SCTE
a subsidiary of CableLabs®

Creating Infinite Possibilities.

Security and Privacy: IoT Vulnerabilities

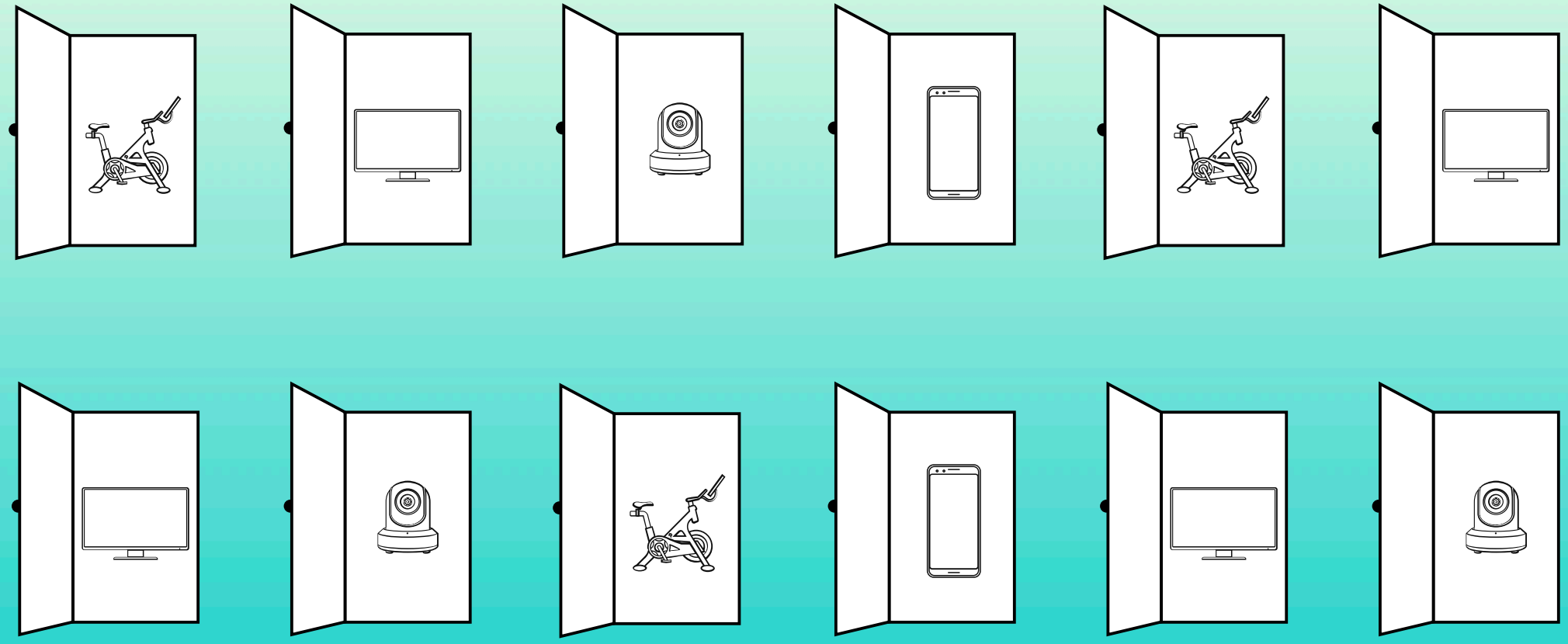
Too Many Entry Points

Mangesh Bhamre, Senior Manager of Product (Cybersecurity), Plume Design, Inc.

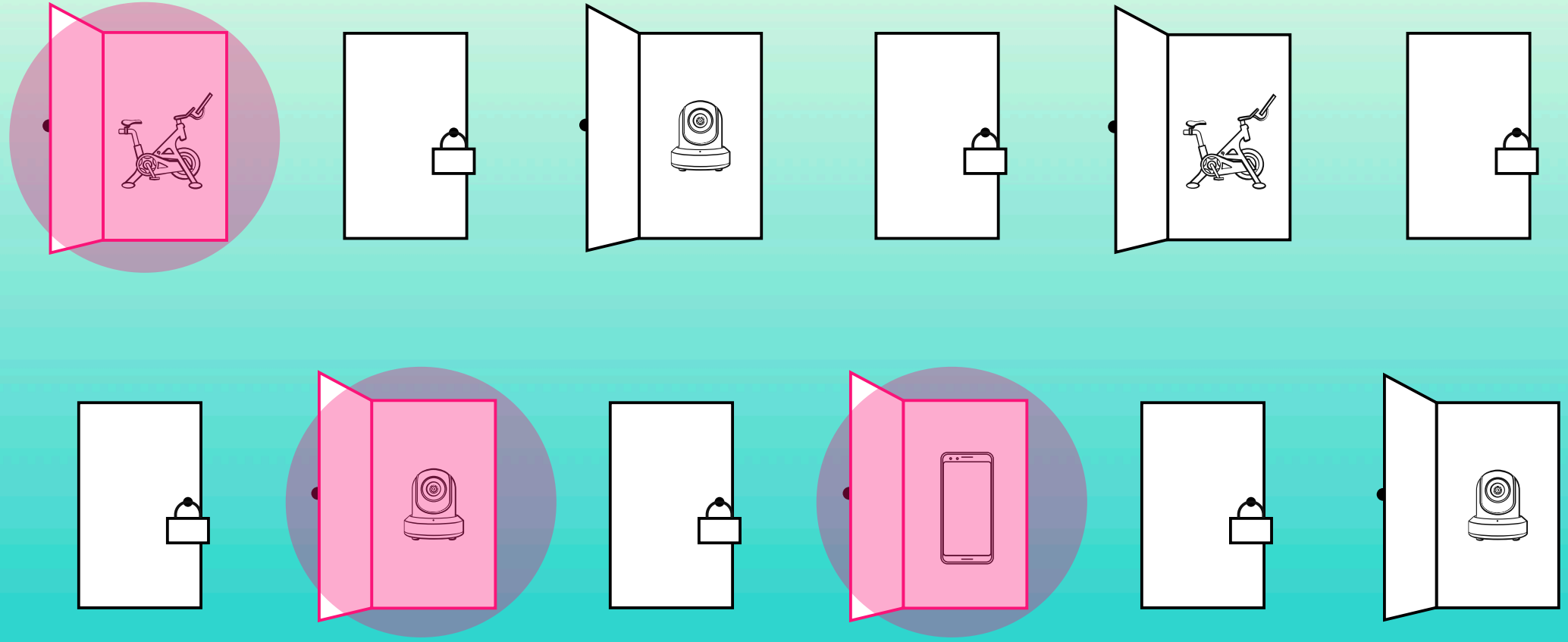
SCTE CABLE-TEC EXPO 22
SEPTEMBER 19-22 • PHILADELPHIA, PA

2022 Fall Technical Forum
SCTE • CABLELABS • NCTA

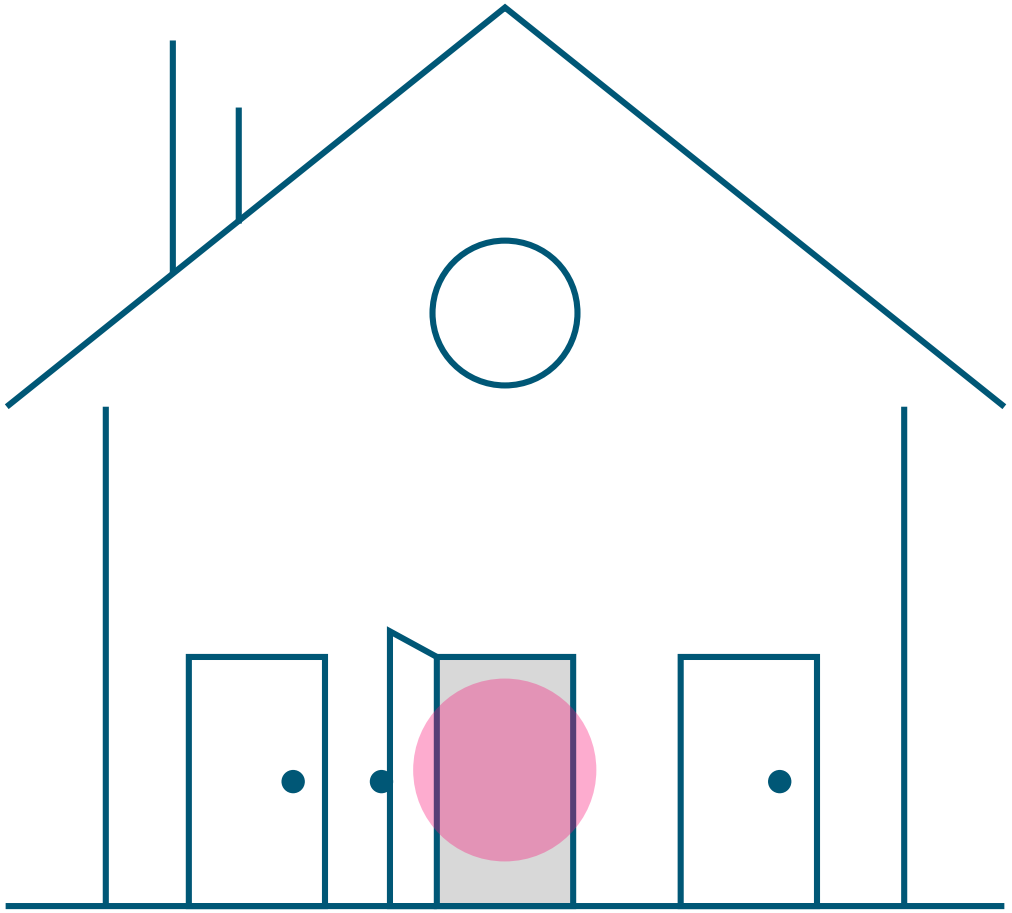
Too many doors



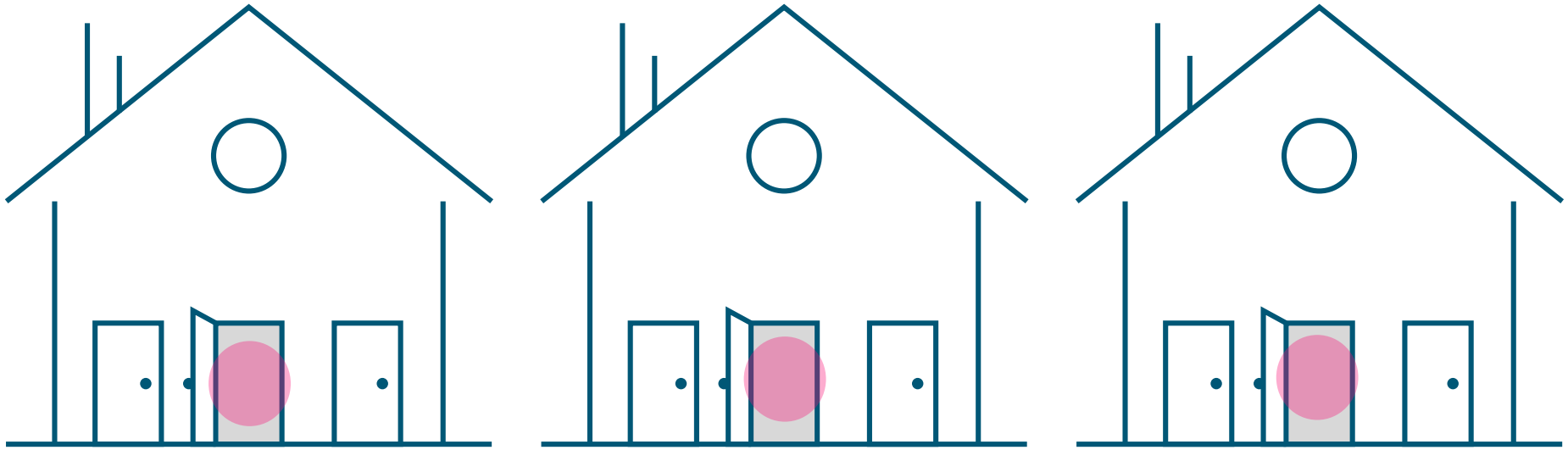
Too many doors



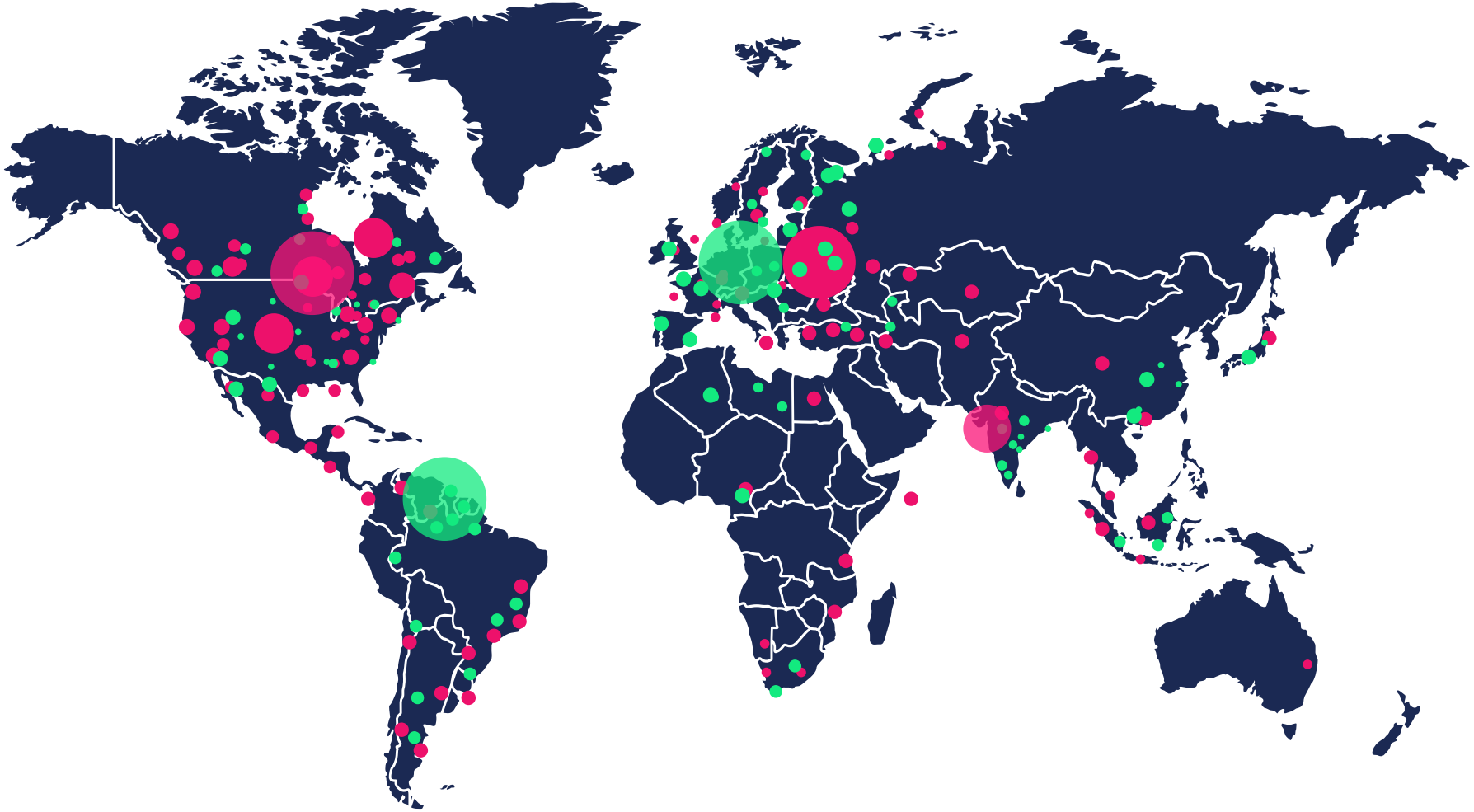
Too many doors



Too many doors



Too many doors



Consumers' Top Smart Home Security Concerns

Hacking

75%

Government spying on in-home smart cameras

53%

Smart speakers

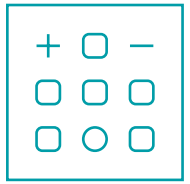
52%

*Source: ADT Survey: Consumers want cyber protection for smart homes

© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

Challenges

Identity and Authentication



Compute Power

IoT Device Heterogeneity

User Awareness

Work-from-home Trends

© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

User Awareness

At least
49%

of consumers don't know how to protect their personal data.

47%

were concerned about the possibility of their data being hacked.

64%

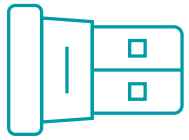
said that companies aren't doing much to help.

*Source: Corporate Data Responsibility: Bridging the Trust chasm, KPMG 2021

© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

Work-From-Home Security Concerns

30% of WFH participants don't use a company VPN to access the company network



40% of WFH participants use a company dongle to connect; the others rely on home WiFi or hotspots on mobile phones for internet access

The average Plume household has **21 devices** connected to the home WiFi network, each one with its own potential vulnerabilities

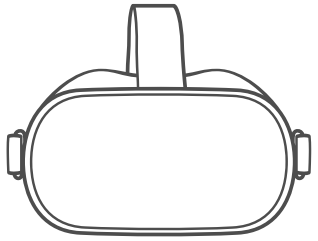
© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

Attack Motivations

- There is a new breed of proficient and well financed attackers
- Key motivations
  - Financial
- War/Defense
- Social/Political
- Motivation defines the attack type and scope

© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

Growth In IoT Devices At Home

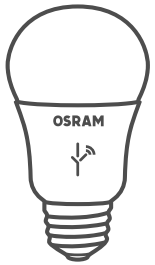


223% ↑

Virtual reality devices

132% ↑

Fitness bikes and trainers

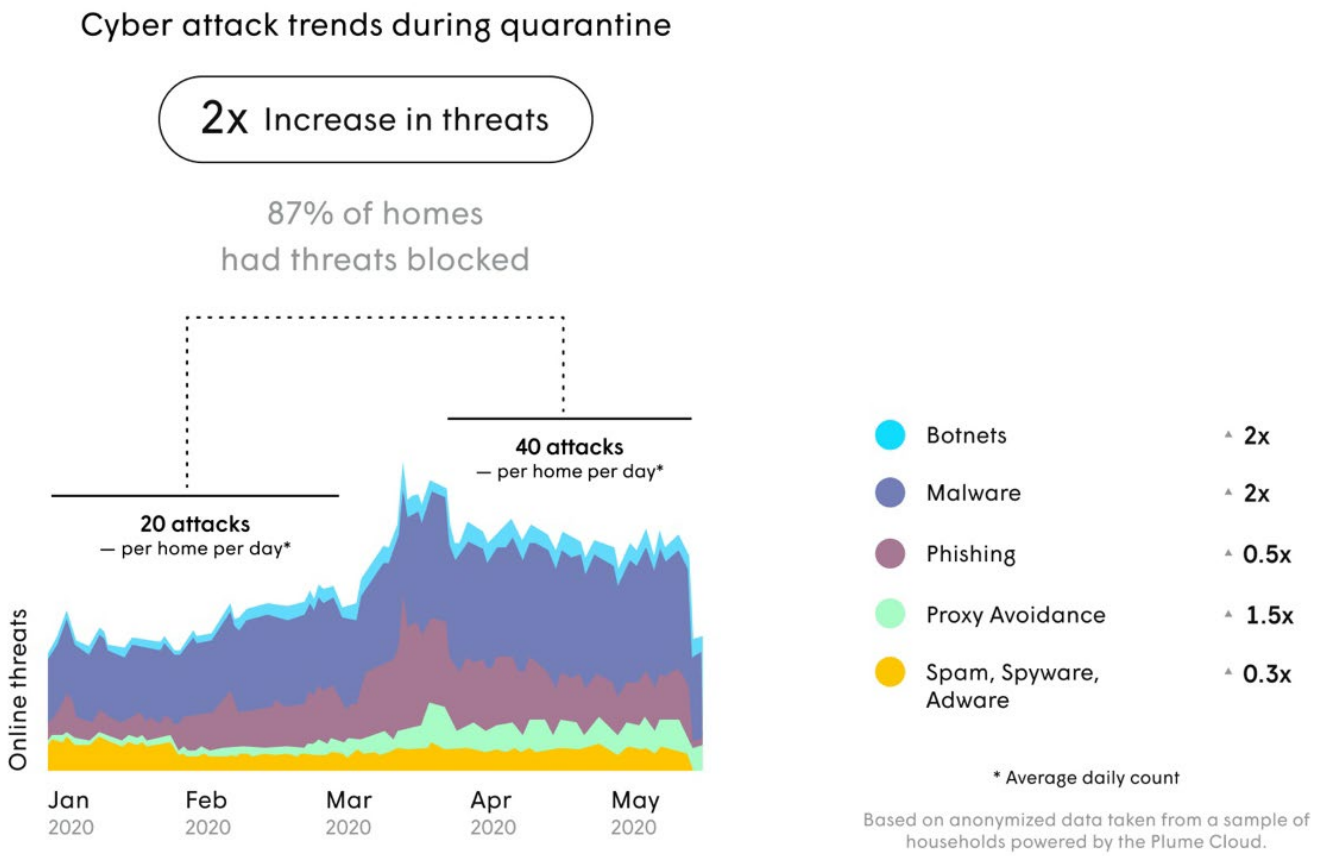


110% ↑

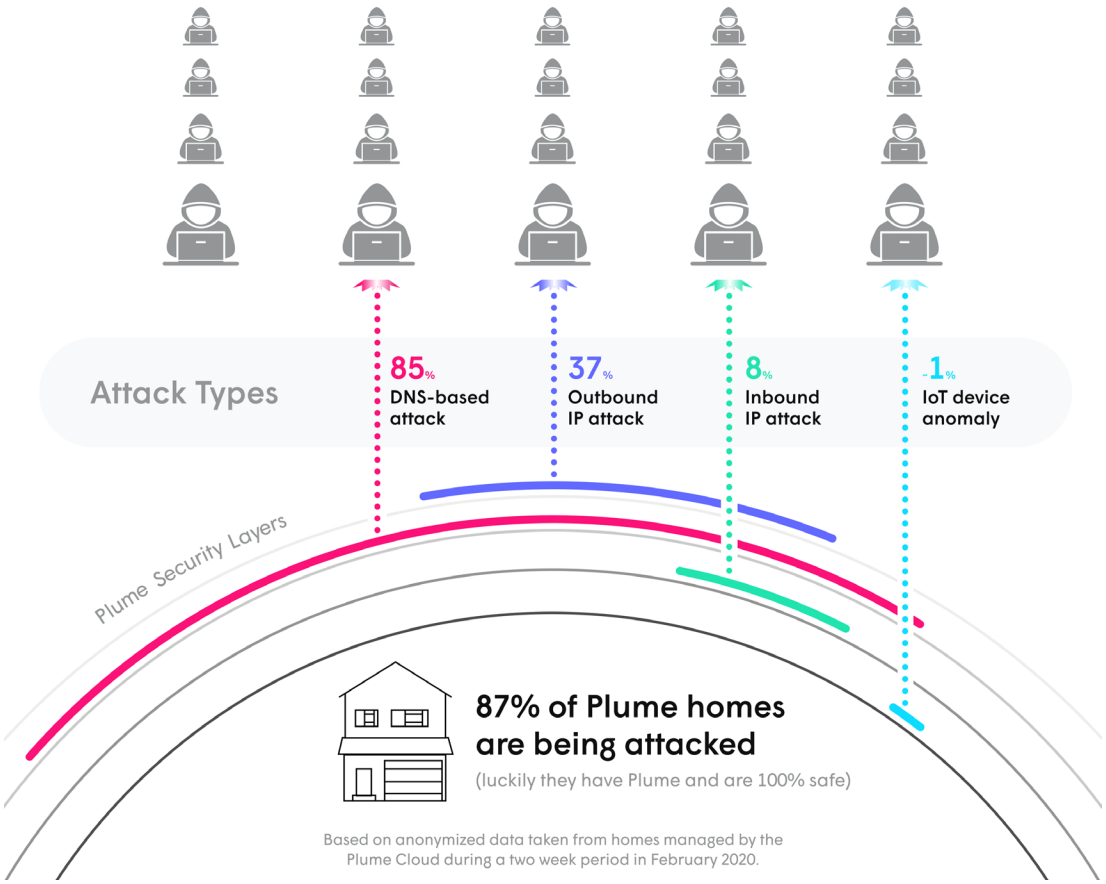
Smart light bulbs

© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

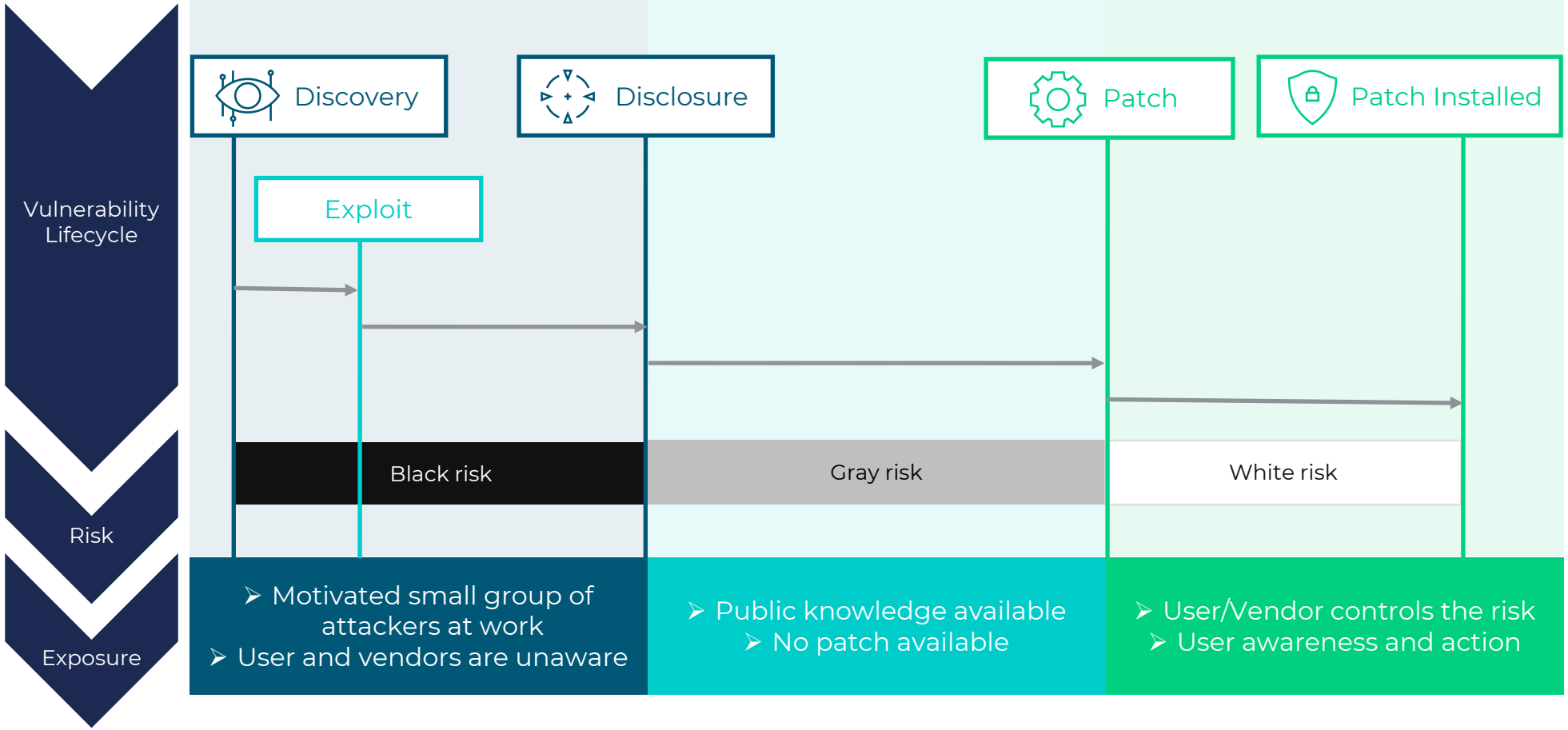
Cyberattack Trends Before and After COVID-19



Types Of Cyberattacks



Risk Exposure Phases



© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

Open Ports

- Common services like HTTP, HTTPS, SSH, RDP, FTP and SMTP constitutes 87.4% of the open ports on the IoT devices
- OpenSSH exists or 88.87% devices, it is associated with 98 vulnerabilities and exposes port 22

Top 10 Open IoT Ports

TCP Port	Service	Ports Open	% of Overall Exposed
443	HTTPS	772,258	35.6%
80	HTTP	670,789	30.9%
22	SSH	184,848	8.5%
3389	RDP	40,893	1.9%
8443	HTTPS-Alt	391,000	1.8%
8080	HTTP_Alt	30,502	1.4%
21	FTP	30,059	1.4%
8081	HTTP_Alt	27,187	1.3%
25	SMTP	23,901	1.1%
8000	Applications	21,028	1.0%

© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

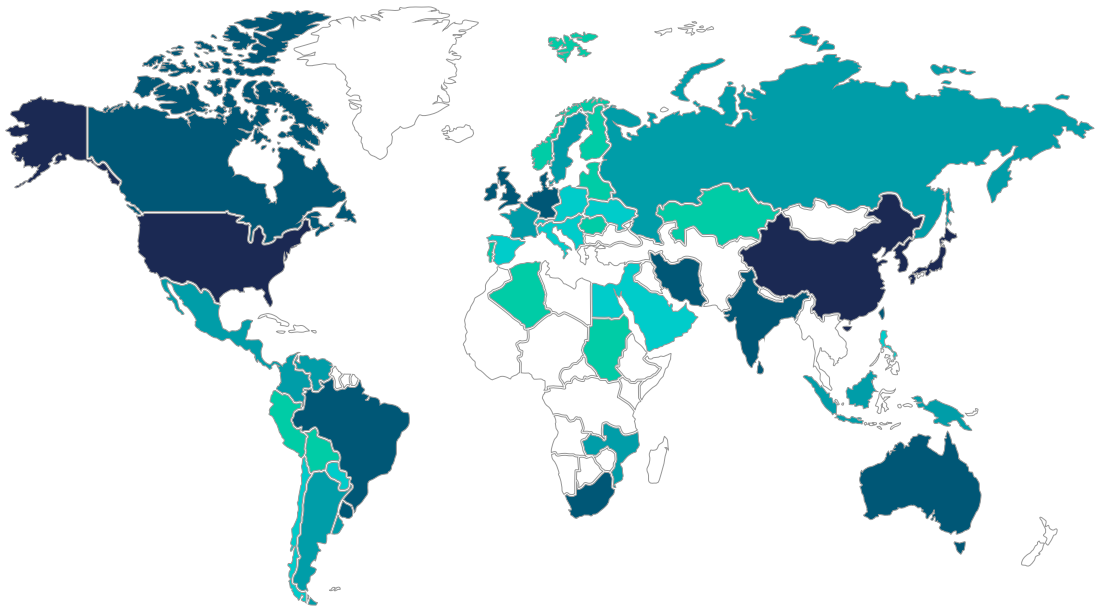
Vulnerabilities And Open doors

- UPnP service is another critical attack vector
- Problem is enormous
- Shodan stats reveal 6M+ open UPnP ports worldwide.

Total Results

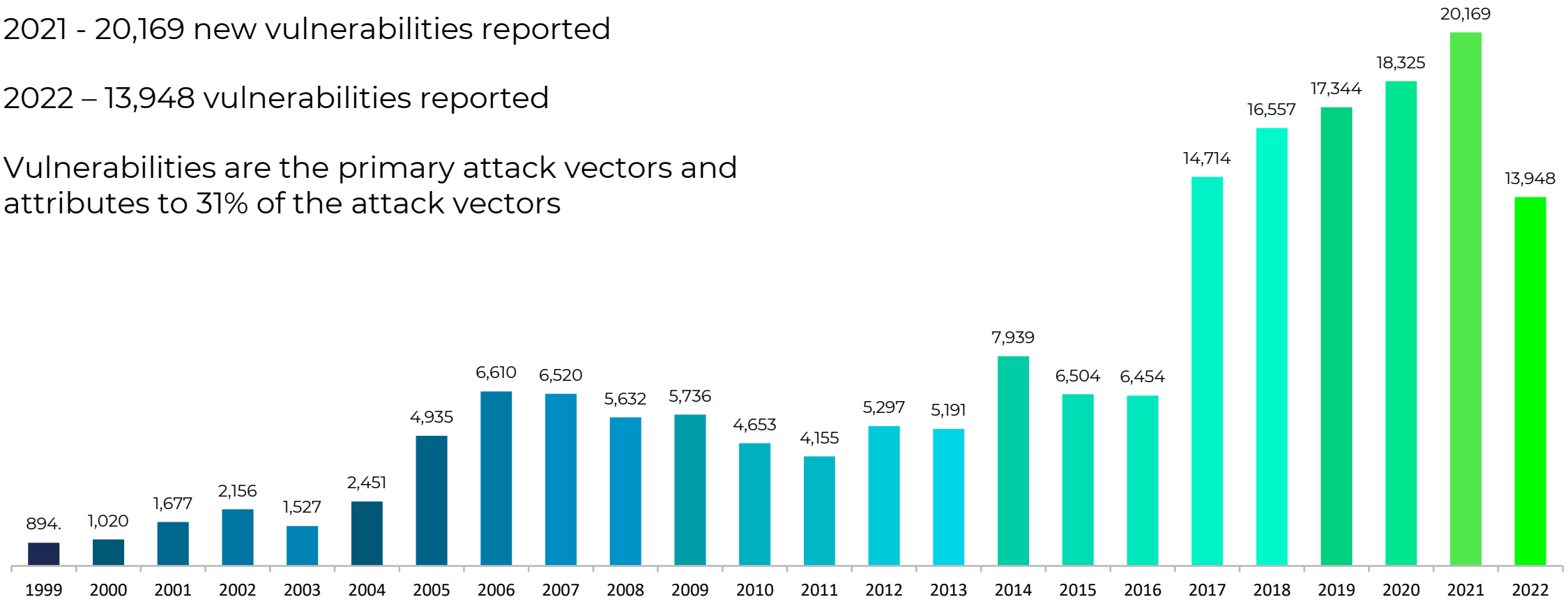
6,201,899

Top Countries



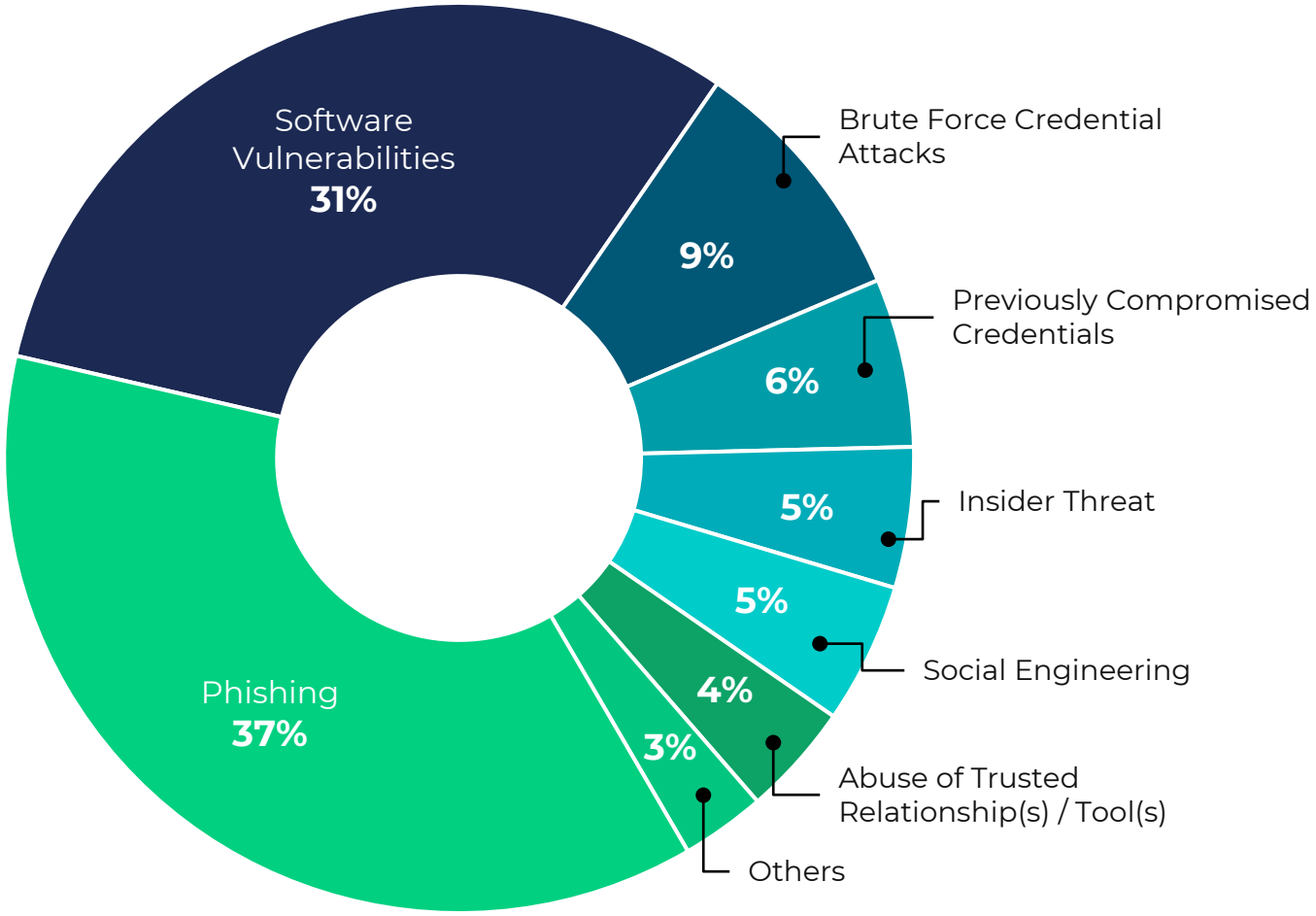
Vulnerabilities By Year

- 2021 - 20,169 new vulnerabilities reported
- 2022 – 13,948 vulnerabilities reported
- Vulnerabilities are the primary attack vectors and attributes to 31% of the attack vectors



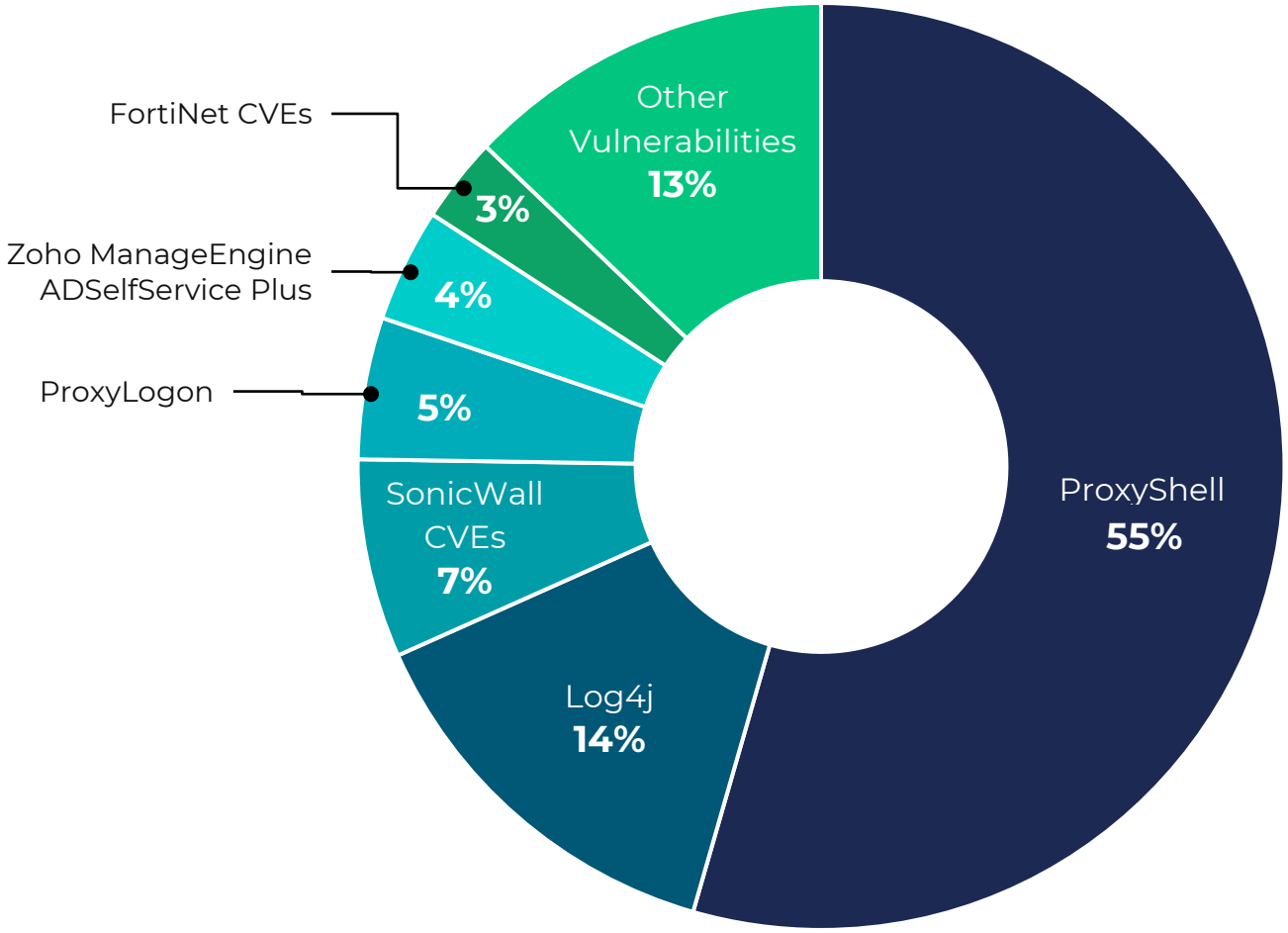
© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

Common Attack Vectors



© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

Most Exploited Vulnerabilities



Vulnerability Prioritization

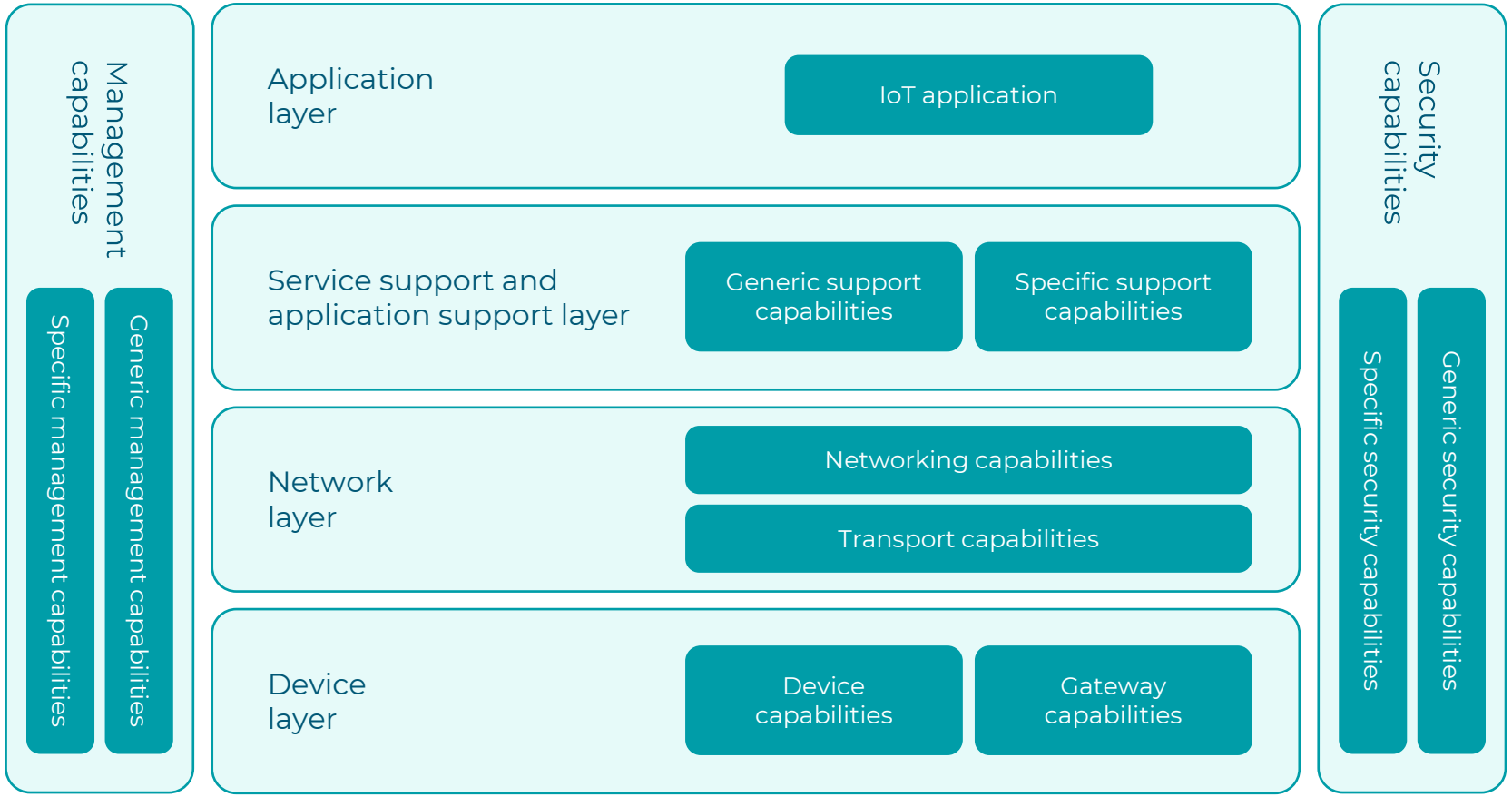
- 30.5% of the vulnerabilities are high severity
- High severity vulnerabilities are critical and have very high attack and damage potential
- These vulnerabilities should be identified and fixed on priority

Distribution Of All Vulnerabilities By CVSS Scores

CVSS Score	Number of Vulnerabilities	Percentage
0-1	1,007	0.60
1-2	1,196	0.70
2-3	8,327	4.60
3-4	9,460	5.20
4-5	42,973	23.70
5-6	34,116	18.80
6-7	27,136	15.00
7-8	36,000	19.90
8-9	895	0.50
9-10	19,978	11.00
Total	181088	

© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

IoT Architecture



Taxonomy Of Vulnerabilities In IoT

Application Layer

- Buffer overflow
- Code injection
- Sensitive data/permission manipulation
- Phising
- Authentication

Middle Layer

- Cloud attacks
- SQL injection
- Web server attacks

Network Layer

- DDos attack
- Traffic analysis
- Mana-in-the-middle
- Replay attack
- Sniffing attack

Device Layer

- Tag based attacks
- Eves dropping
- RF jamming
- Spoofing

© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

Common Vulnerabilities And Exposures

- CVE-2021-22893
- CVE-2020-8260
- CVE-2020-8243
- CVE-2019-11539
- CVE-2019-11510

Pulse Secure VPN

- CVE-2020-8196
- CVE-2020-8195
- CVE-2019-19781
- CVE-2019-11634

Citrix

- CVE-2021-34523
- CVE-2021-34473
- CVE-2021-31207
- CVE-2021-26855

Microsoft Exchange

- CVE-2021-22986
- CVE-2020-5902

F5

- CVE-2020-2021
- CVE-2019-1579

Palo Alto

- CVE-2021-28799
- CVE-2020-36198

QNAP

- CVE-2019-0708
- CVE-2020-1472
- CVE-2021-31166
- CVE-2021-36942

Microsoft Windows

- CVE-2017-0199
- CVE-2017-118822
- CVE-2021-40444

Microsoft Office

- CVE-2021-21985

vCenter

© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

Vulnerabilities Exploited In Ransomware Attack Path

Vulnerability identified	CVE-2021-44228, CVE-2021-45046, CVE-2021-44832, CVE-2017-5645, CVE-2021-45105, CVE-2019-17571
Vulnerability category	Remote code execution, denial of service

© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

IoT Attack Flow: Ransomware Use Case

Nov 24 2021

Vulnerability Report

Vulnerability privately reported to Apache

Dec 9 2021

Exploits In the Wild

A remote code execution (RCE) vulnerability in Apache log4j 2 was identified being exploited in the wild

Dec 10 2021

CVE Alert Published

NIST published CVE Alert with CVSS of 10 (critical)

Dec 6-16 2021

Updates Released

Apache releases updates 2.15.0, 2.15.1, 2.16.0 and 2.17.0 (which removes Lookups)

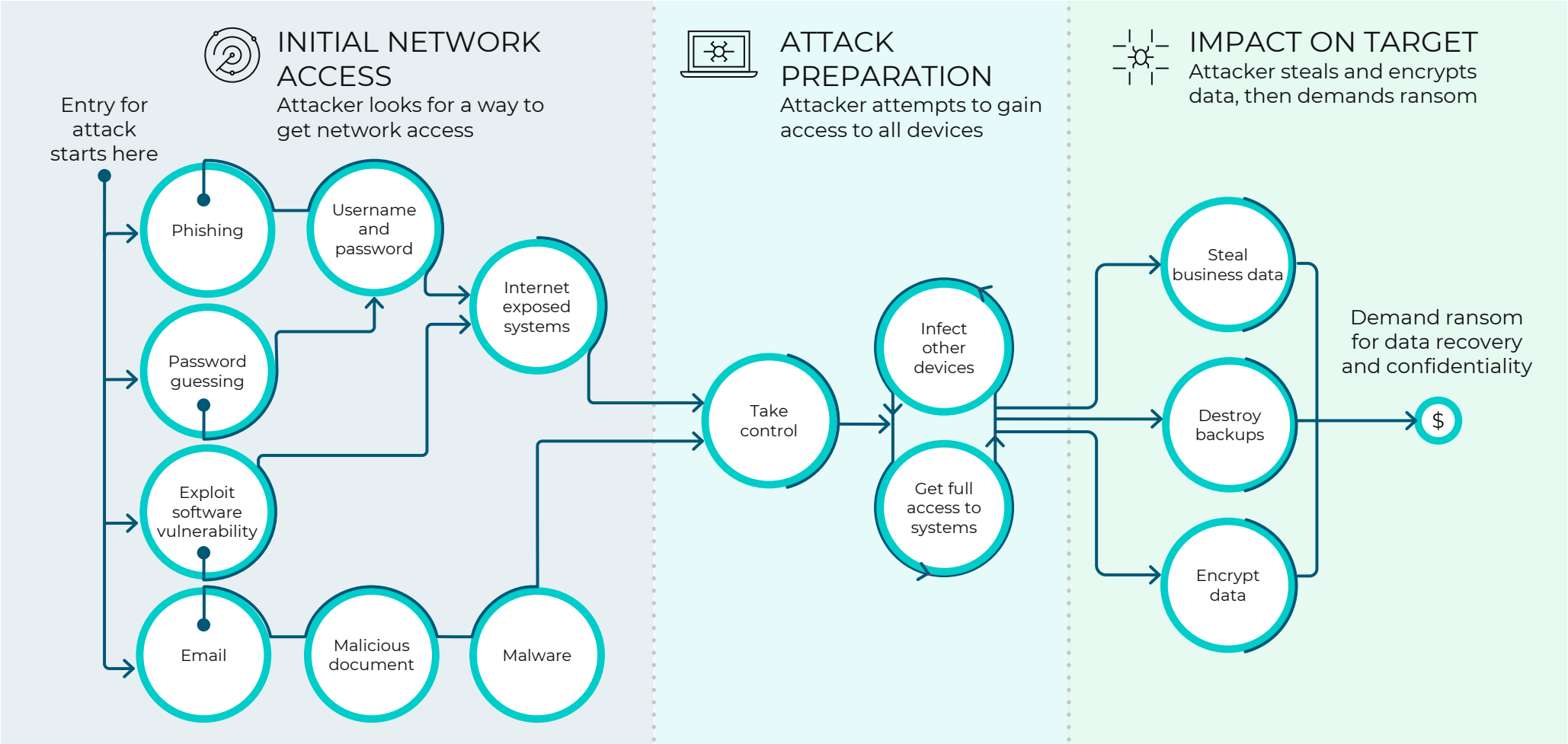
Dec 2021...

Attackers Scan for Vulnerable Systems

Widespread scanning, coin miners, botnets, nation states, access brokers associated with ransomware groups, Ransomware

© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

Ransomware Attack Path



© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

Vulnerability Assessment And Management

Scan Devices

- Periodically scan devices for open ports and services listening on those parts.
- Scan for weak and default passwords.

Analysis and Vulnerability Detection

- Find CPE based on the detected service and version.
- Identify vulnerabilities in the services using CPE.

Prevent and Protect

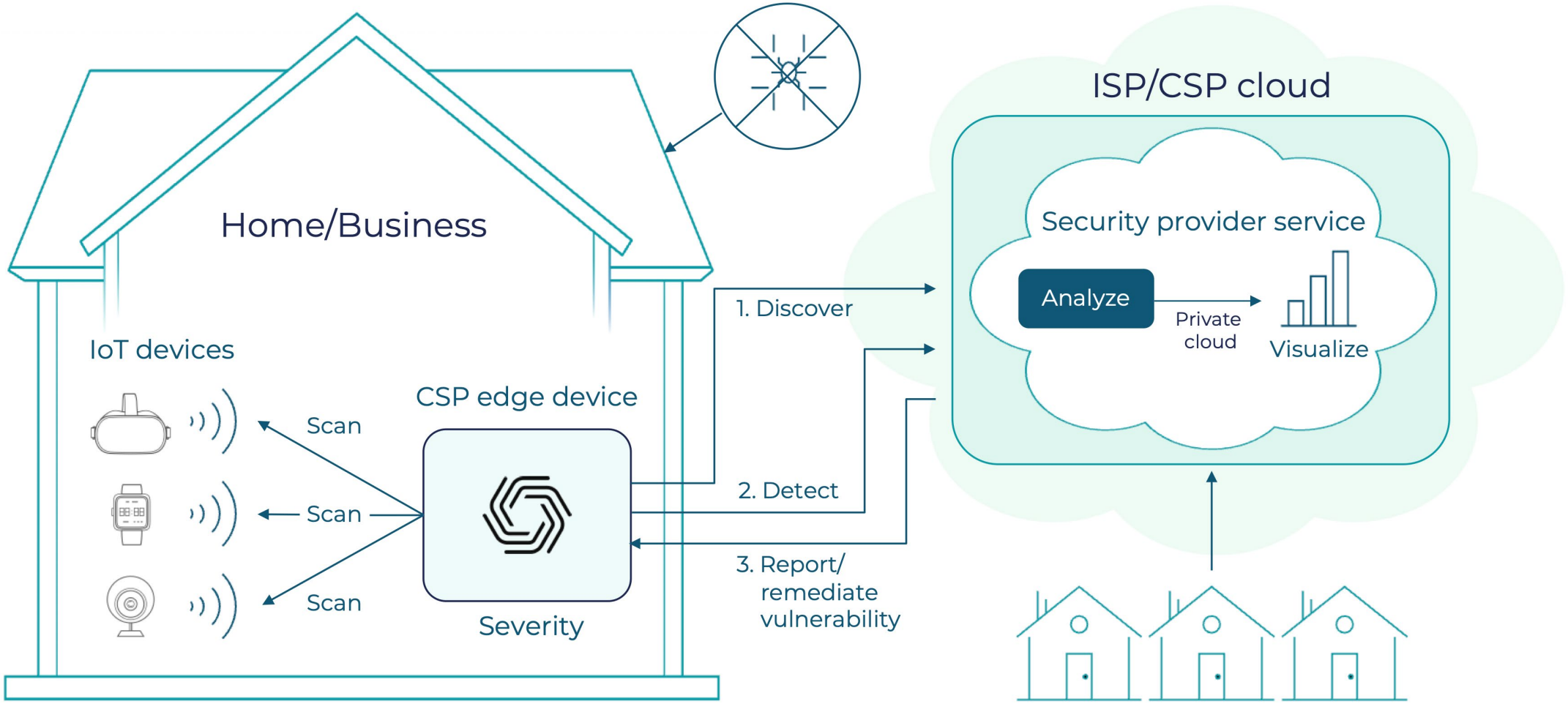
- Guide user to apply vendor patch.
- Immediate protection by creating and applying a virtual patch.

Reporting

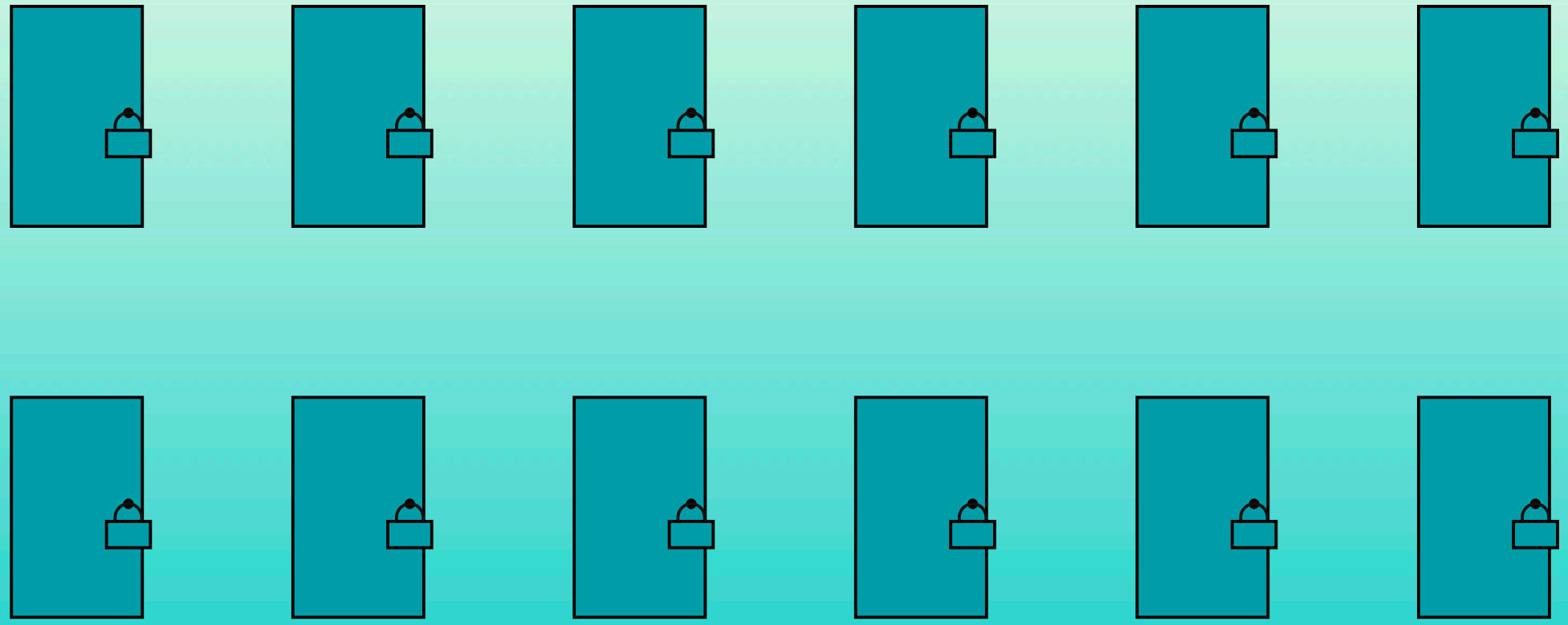
- Provide a vulnerability report to the user for awareness and visibility.
- Provide the threat exposure score on vulnerability severity.

© 2022 Society of Cable Telecommunications Engineers, Inc. a subsidiary of CableLabs | expo.scte.org

Discover, detect, report, remediate



Too many doors



SCTE
a subsidiary of CableLabs®

Creating Infinite Possibilities.

Thank You!

Mangesh Bhamre, Senior Manager of Product (Cybersecurity), Plume Design, Inc.

mbhamre@plume.com
1-408 498 5512