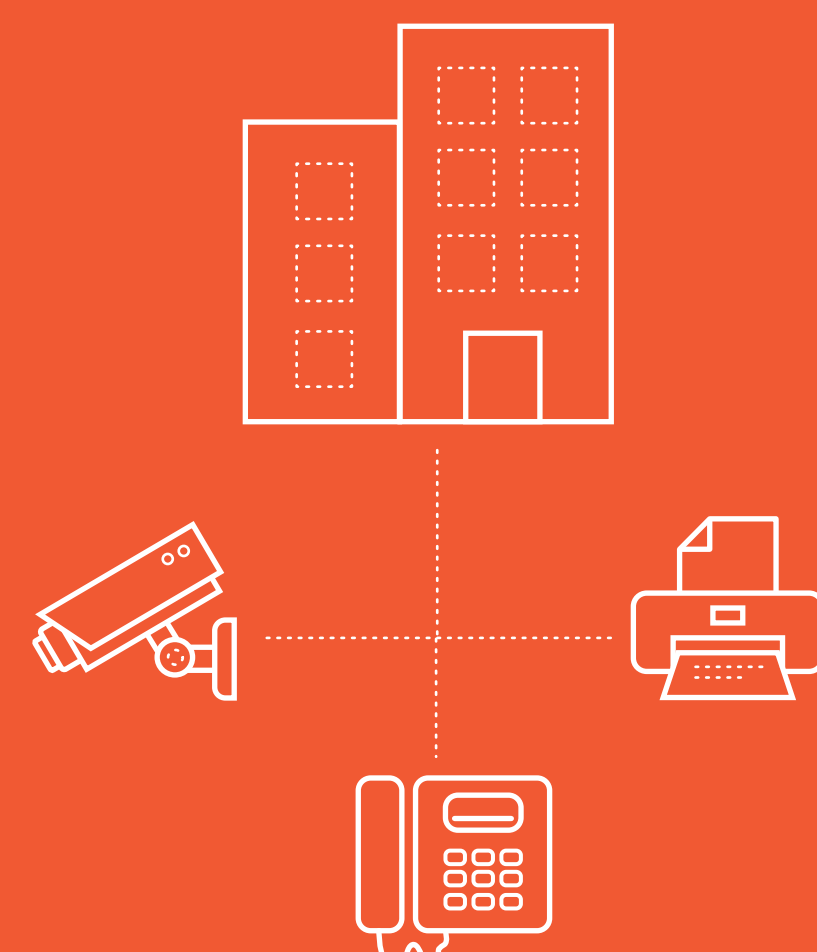


State of Enterprise IoT Security in 2020

While the internet of things (IoT) opens the door for innovative new approaches and services in all industries, it also presents new cybersecurity risks. Today an increasing number of newly developed IoT and operational technology (OT) devices are either connected to the network or to the internet, leaving organizations vulnerable to new IoT-targeted malware as well as legacy attack techniques that are finding new life.

IoT Adoption is Soaring in the Enterprise

Today **>30%** of all network-connected endpoints are IoT devices (excluding mobile devices) at the average enterprise.



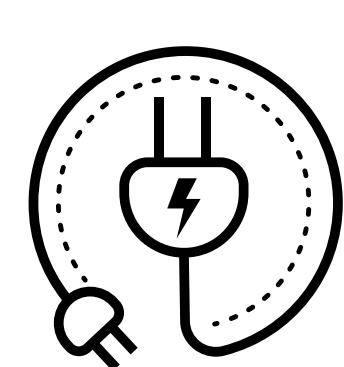
5.8B

IoT endpoints in 2020, up from **4.8B** in 2019¹

21%

Increase from 2019²

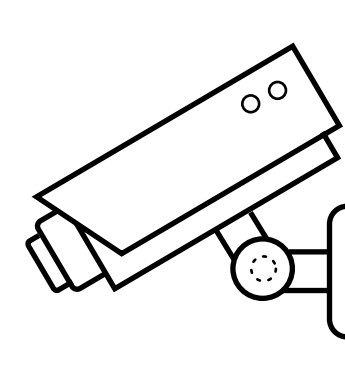
ENTERPRISE SEGMENTS WITH HIGHEST USE IN 2020



Utilities

1.37B

IoT endpoints in 2020

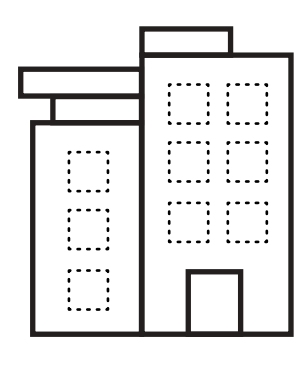


Physical Security

1.09B

IoT endpoints in 2020

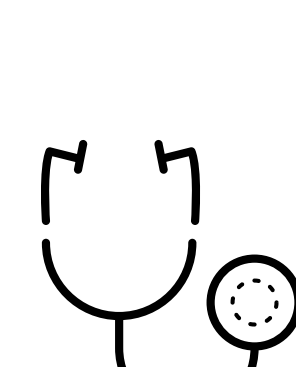
ENTERPRISE SEGMENTS WITH LARGEST GROWTH IN 2020



42% Building Automation



31% Automotive



29% Healthcare

Security is a Cause for Concern

98%

of all IoT traffic is unencrypted, exposing personal and confidential data on the network.

57%

of IoT devices are vulnerable to medium- or high-severity attacks, making IoT the low-hanging fruit for attackers.

83%

of medical imaging devices run on unsupported operating systems—a 56% jump from 2018

What is an IoT Device?

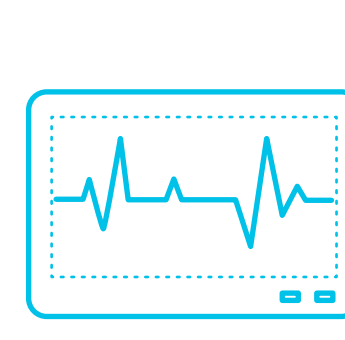
A network connected electronic device that senses or interacts with an internal state or the external environment, including operational technology (OT) devices that monitor and control equipment or their processes. These devices are all targets for attackers, and often aren't maintained by IT, unlike computers and phones that are managed by agents.

IoT Devices with Highest Share of Security Issues



Medical Imaging Systems

51%



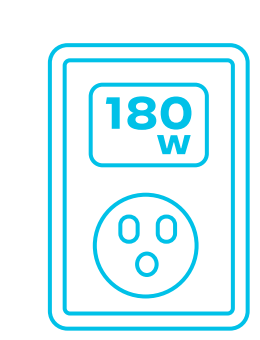
Patient Monitoring Systems

26%



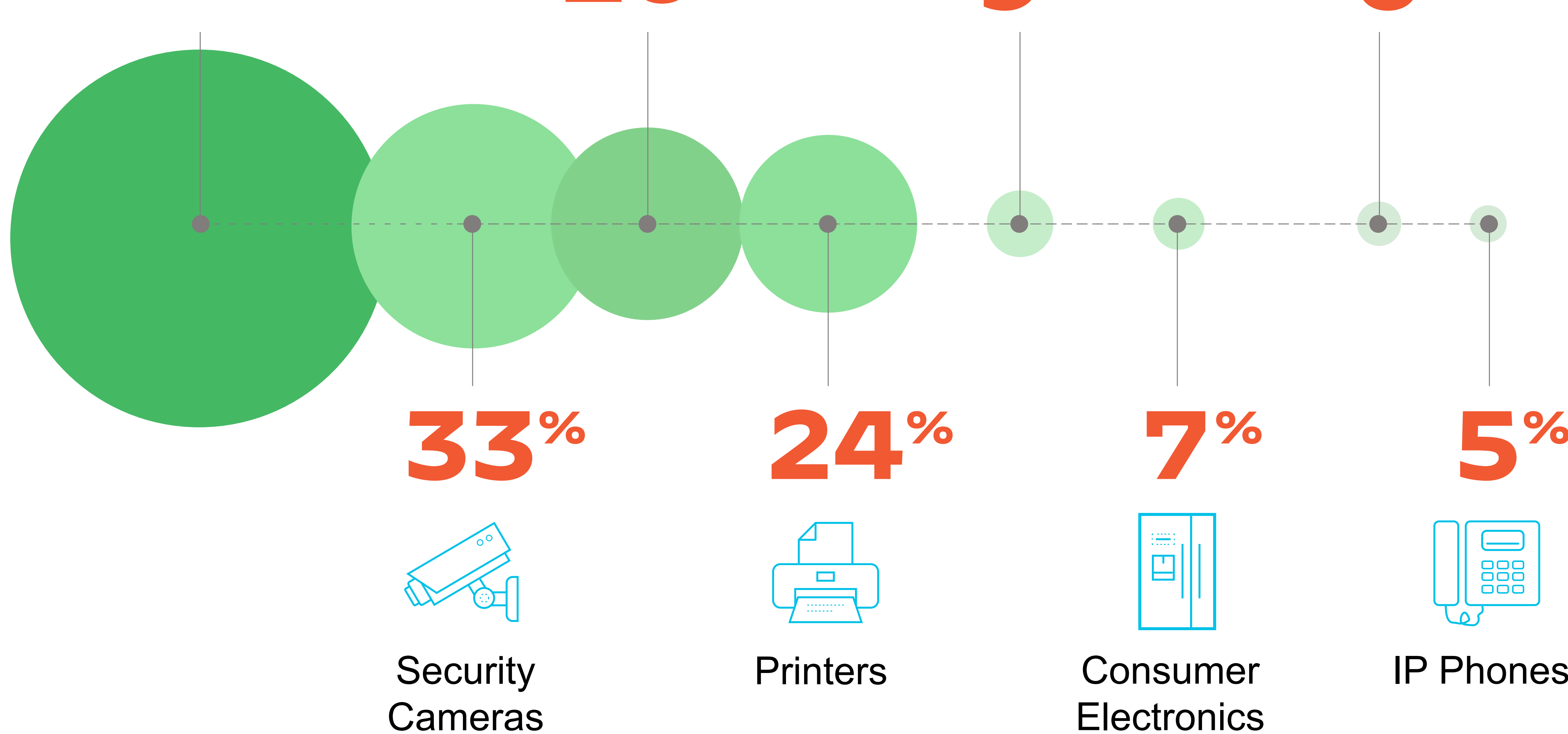
Medical Device Gateways

9%

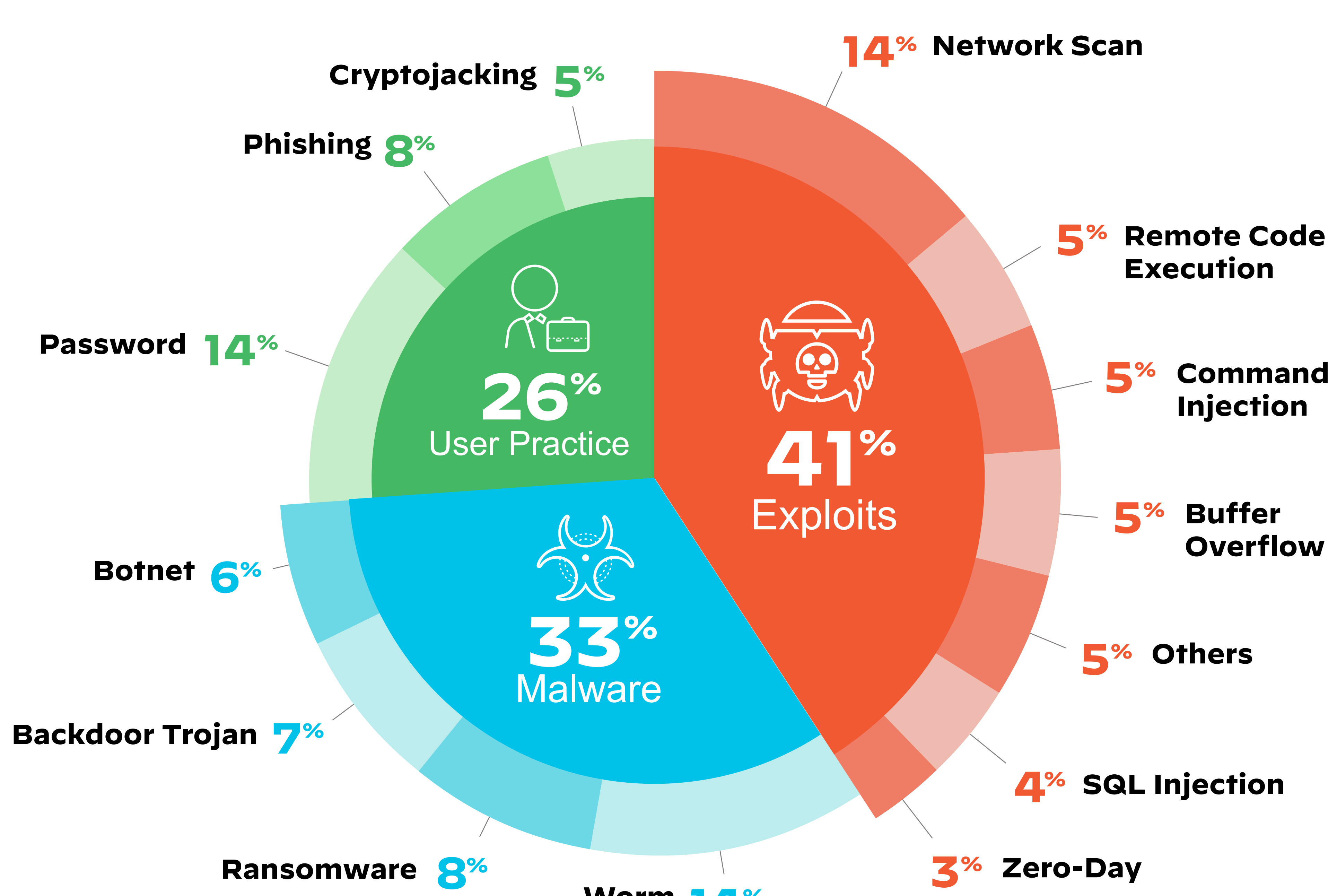


Energy Management Devices

6%



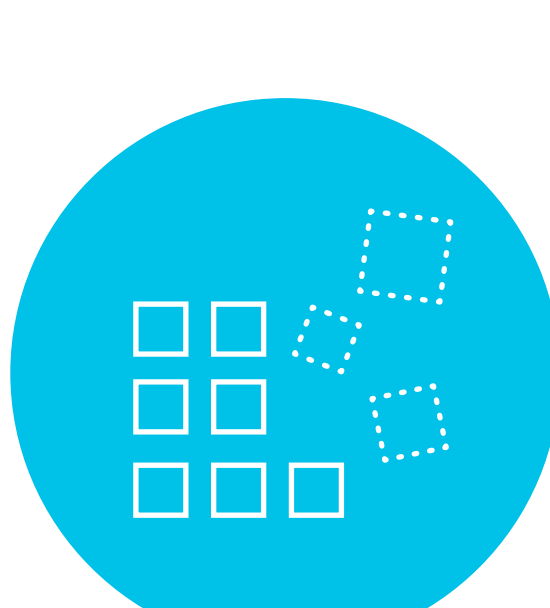
Breakdown of Top 3 IoT Cyber Threats



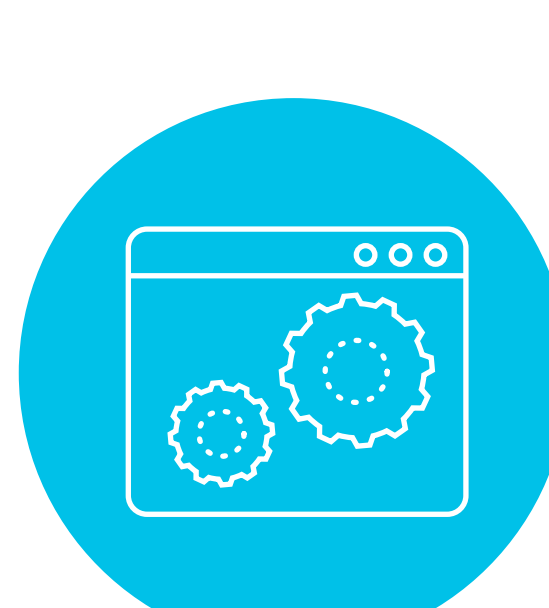
Why are IoT Devices Ideal Entry Points for Attacks



Zero to Minimum Built-In Security



Browser Interface Vulnerabilities



Outdated Operating Systems



Failure to Adhere to Security Best Practices

What Should You Do Next?



The short answer for enterprises looking to safeguard their IoT investments is: Know and manage risks with an effective IoT security strategy.

Read our 2020 Unit 42 IoT Threat Report to learn from our analysis of 1.2 million IoT devices. Uncover ways to perfect your IoT strategy with actionable next steps to immediately reduce IoT risk.

GET REPORT

1,2. Gartner Press Release on Scenarios for the IoT Marketplace, 2019 <https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-iot-2020-unit-42-iot-threat-report>, Palo Alto Networks <https://start.paloaltonetworks.com/unit-42-iot-threat-report>