MARCH 2021

THE STATE OF IoT SECURITY IN 2020

Bitdefender®

WWW.BITDEFENDER.COM/IOT

COMMUNICATION SERVICE PROVIDERS

THE UNSUNG HEROES OF THE EPIDEMIC

As millions of people started working and studying from home during the pandemic, communication service providers and networking equipment vendors have been struggling to accommodate them all. Broadband and mobile internet connections have become lifelines in doing business, in staying in touch with families, and in education.

The 40% spike in residential traffic in 2020 has placed considerable strain on a business model designed to only accommodate peaks. Increased bandwidth consumption, malicious traffic and a spate of cyber-attacks left communication service providers scrambling to serve everyone. In this new reality, it has become crucial for Internet Service Providers and telecoms to filter unwanted or malicious traffic to improve customer security and to offer reliable bandwidth to homes.

Our mission is to help them integrate and automate security at any level – from core infrastructure down to low-performance, less expensive residential gateways, where heavy local processing would impact end-user QoS due to hardware constraints.

Ciprian Istrate
VP of Consumer Solutions @ Bitdefender

01

TRAFFIC DEMAND

Monthly residential bandwidth consumption peaked at an average of 1.2 terabytes per household

02

VULNERABILITIES

NAS drives, smart TV sets, media players, routers and IP cameras are the world's most vulnerable devices

03

IMPACT

Almost 75% of identified vulnerabilities in smarthomes have a medium or high impact.

04

CONNECTIVITY

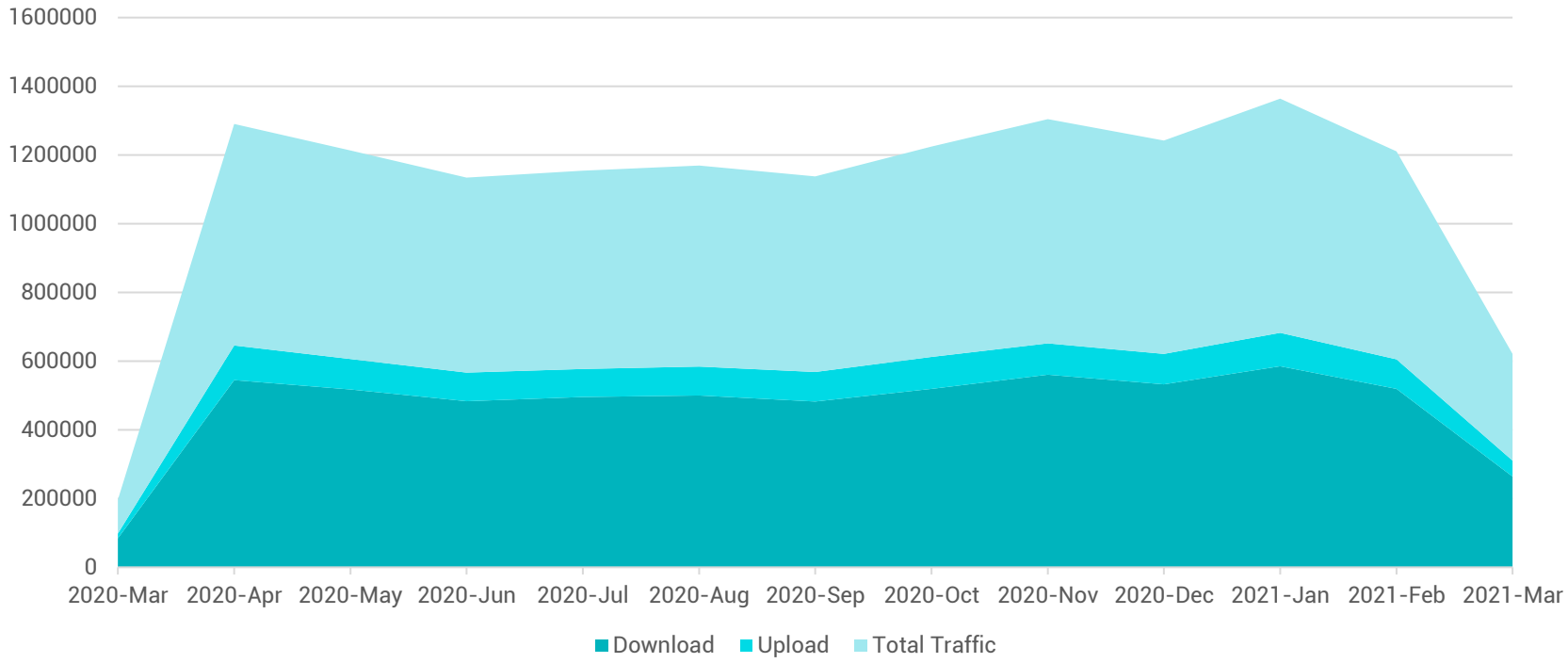
The average smart home has 25 devices connected to the Internet

MONTHLY BANDWIDTH USAGE DURING THE PANDEMIC (MB/HOUSEHOLD)

Since March 2020, when most of the world started working and studying from home, residential bandwidth consumption has grown to all-time heights.

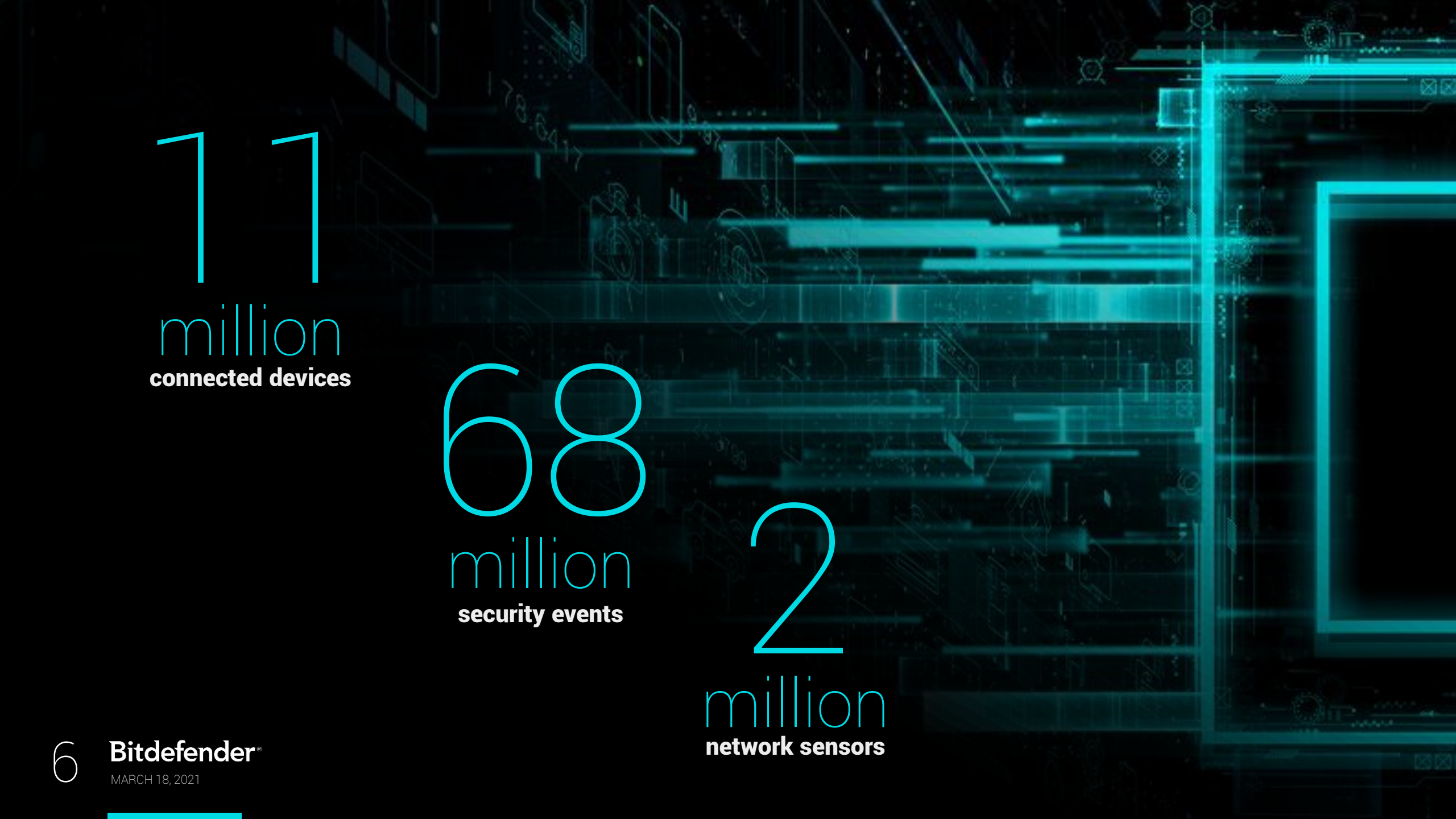
Zooming, surfing the web and streaming media to keep family busy was just part of what ISPs had to keep up with.

New botnets, such as Mozi, generated 90% of the total IoT traffic last year.



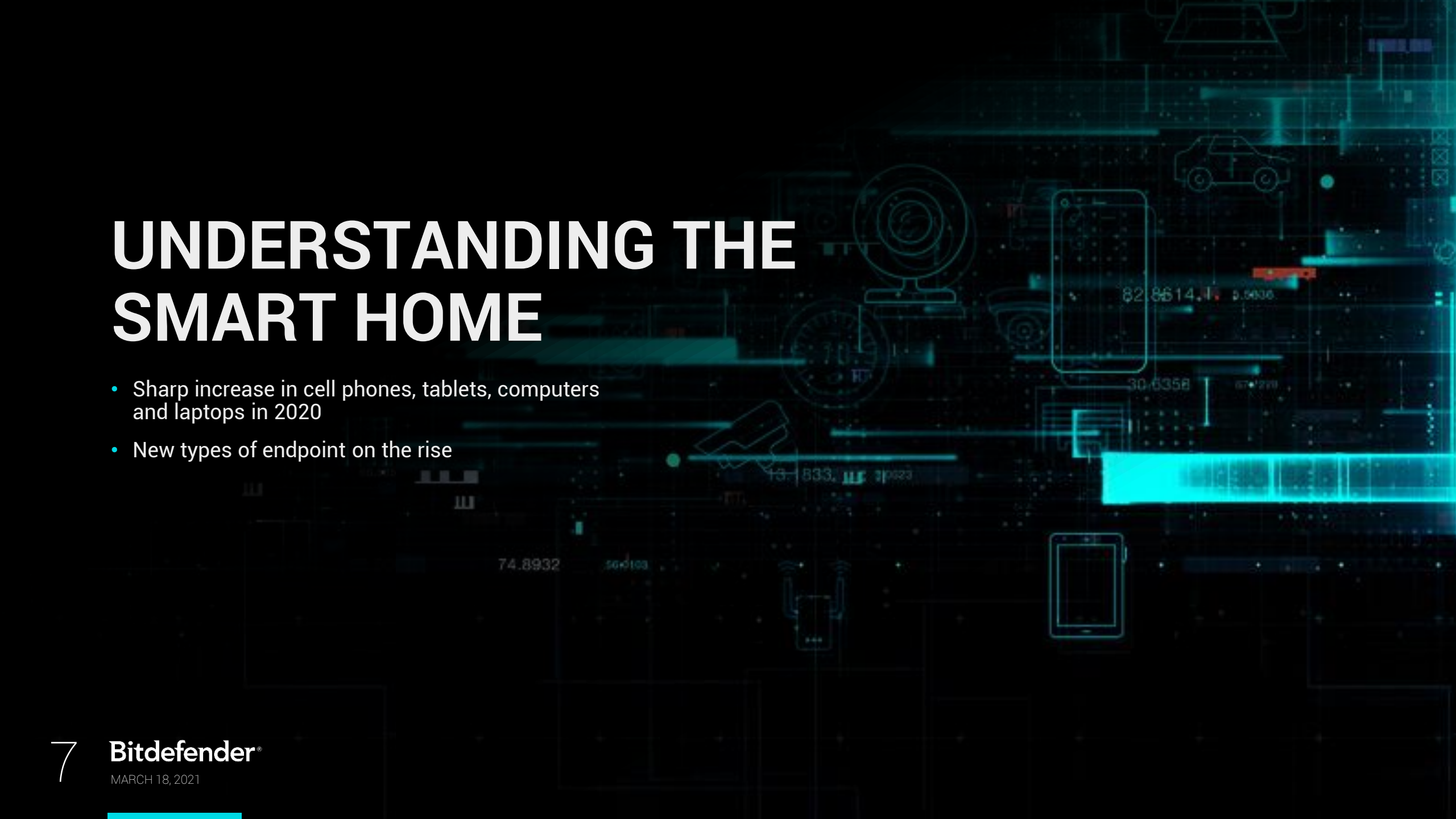
A LOOK AT THE THREAT LANDSCAPE

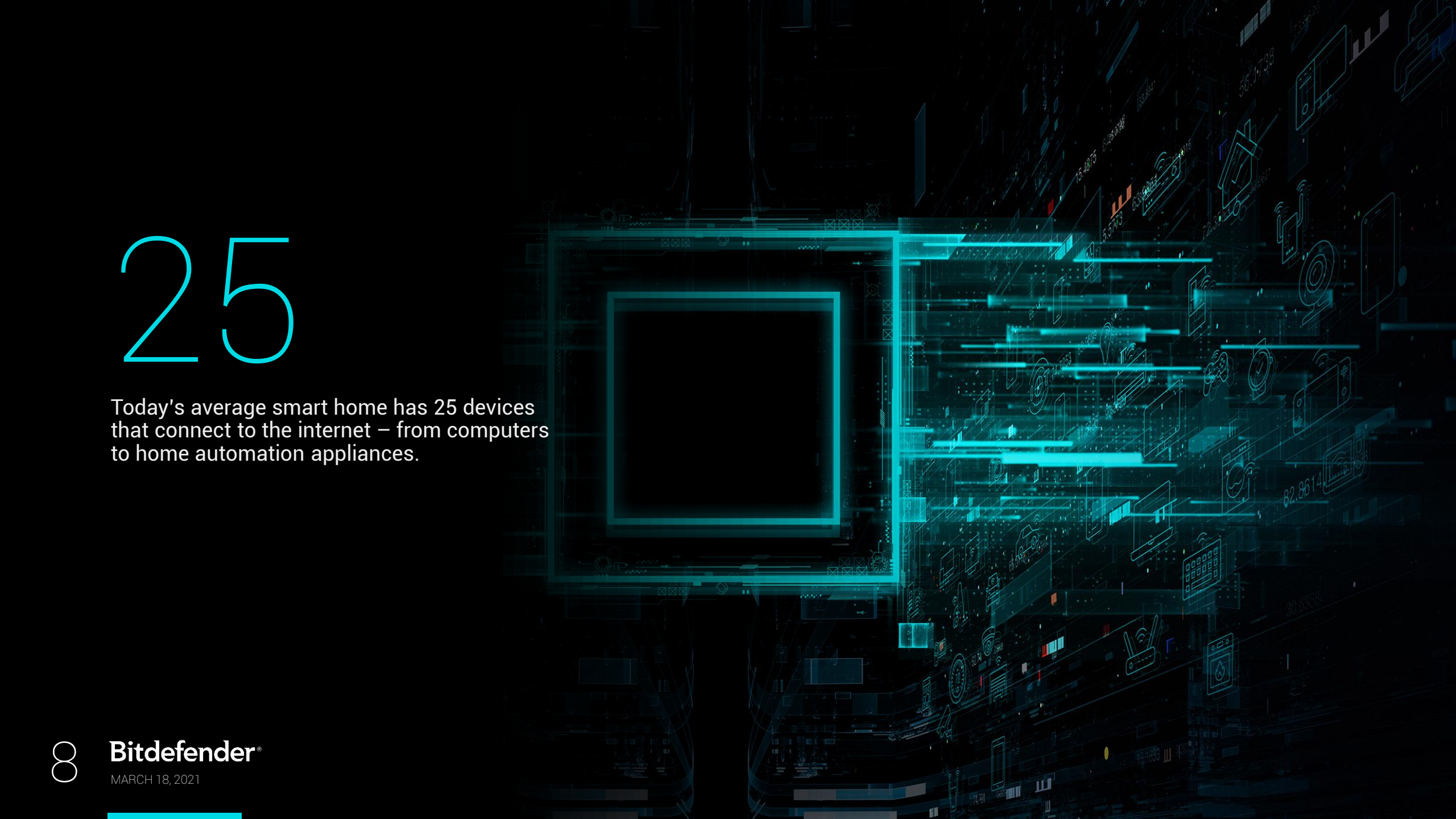
We investigated more than 11 million IoT devices and 68 million security events around the world to uncover vulnerabilities and attack scenarios and make the smart home a safer environment for everybody.


11
million
connected devices
68
million
security events
2
million
network sensors

UNDERSTANDING THE SMART HOME

- Sharp increase in cell phones, tablets, computers and laptops in 2020
- New types of endpoint on the rise





25

Today's average smart home has 25 devices that connect to the internet – from computers to home automation appliances.

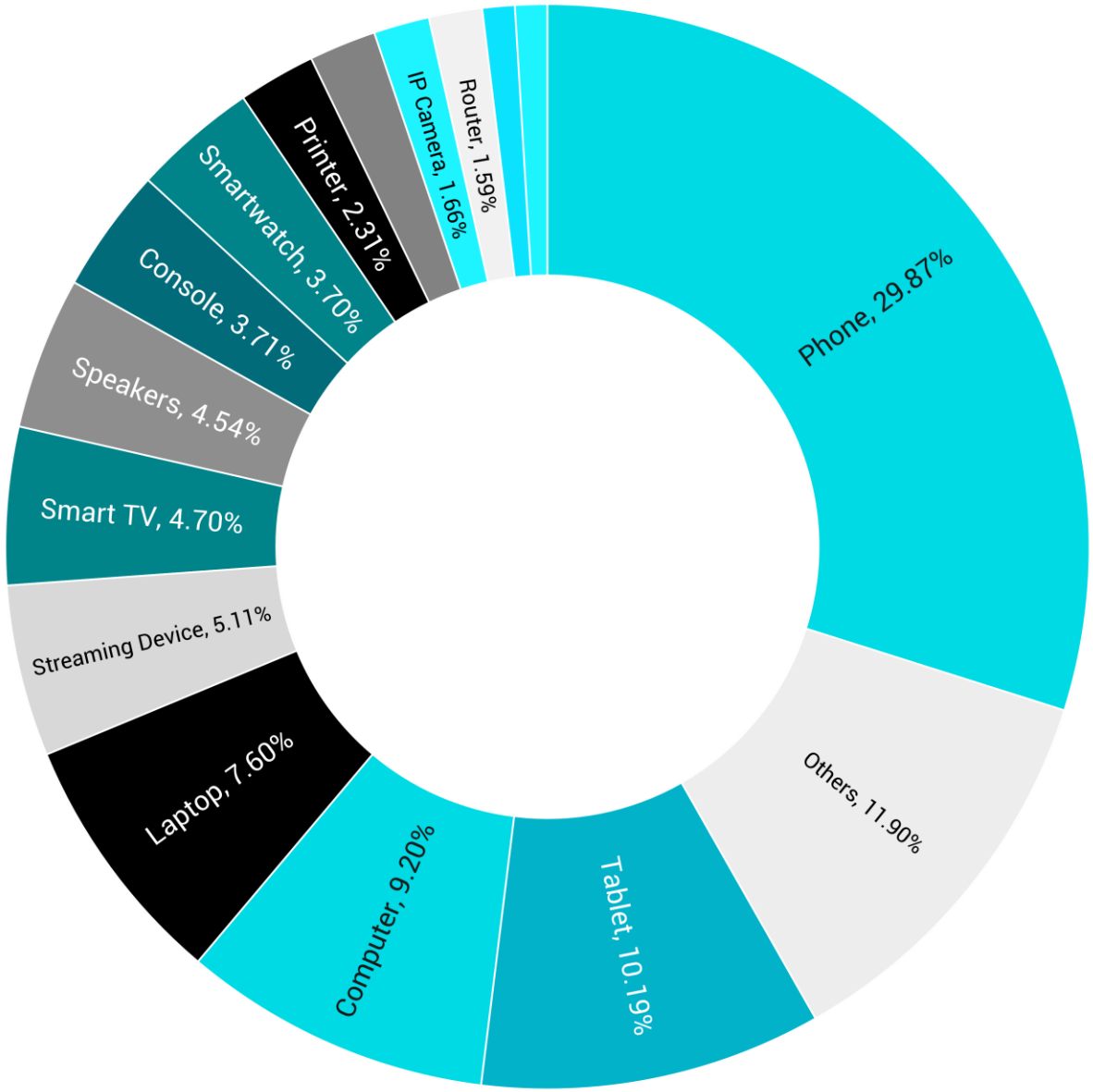
Bitdefender®

MARCH 18, 2021

MOST POPULAR DEVICES IN THE CONNECTED HOME

Cell phones, tablets, computers, and laptops grew in popularity throughout 2020 as online education forced parents and schools around the world to provide equipment for students at home.

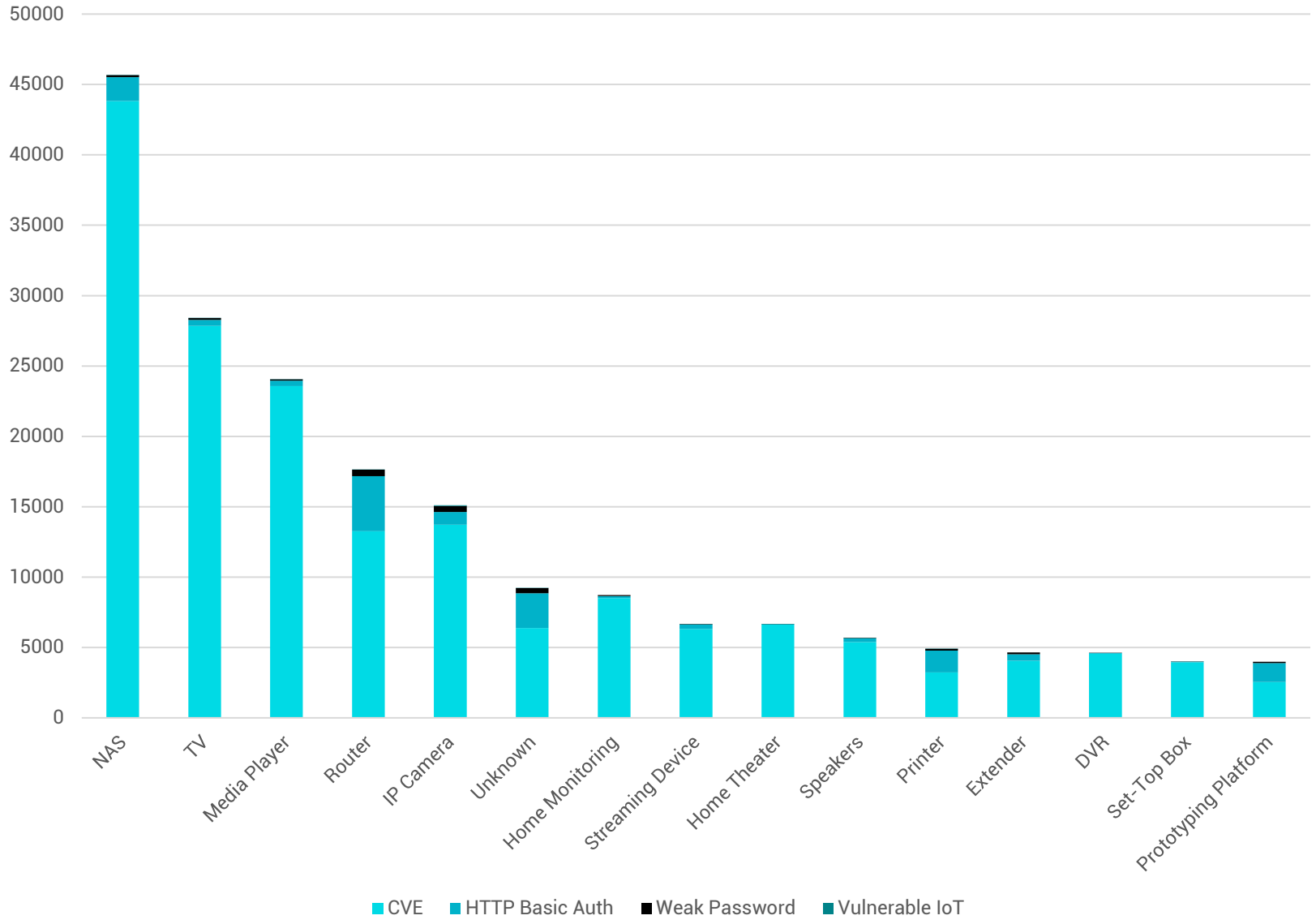
At the opposite end, connected beer-brewing gear, smart bikes, and weather sensors are the world's least popular internet-connected devices.



TOP VULNERABLE DEVICES

Telemetry received by Bitdefender from more than 2 million network sensors pinpoints the most vulnerable types of devices in homes.

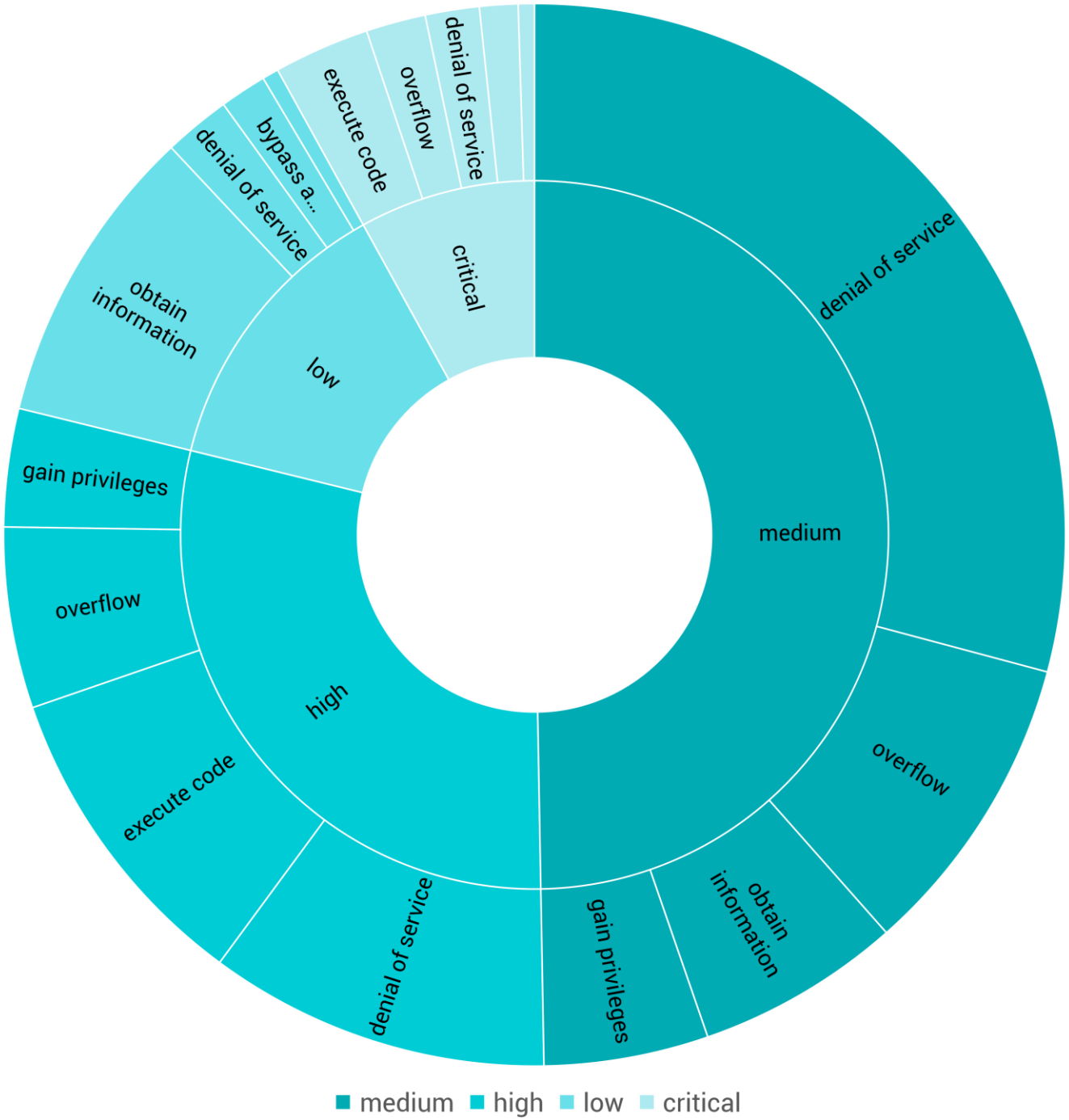
NAS drives, smart TV sets, media players, routers and IP cameras lead the pack in terms of security issues.



VULNERABILITIES AND RISKS

Most IoT devices run proprietary operating systems that rarely receive security updates, if ever.

Many such operating systems have known security vulnerabilities that remote attackers leverage to compromise the device and pivot on the network. These vulnerabilities can be used for code execution, to obtain information, or to completely take the device offline.



75% OF IDENTIFIED VULNERABILITIES HAVE MEDIUM AND HIGH IMPACT

Bitdefender IoT Landscape Report, 2021

Effective security management of IoT devices requires more than keeping lists of devices and their associated IP addresses on the network.

Network-based cybersecurity solutions can identify these devices, assess their risk level, and monitor for anomalies in incoming or outoing communication.

PREDICTIONS FOR 2021 AND BEYOND

1

Data breaches will start at home.
Home routers and computers will continue to get hacked.

Threat actors specialized in hijacking devices will either rent out access to other groups seeking distributed command and control capabilities or sell it in bulk to underground operators to reuse as proxy nodes to conceal malicious activity.

2

Urgent need for change.

Devastating corporate data breaches will start at home. Data breaches are the new normal, and companies expend a great deal of effort trying to put safeguards in place.

As more people adhere to the work-from-home schedule imposed by the Coronavirus pandemic, employees will take cybersecurity shortcuts for convenience. Poorly secured personal devices and home routers, and the transfer of sensitive information over unsecured or unsanctioned channels (such as instant messaging apps, personal e-mail addresses and cloud-based document processors) will play a key role in data breaches and leaks.

3

Connectivity chaos.

With global data usage rising sharply, Internet Service Providers have very little room to accommodate malicious traffic. Distributed-denial-of-service attacks and botnet traffic will force communications providers to integrate security at the core of the offering.

As threats grow in complexity, web filtering technologies are no longer enough. Fully-fledged security agents for laptops, desktops, and mobile devices add an important extra security layer and complement the security solution running at the gateway.

HOW TO STAY SAFE

- Stay aware of your IoT devices
- Move all smart "things" to your guest network
- Patch devices as soon as a new firmware version becomes available
- Ask your ISP about routers or gateways with built-in security
- Probe your network for vulnerable devices with a smart home scanner
- Do not expose LAN devices to the Internet unless necessary

Awarded IoT Security Platform for ISPs and Router Manufacturers

18 Bitdefender®
MARCH 18, 2021

BITDEFENDER IS A GLOBAL CYBERSECURITY LEADER DELIVERING BEST-IN-CLASS THREAT PREVENTION, DETECTION AND RESPONSE SOLUTIONS WORLDWIDE

FOUNDED IN 2001

1800+

EMPLOYEES

MANAGED DETECTION

24/7

SECURITY OPERATIONS CENTER

EUROPE & US HEADQUARTERS

17

REGIONAL OFFICES

GLOBAL ALLINACES

150+

TECHNOLOGY PARTNERS


Bitdefender®
WWW.BITDEFENDER.COM/IOT