SERENIoT

Distributed Network Security Policy Management and Enforcement for Smart Homes

ACSAC 2020, December 7–11, 2020

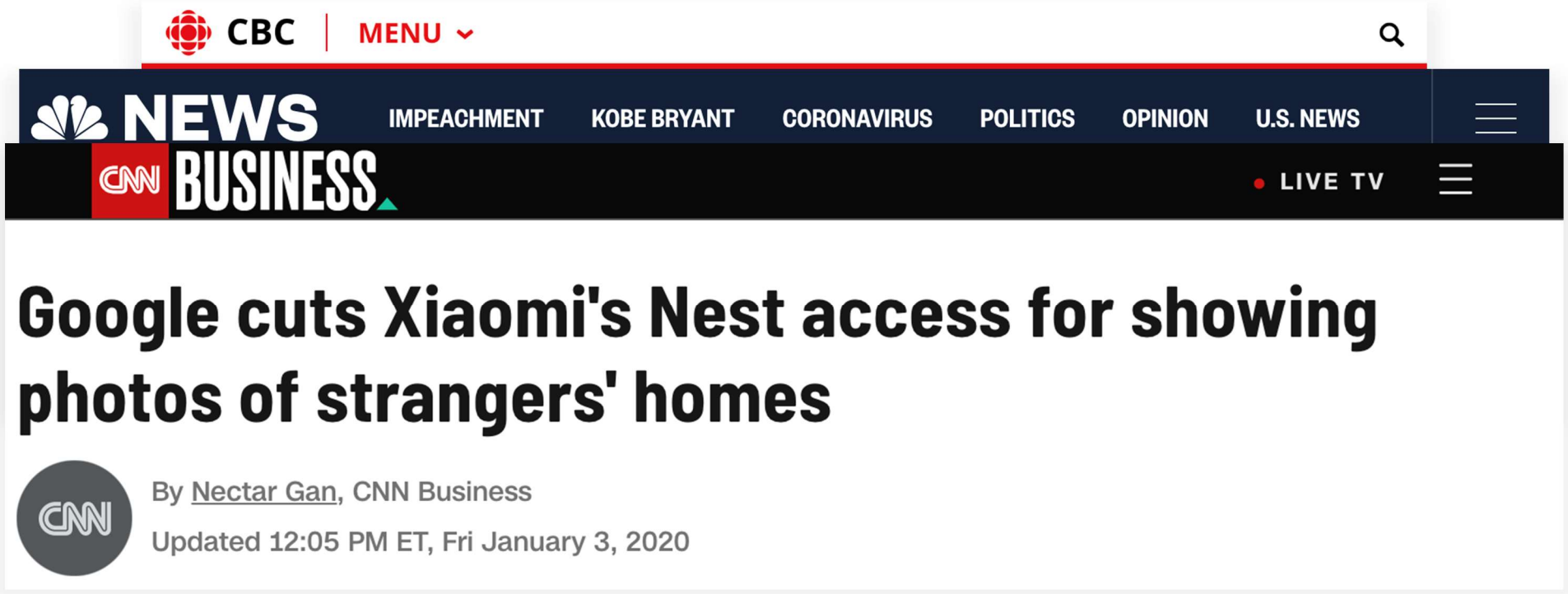
2020/10/12

Corentin THOMASSET
David BARRERA

Corentin THOMASSET

Master's Student - Polytechnique Montréal

Supervised by David Barrera


CBC
MENU
NEWS
IMPEACHMENT
KOBE BRYANT
CORONAVIRUS
POLITICS
OPINION
U.S. NEWS
CNN BUSINESS
LIVE TV
Google cuts Xiaomi's Nest access for showing photos of strangers' homes
By Nectar Gan, CNN Business
Updated 12:05 PM ET, Fri January 3, 2020

40%

of smart homes globally have at least one vulnerable device.

1:Avast. Avast smart home security report 2019.

Security risks of smart homes

Privacy

Attacker can intercept / access private data.

Physical Security

Attacks on IoT devices can have repercussions in the real world.

Cybersecurity

Attacks on IoT devices can have repercussions on computer systems and infrastructures.

SERENIoT

Distributed Network Security Policy Management and Enforcement for Smart Homes

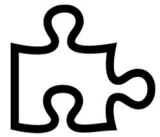
(Serenity)

Goals

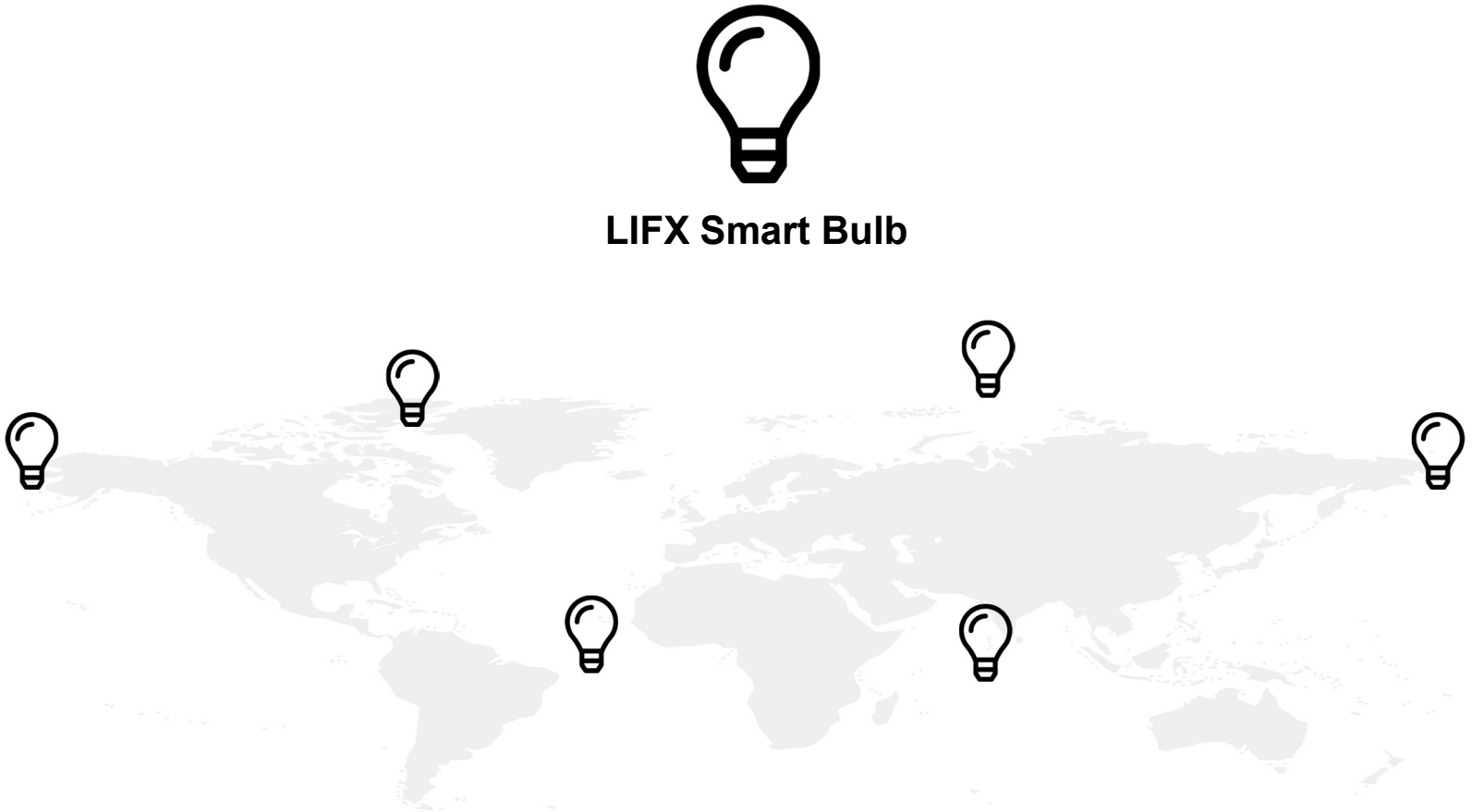
Protect
Smart Homes and consumer IoT against device hijacking.

User friendly
Autonomous & tailored for home use.

Independent
From manufacters and other third parties.

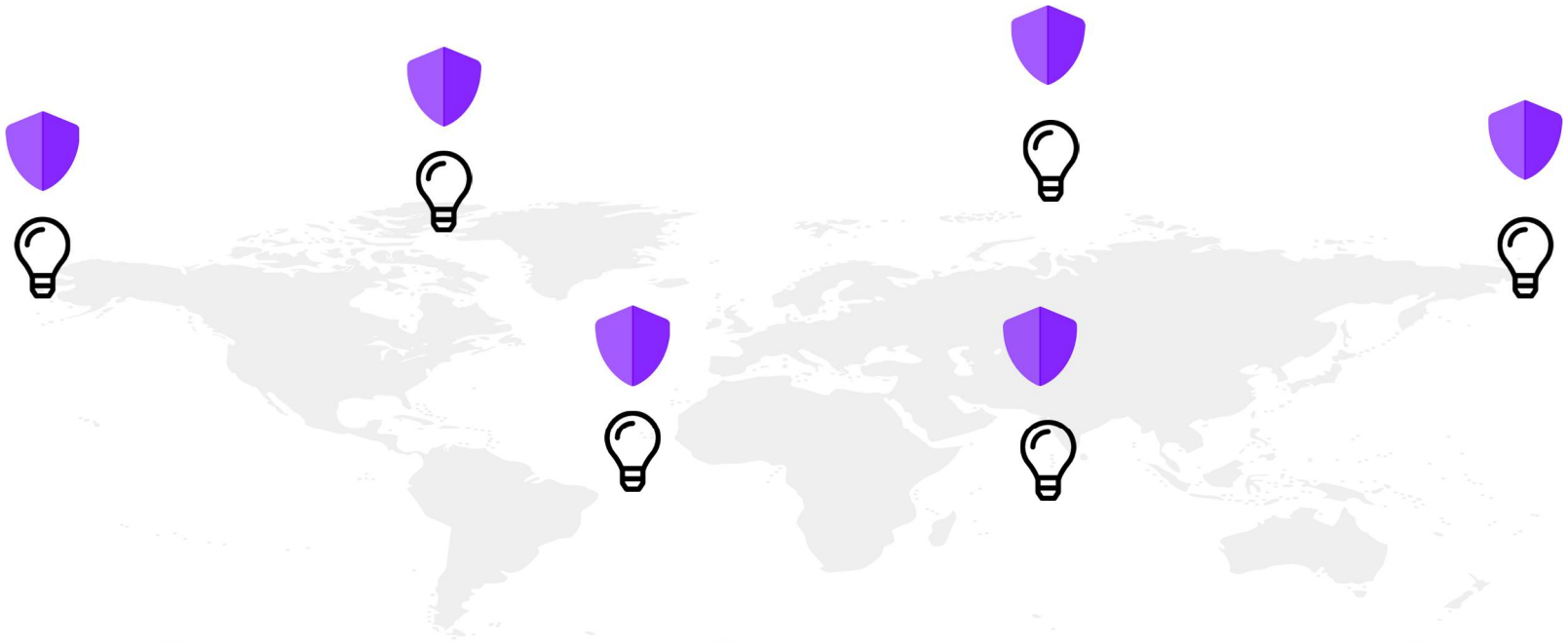


Compatible
With existing and future IoT devices.



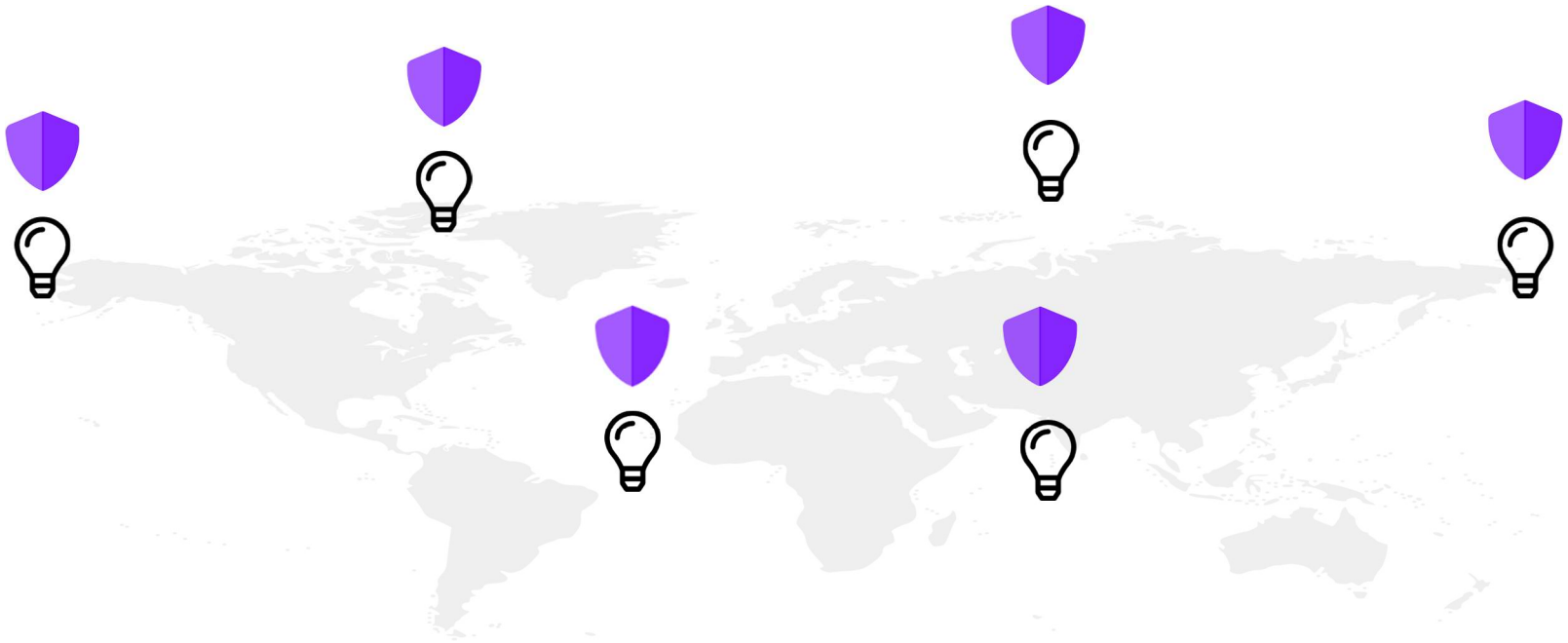
IoT devices are monitored in different locations

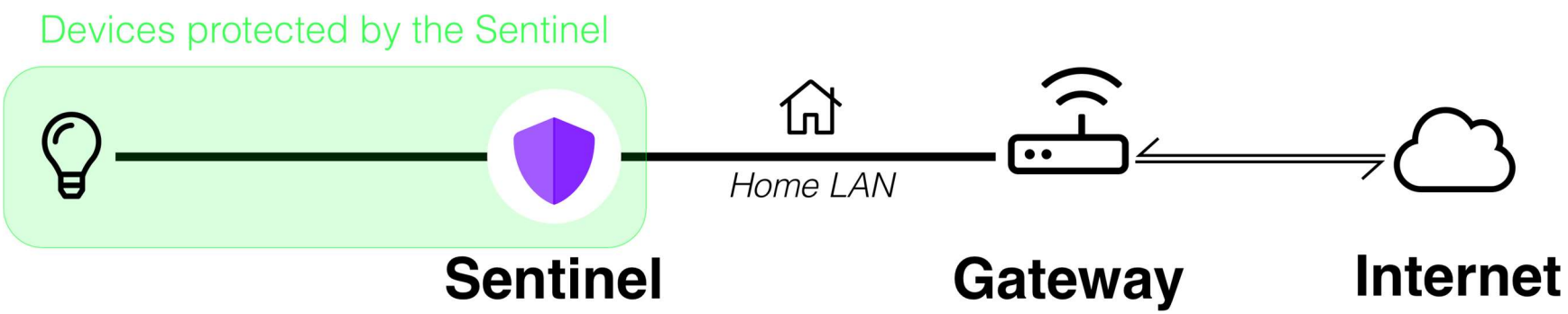
Sentinels



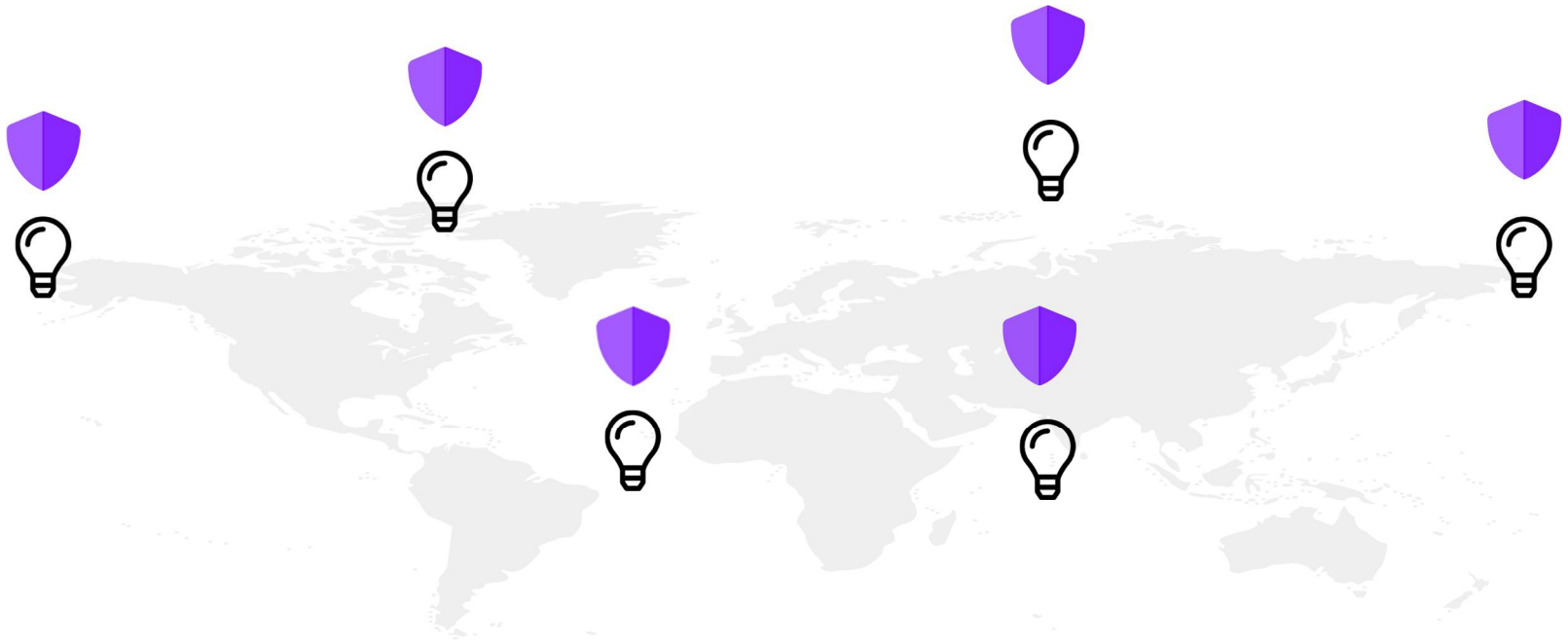
Sentinels analyse and filter the devices' network trafic.

Sentinels

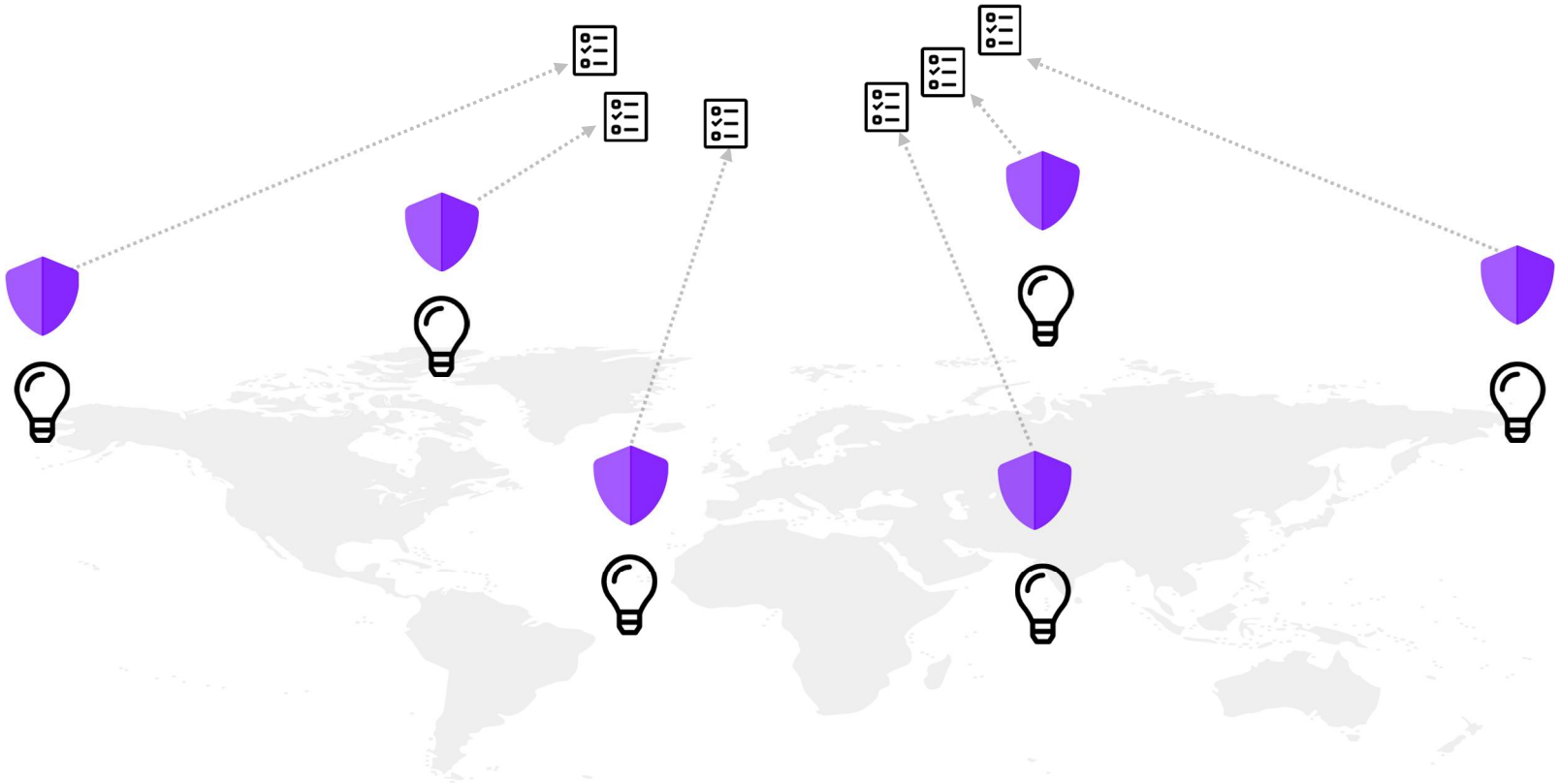



Devices protected by the Sentinel
Home LAN
Sentinel
Gateway
Internet

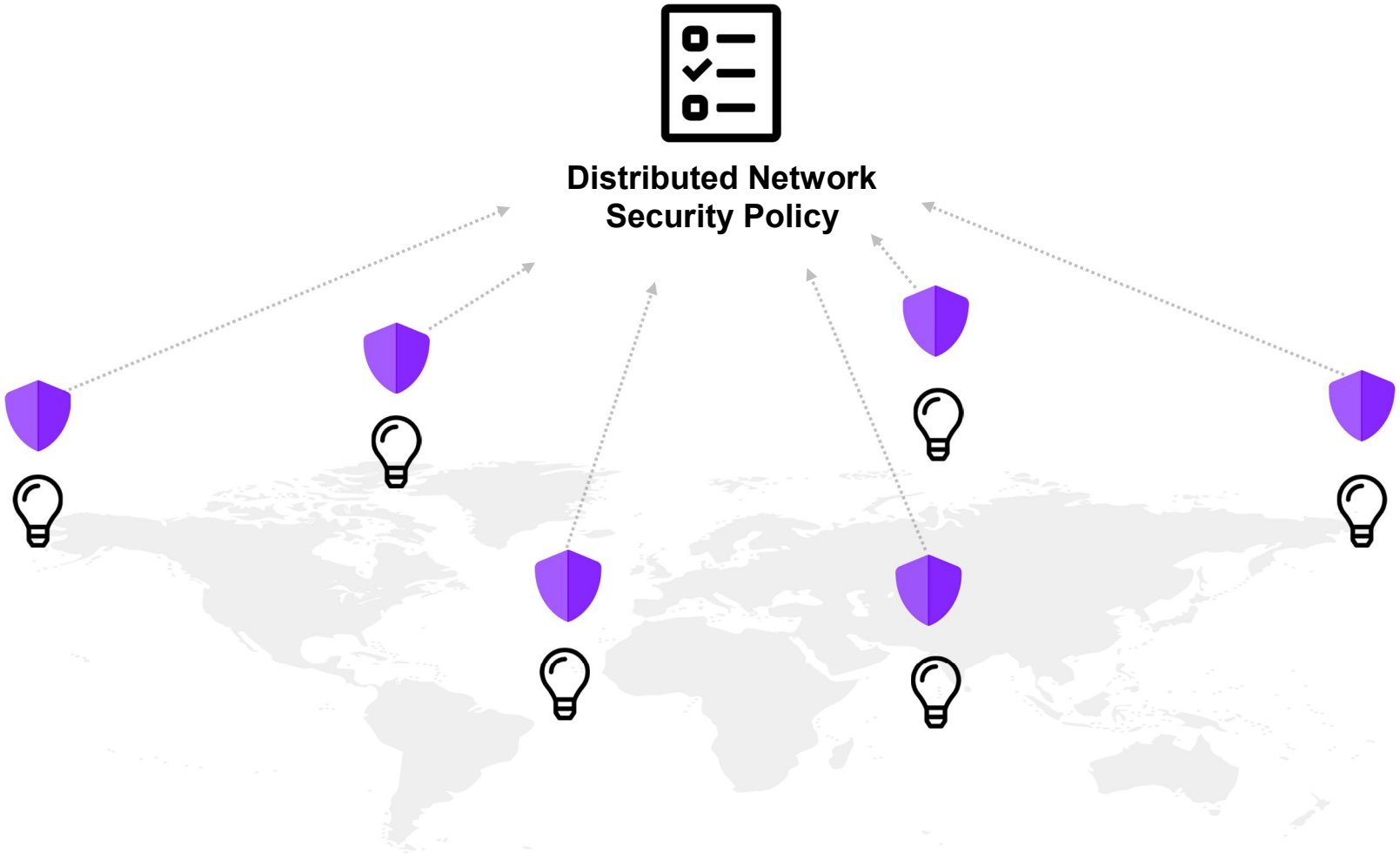
II - METHODOLOGY



II - METHODOLOGY

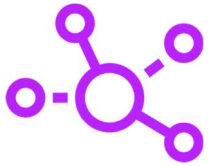


II - METHODOLOGY



Sentinels

Sentinels filter and analyse the devices network trafic. One Sentinel is deployed per home. Sentinels collaborate to build the policies.



Blockchain

The blockchain provides the decentralised ledger used to record Sentinels' observations and build the policies.

Allow list

Security policies list packet signatures corresponding to behaviors observed by a majority of Sentinels.

Sentinels' workflow

1- Intercept

2- Compute signature

3- Check security policy

4- Make decision

Packet signatures

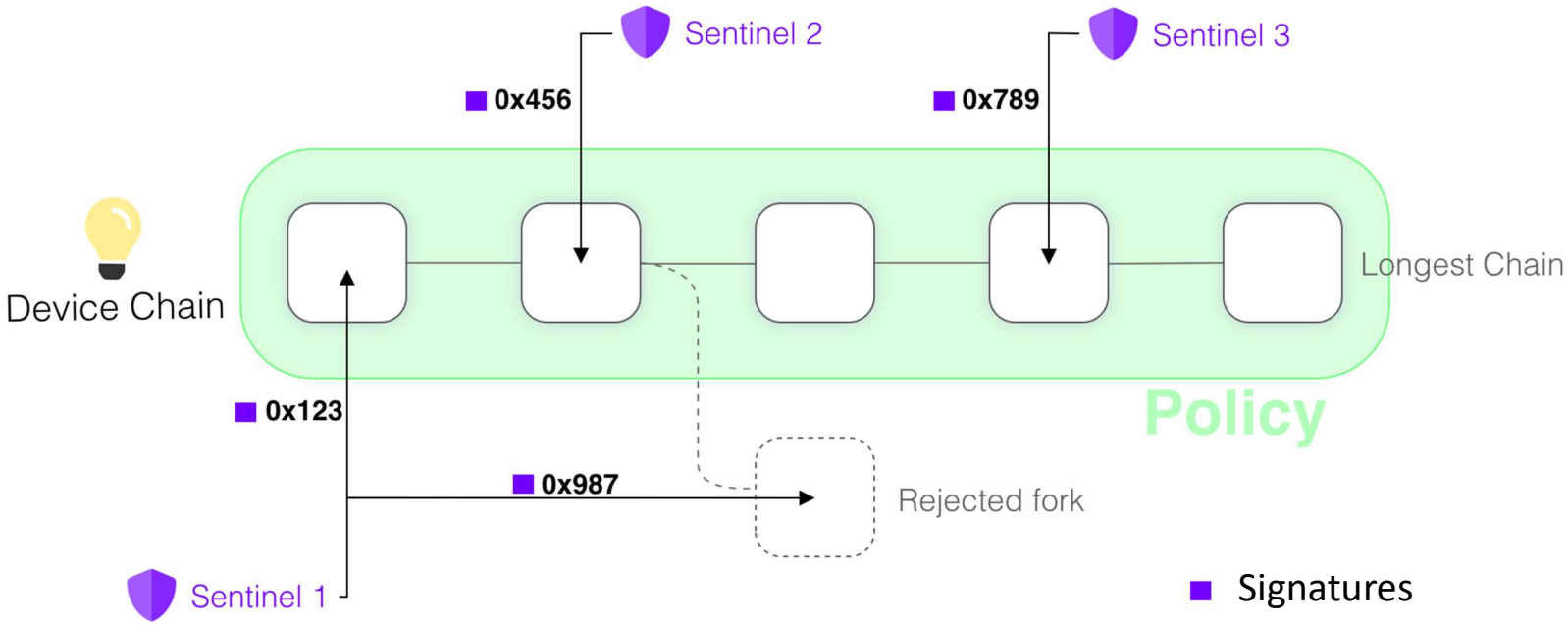
IP payload protocol ID

Destination L: Local, R: Remote

= SHA-256(protocol, host domain, L | R, service port);

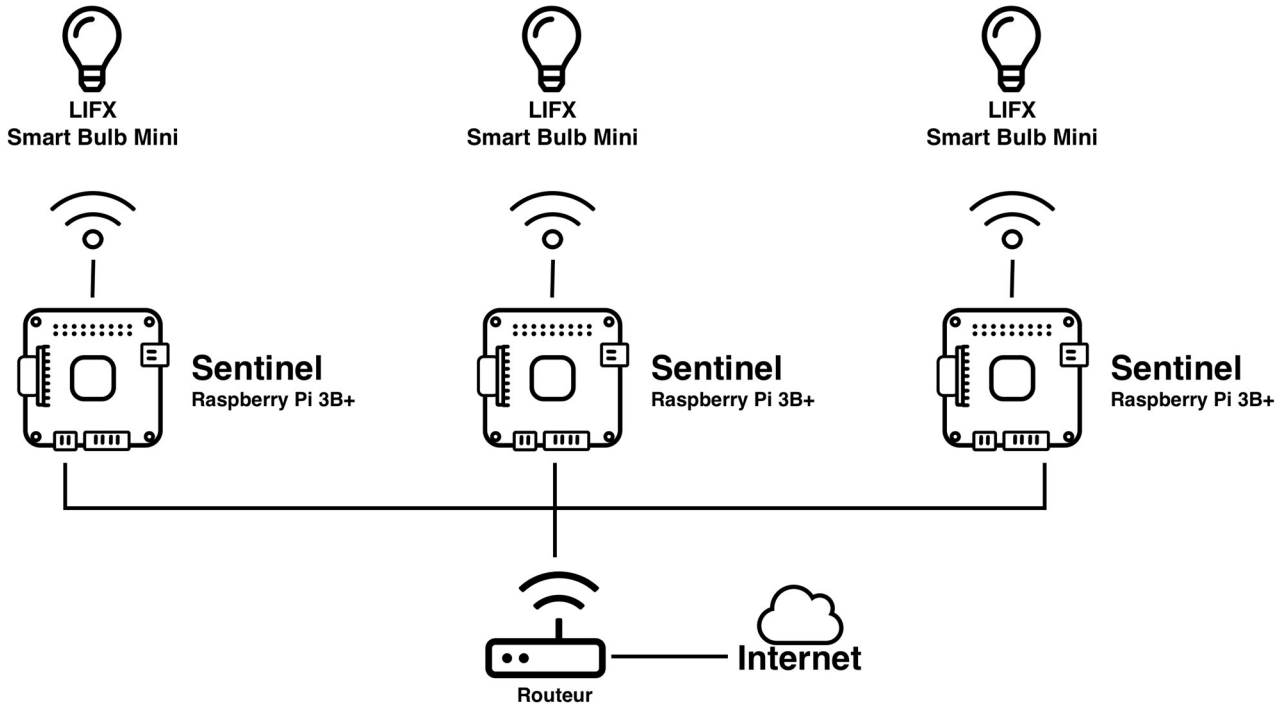
or dest IP if domain is unavailable

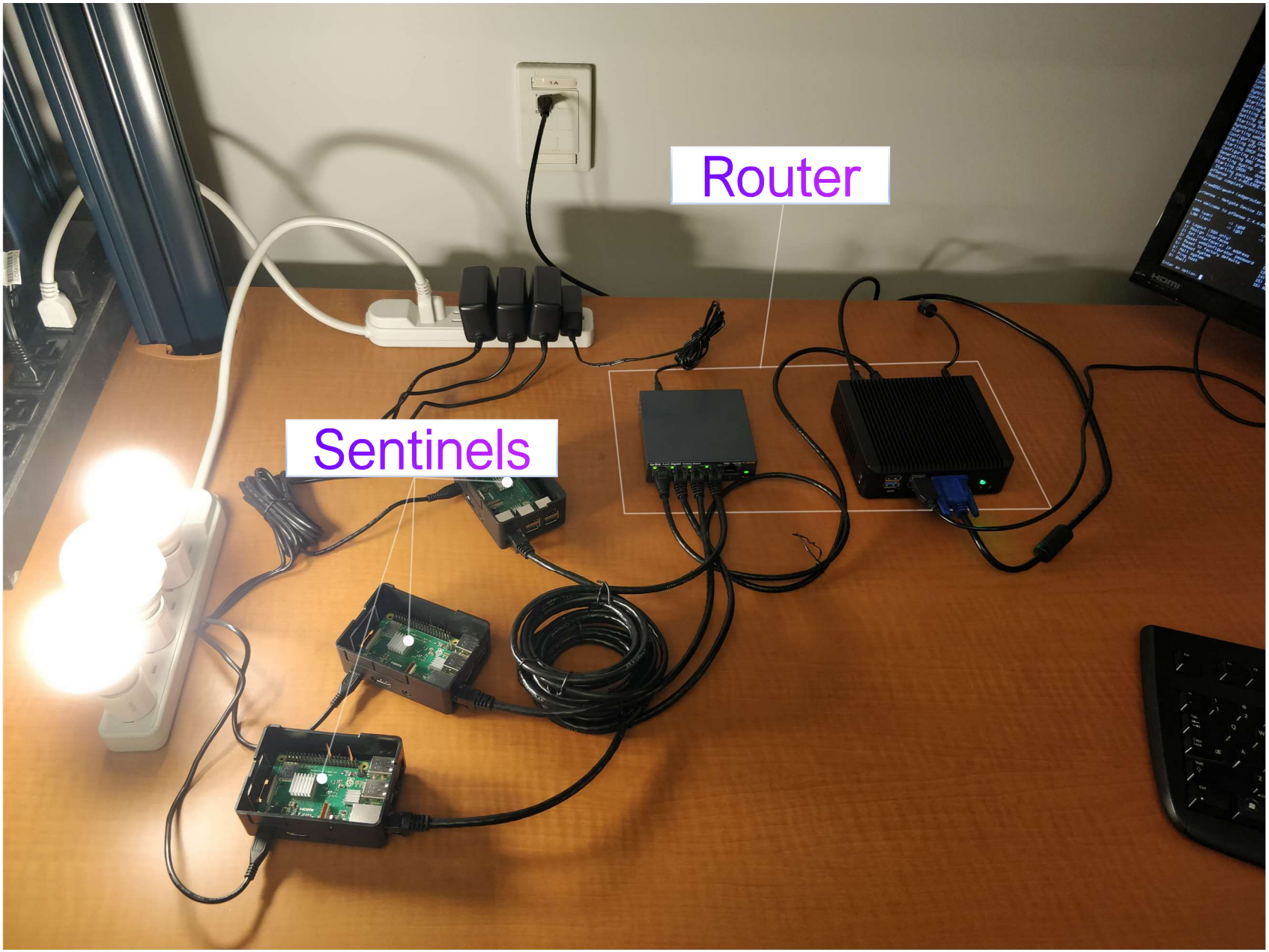
Blockchain


Sentinel 2
Sentinel 3
0x456
0x789
Device Chain
Longest Chain
Policy
0x123
0x987
Rejected fork
Sentinel 1
Signatures

Experiment

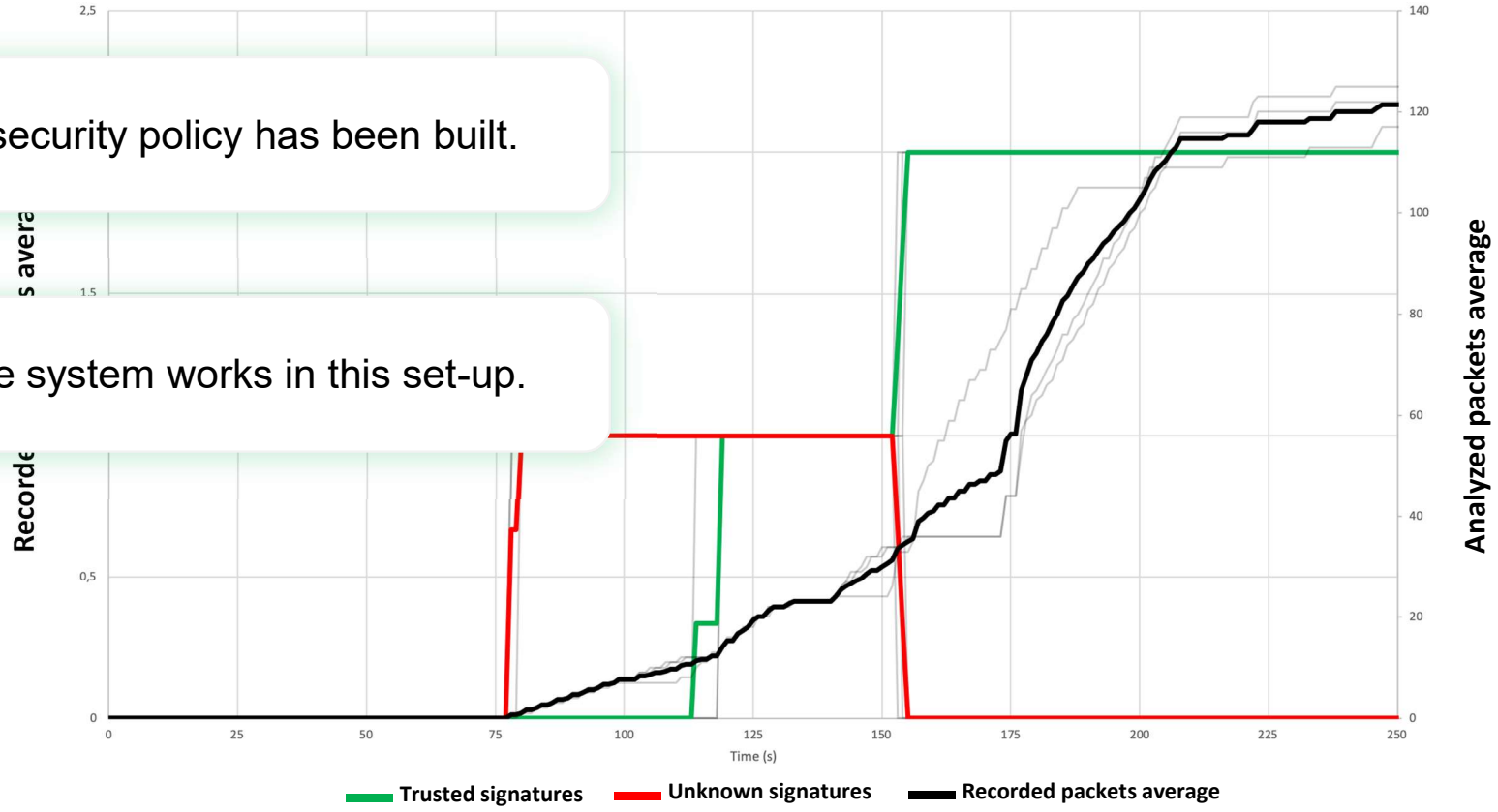
With real IoT devices




Router
Sentinels

Experiment
With IoTdevices

- ✓ A security policy has been built.
- ✓ The system works in this set-up.



Experiments

Simulations

Infra. Cloud

Simulated Sentinels and devices in the cloud.

1K Sentinels

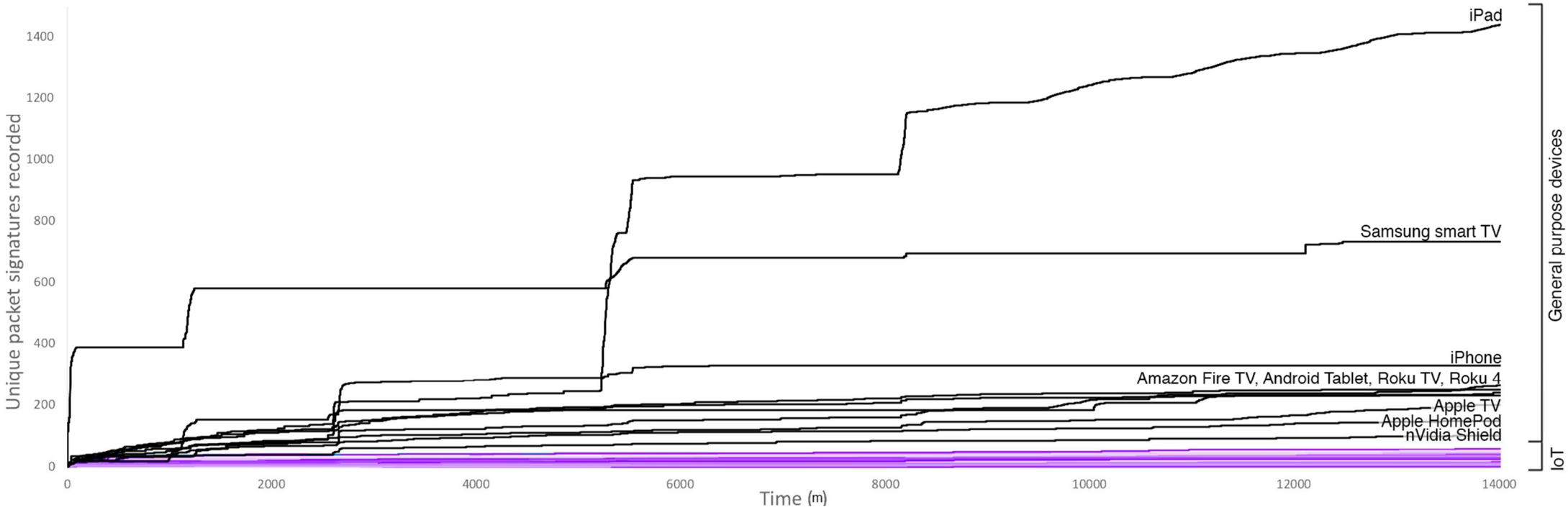
Simulations with up to 1000 Sentinels.

53 IoT

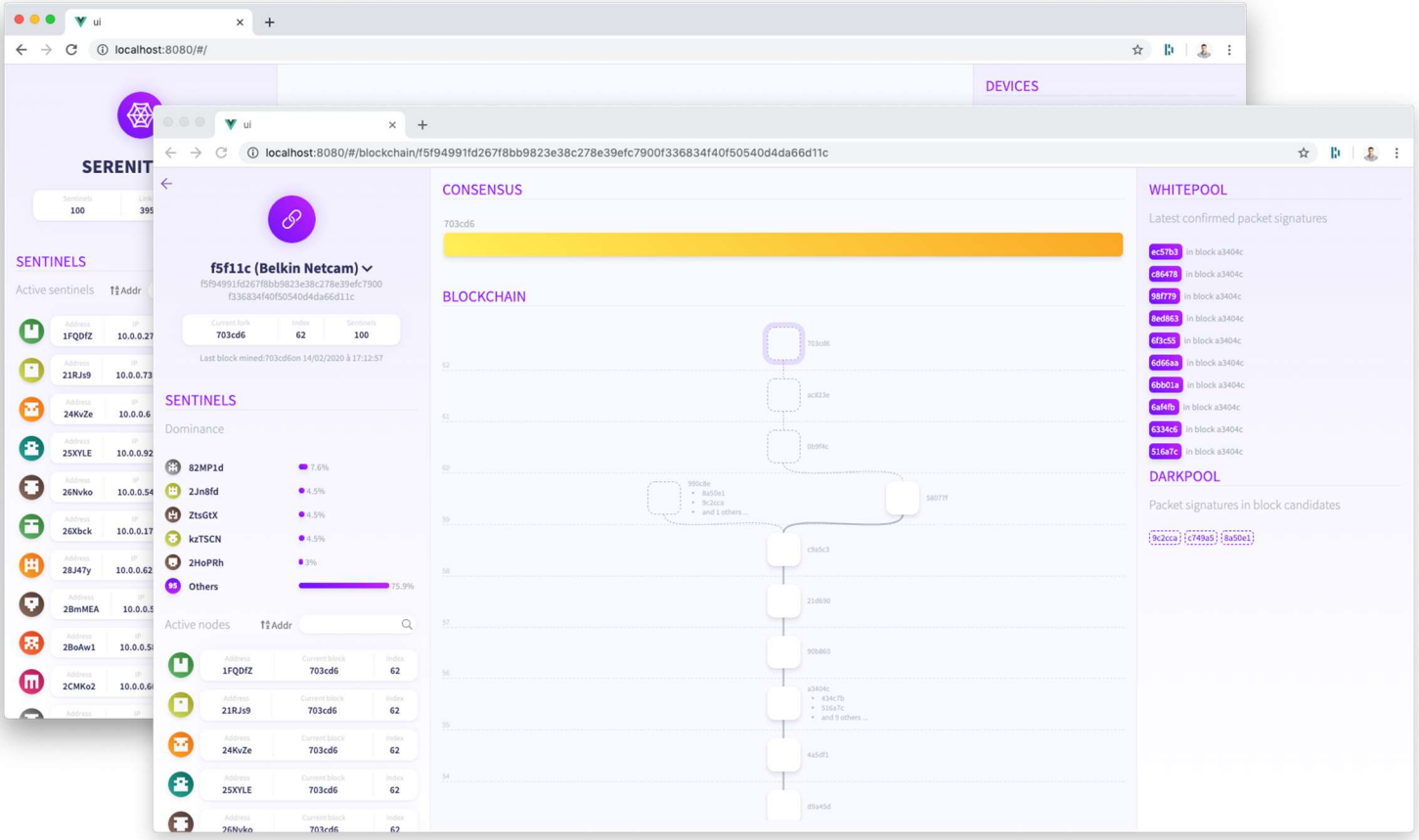
53 device types simulated from Alrawi et Al. dataset[1]

1: O. Alrawi et al., "SoK : Security evaluation of home-based IoT deployments," in IEEE 40th Symposium on Security and Privacy (S&P), 2019.

Dataset Analysis



Simulations
Demo



SERENITY NET

Sentinels	Links	Devices
20	74	60

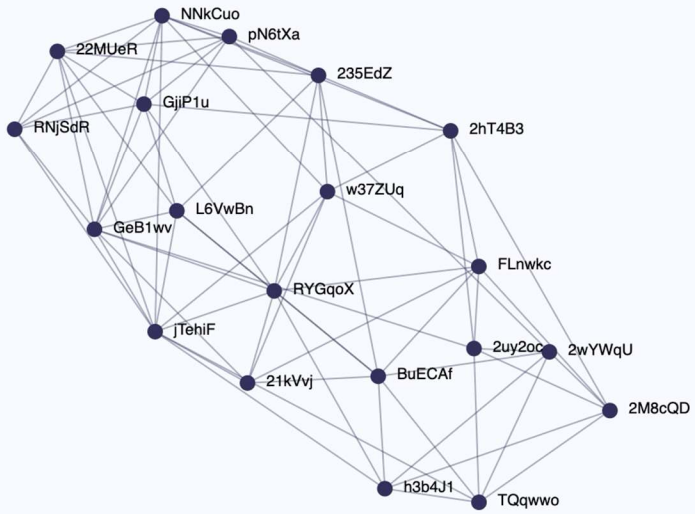
SENTINELS

Active sentinels

Addr

Address	IP	Neighbors	Devices
21kVvj	192.168.128.15	6	3
22MUeR	192.168.128.18	8	3
235EdZ	192.168.128.17	8	3
2M8cQD	192.168.128.11	6	3
2hT4B3	192.168.128.22	7	3
2uy2oc	192.168.128.7	6	3
2wYWqU	192.168.128.14	6	3
BuECAf	192.168.128.16	8	3
FLnwkc	192.168.128.9	7	3
GeB1wv	192.168.128.6	10	3

Sentinels: 20 Links: 74



- +

BLOCKCHAINS

Most popular devices

20	Belkin WeMo Motio... e60305	33.33%
20	LIFX Virtual Bulb 0f1249	33.33%
20	Belkin Netcam f5f11c	33.33%

Blockchains

Devices	Chain Id	Sentinels	Index
no device	c_chain	20	41
Belkin WeMo Motio...	e60305	20	26
LIFX Virtual Bulb	0f1249	20	32
Belkin Netcam	f5f11c	20	25

0f1249 (LIFX Virtual Bulb)

0f1d437ef2d86195fd6efa00f2a9b8d6d4b4f460a5a87c56b486d76ca1cb9249

Current fork	Index	Sentinels
ef9136	35	20

Last block mined:ef9136on 02/07/2020 à 12:11:22

SENTINELS

Dominance

w37ZUq	10%
pN6tXa	7.5%
22MUeR	7.5%
GjiP1u	7.5%
2hT4B3	7.5%
15 Others	60.0%

Active nodes

Addr

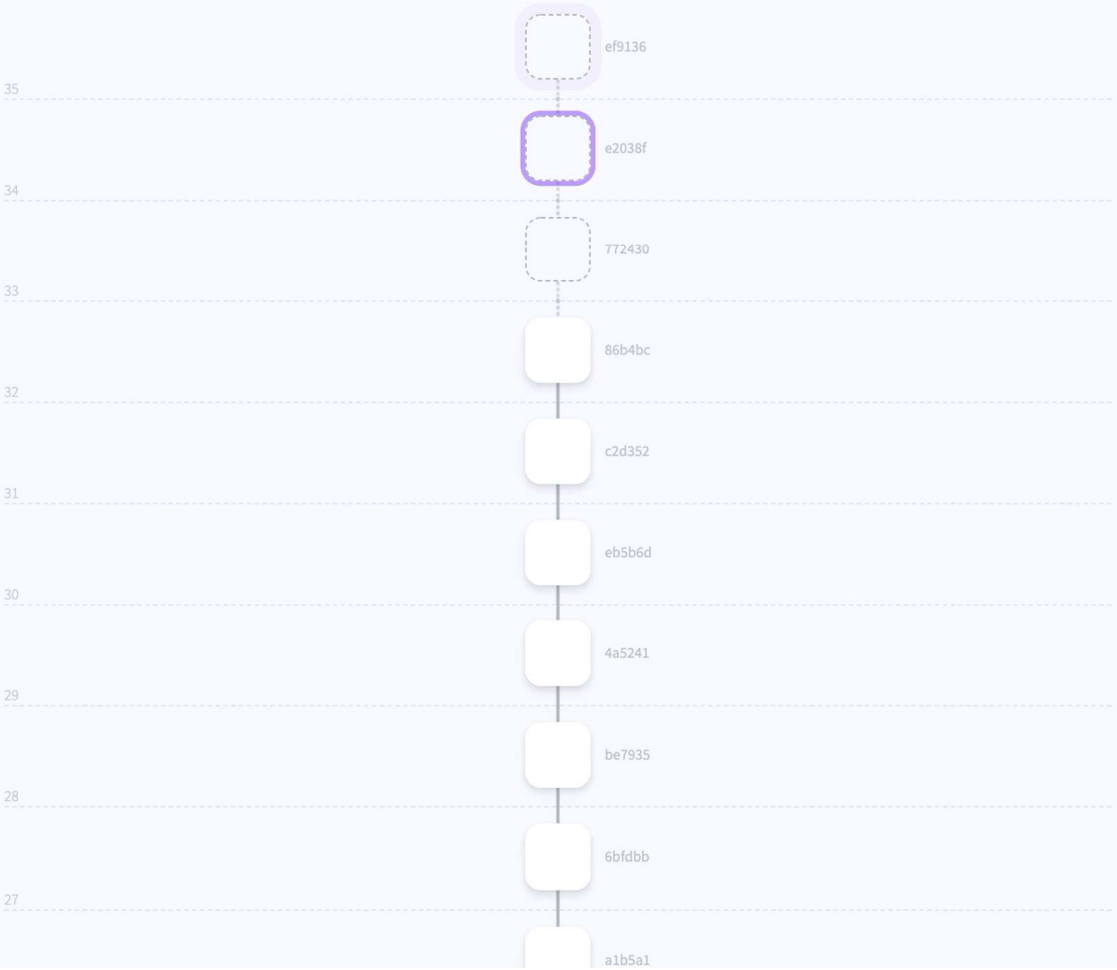
Address	Current block	Index
21kVvj	ef9136	35
22MUeR	ef9136	35
235EdZ	ef9136	35
2M8cQD	ef9136	35

CONSENSUS

Show network graph

ef9136 — e2038f

BLOCKCHAIN



WHITEPOOL

Latest confirmed packet signatures

- 4e2474 in block 686824
- 0cc4d4 in block 686824
- 4e2474 in block a6beb3
- 0cc4d4 in block a6beb3
- 4e2474 in block 3a019a
- 0cc4d4 in block 3a019a

DARKPOOL

No fingerprint in block candidates

0f1249 (LIFX Virtual Bulb)

0f1d437ef2d86195fd6efa00f2a9b8d6d4b4f460a5a87c56b486d76ca1cb9249

Current fork	Index	Sentinels
2303fc	39	20

Last block mined:2303fcon 02/07/2020 à 12:12:46

SENTINELS

Dominance

GjiP1u	9.1%
w37ZUq	9.1%
pN6tXa	6.8%
22MUeR	6.8%
235EdZ	6.8%
15 Others	61.4%

Active nodes

Addr

Address	Current block	Index
21kVvj	2303fc	39
22MUeR	a88adb	38
235EdZ	a88adb	38
2M8cQD	a88adb	38

CONSENSUS

Show network graph

a88adb 2303fc

BLOCKCHAIN

39 2303fc
- 8a50e1
- 9c2cca
- and 1 others ...

38 a88adb

37 c221e5

36 e37458

35 ef9136

34 e2038f

33 772430

32 86b4bc

31 c2d352

eb5b6d

WHITEPOOL

Latest confirmed packet signatures

4e2474 in block 686824
0cc4d4 in block 686824
4e2474 in block a6beb3
0cc4d4 in block a6beb3
4e2474 in block 3a019a
0cc4d4 in block 3a019a

DARKPOOL

No fingerprint in block candidates

Experiments
Simulations

- ✓ Sentinels were able to converge and build security policies for the devices with a small network footprint.
- ✓ Sentinels were able to identify and block anomalous packets.

SERENIoT

Filter

Anomalous packets.

Zero Conf

Security policies are always up to date thanks to the blockchain.

Independent

From IoT manufaturers and security vendors. Fully decentralized.

Compatible

With current and future TCP/IP devices with a small network footprint.

Limitations

LAN to WAN

Current version only monitors LAN to WAN

Small network footprint

Works best for devices with a small and constant network footprint.

No user defined connections

User defined connections are blocked. Early adopters may observe a delay before being able to use new functionalities.

Performance linked to adoption

Greater chance of abuse when adoption remains small.

THANK YOU!

ANY QUESTION?

corentinthomasset.me/serenity

Contact: corentin.thomasset@polymtl.ca