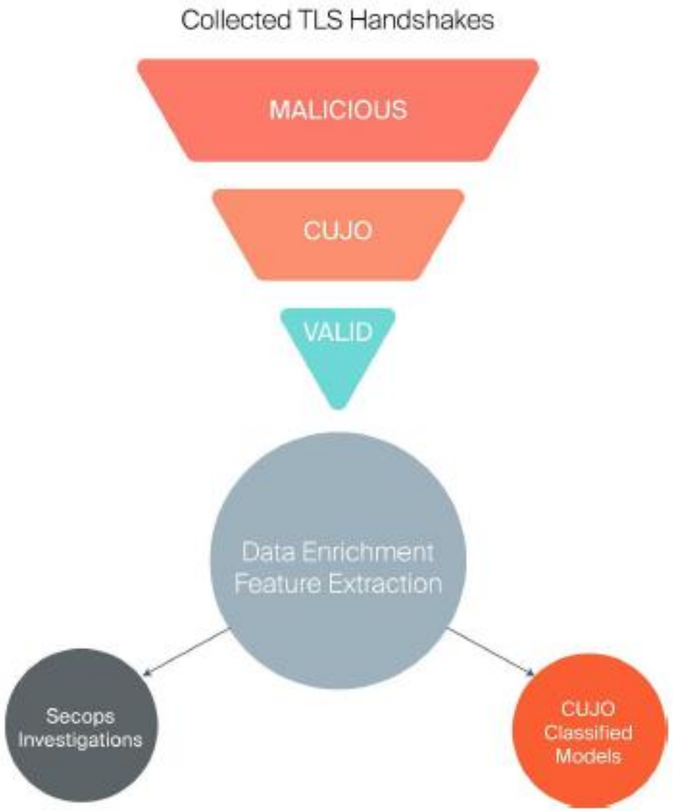
Create content profiles

After precising which content is considered negative, the ML algorithms can create behavioral profiles for good and bad content.

Accurately predict nuance

Block subtle and nuanced negative content (predatory, racist, bullying). Push a notification to alert the user.

User data stays private - the notification is automated.



Results

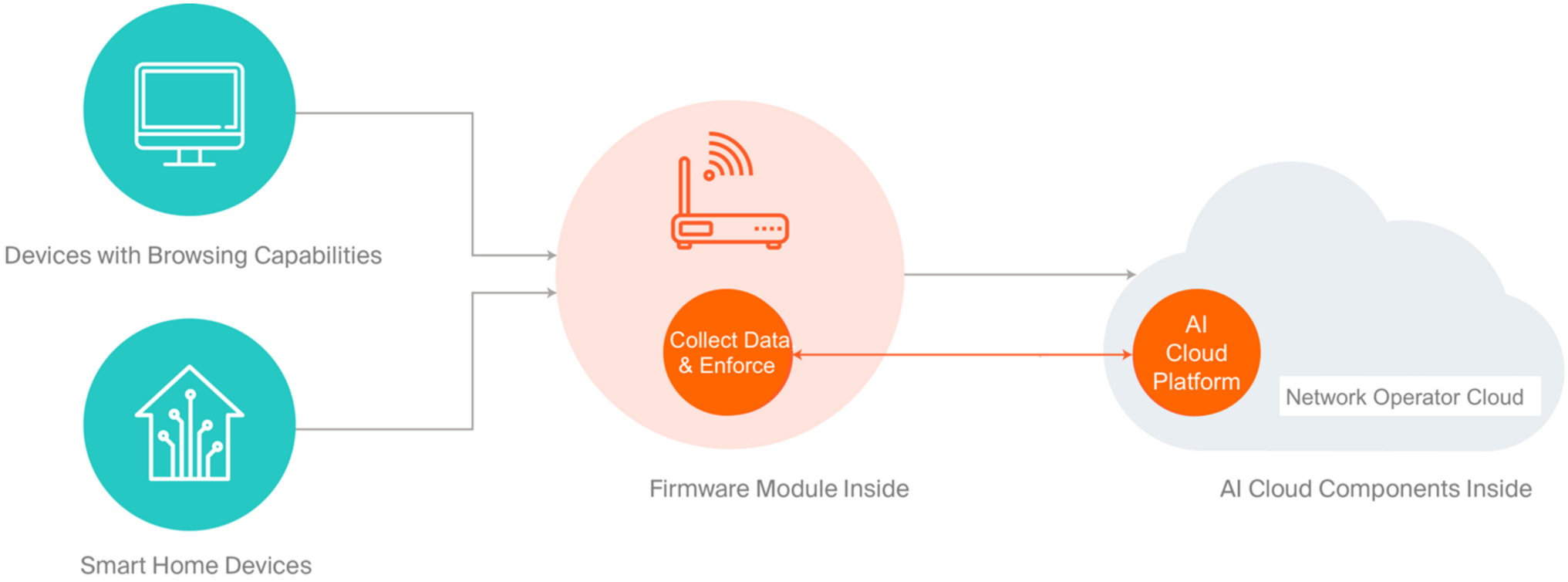
The results show an overall probability score of 0 to 100, with 0 meaning "no malicious intent" and 100 meaning the system is "certain of malicious intent".

url_score	5.8
reputation_score	0.5
tls_score	30.8
content_score	88.8
score	0.8

Check another URL

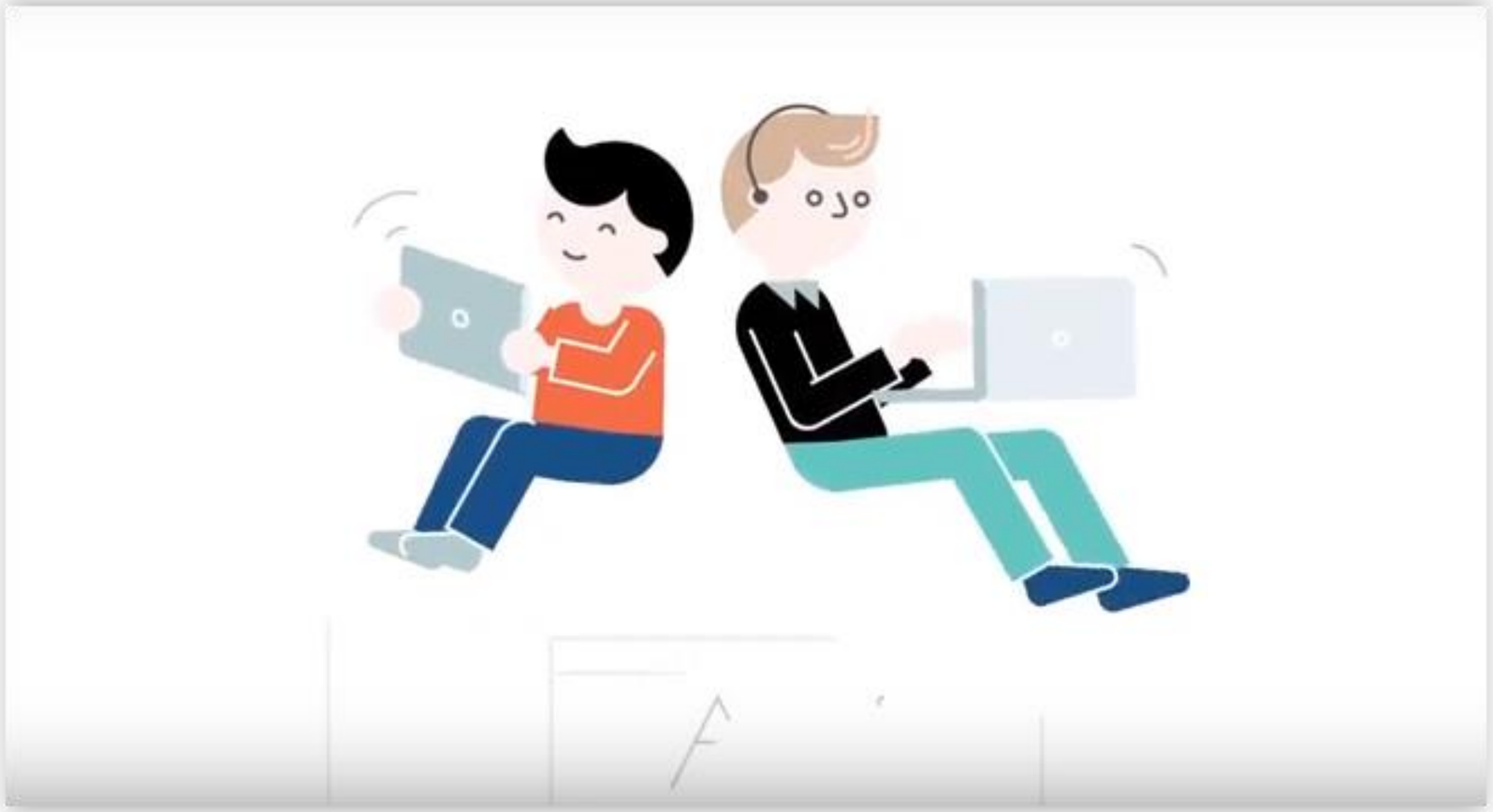
Adding AI-based IoT Security Services

To a network operator's broadband portfolio

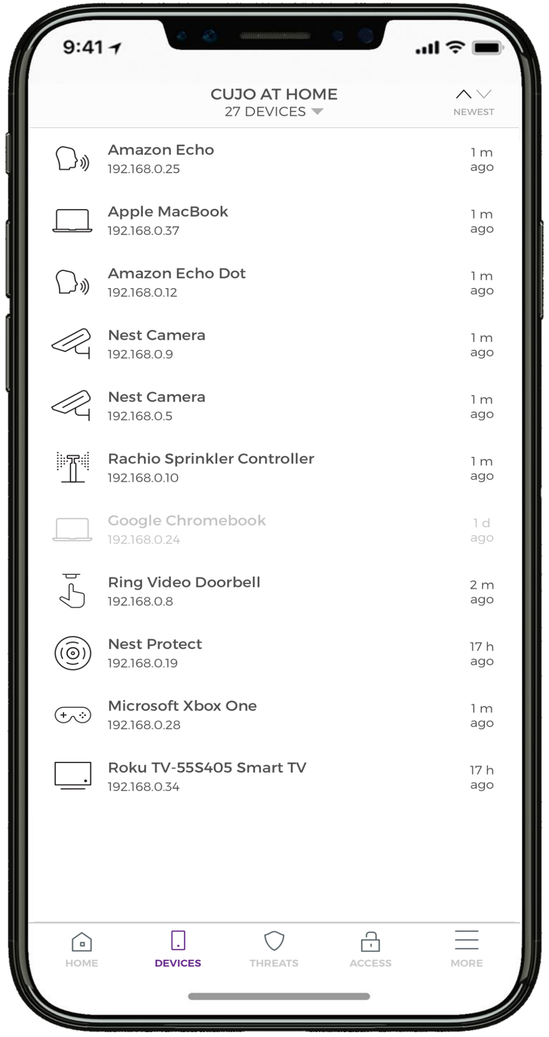


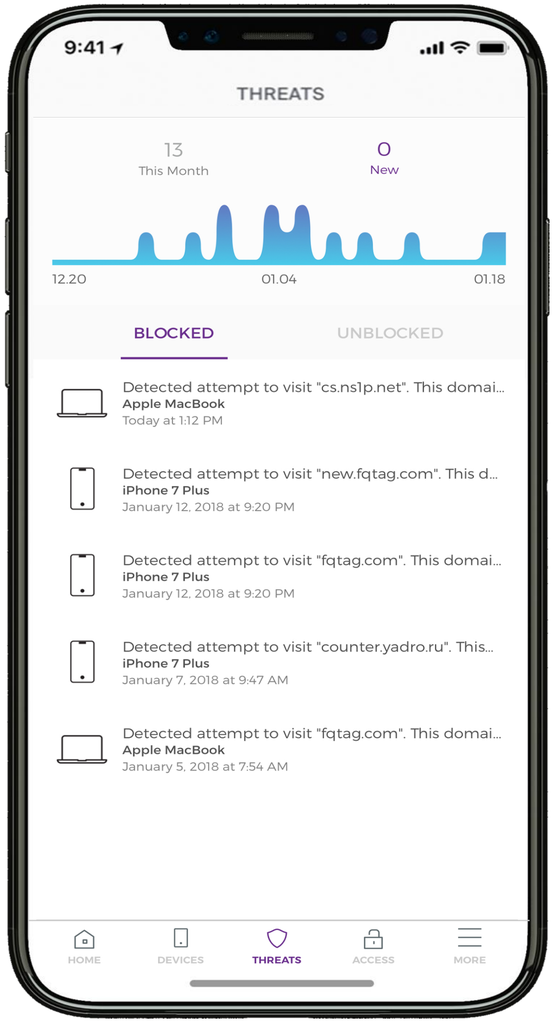
https://youtu.be/3eycVPEQQDE

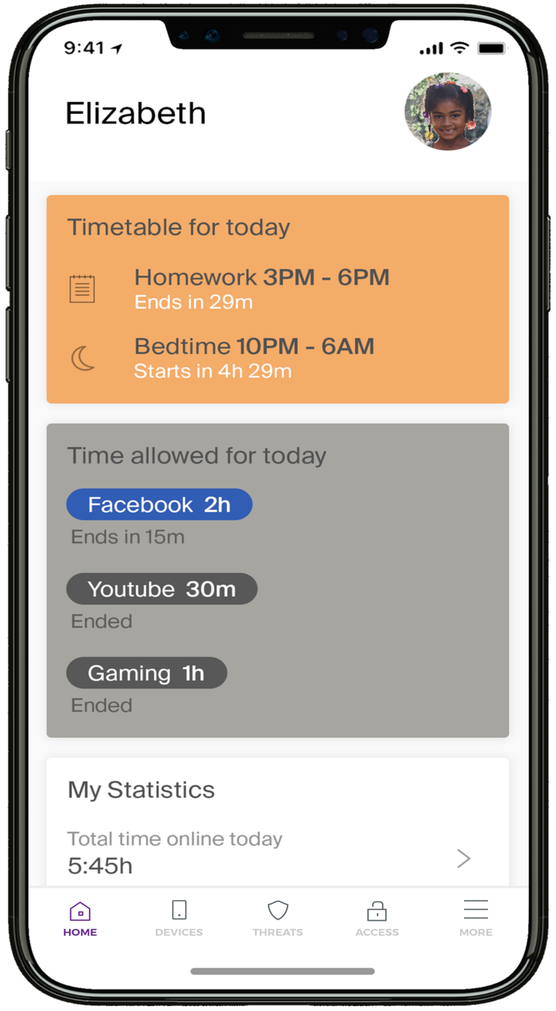
Example on what AI can do for protecting children



I want My Devices to work for Me







The Ultimate Choice Powered by AI

Simple and Intuitive

Understand your network and know what devices are on it. Connect seamlessly, keep your family safe and enjoy a personalized experience.

In and Out of Home

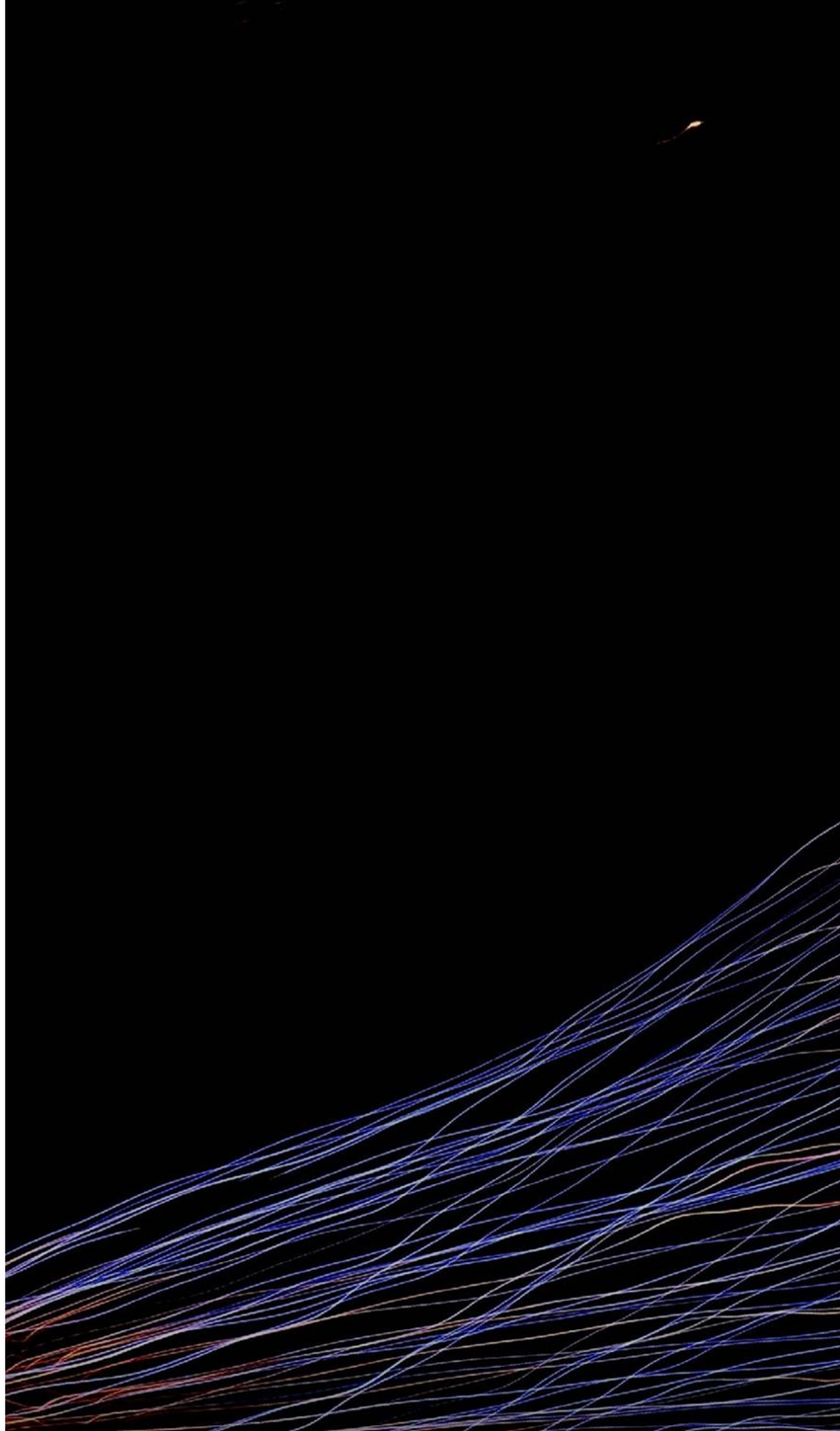
Make sure your devices are protected against malware, phishing and other threats in and out of the home. No matter which OS or device you are using.

Protected Children

Help your children build a healthy relationship with technology. Schedule, set limits, block content. Protect kids from threats.

Summary

- Current state of the internet does not fit the needs of the users
- New devices are constantly added to home networks
- Cyber threat landscape is growing
- Legacy security methods are not effective
- Artificial intelligence provides proactive and private solution



CUJOAI

The CUJO AI Platform provides network operators a software solution consisting of:

- AI security
- Advanced device identification
- Advanced parental controls
- Network analytics

CUJOAI

Sam Lee
Regional Director
sam.lee@cujo.com