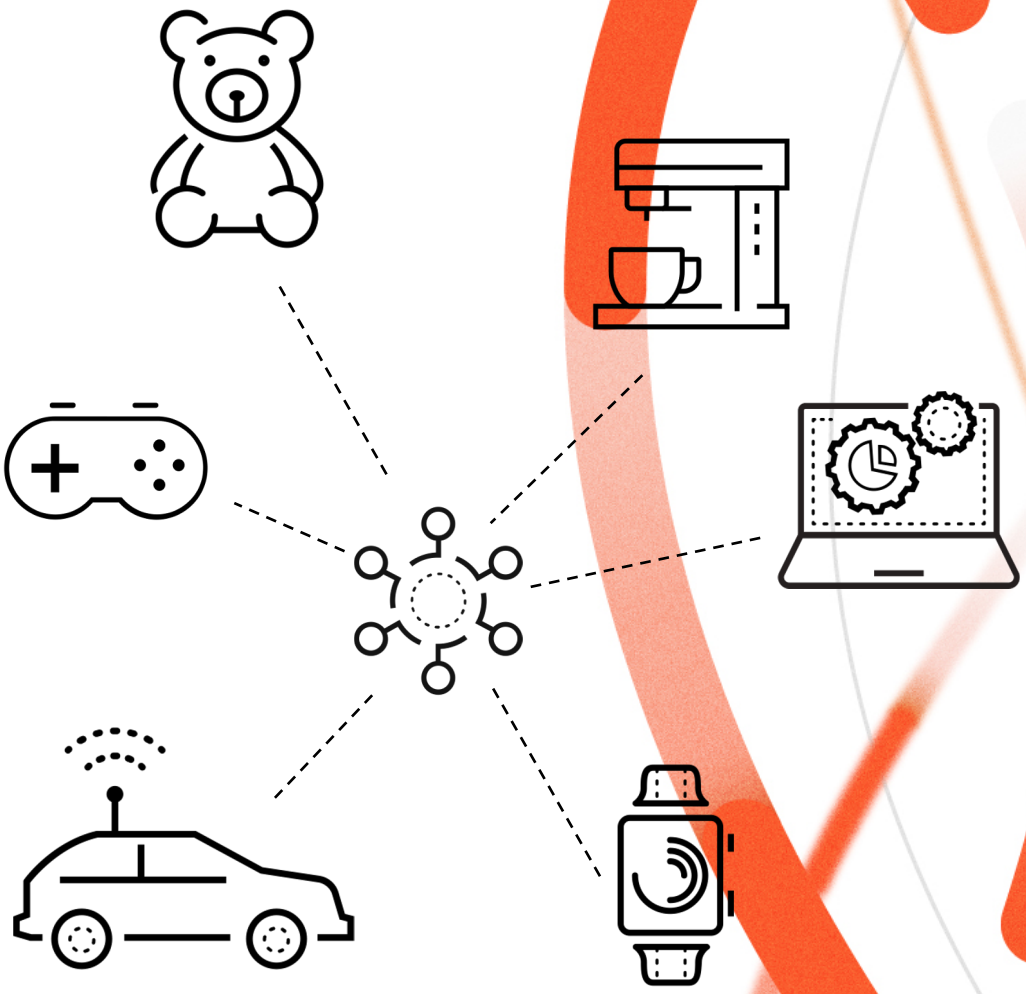
paloalto NETWORKS

The Connected Enterprise: IoT Security Report 2020



International study, September 2020

EXECUTIVE SUMMARY

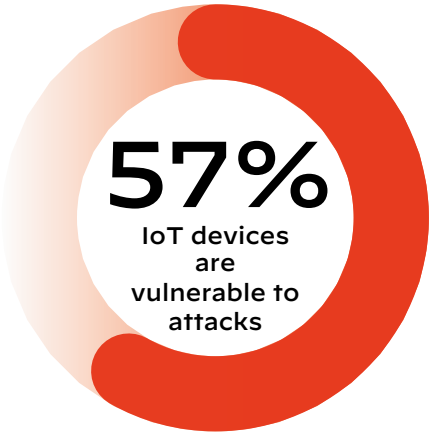
In an ongoing effort to shed light on security threats posed by the surge in internet of things (IoT) device deployment, Palo Alto Networks, the global cybersecurity leader, commissioned research company Vanson Bourne to conduct a survey on IoT security practices. It polled 1,350 IT business decision-makers in 14 countries across Asia, Europe, the Middle East and North America.

Most IT decision-makers (95%) say they are confident that they have visibility of all the IoT devices on their organizations' networks. They are seeing a growing number of devices as well as a greater variety, such as connected vehicles (27%), connected toys (34%) and wearable medical devices (44%).

While these decision-makers say they can see the problem growing, they know they are not prepared for it. 41% of respondents said they need to make a lot of improvements to the way they approach IoT security, and 17% said that a complete overhaul is needed, amounting to more than half of those polled.

A GROWING CHALLENGE

IoT is the soft underbelly of many businesses and an area they need to do more to protect. Failure to secure IoT poses a major threat to organizations. According to research conducted by Unit 42, Palo Alto Networks threat intelligence research arm, 57% of IoT devices are vulnerable to attacks of medium to high severity.

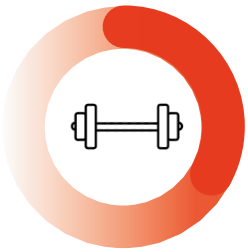


IoT device proliferation is a growing issue. Most IT decision-makers (89%) reported seeing increased numbers of IoT devices on their networks in the past 12 months, with more than a third (35%) reporting a significant increase.

The challenges are growing in terms of both volume and variety. More non-business devices are coming onto networks, with everything from connected teddy bears to medical devices to electric vehicles now needing to be secured alongside business IoT.

44%
Connected medical wearables

43%
Connected kitchen appliances (e.g. kettles, coffee machines)



38%
Connected sports equipment (exercise machines, skipping ropes, weights)

35%
Connected gaming devices

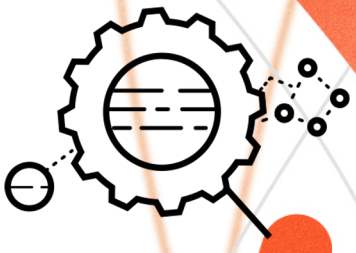
34%
Connected desk toys (teddy bears, robots etc.)

27%
Connected cars

YOU CAN'T SECURE WHAT YOU CAN'T SEE

Most IT decision-makers (95%) are confident that they have full visibility of all the IoT devices connecting to their organizations' network.

However, their reported belief in their ability to completely secure these IoT devices does not reflect this confidence. Only 4% believe there is no need to improve their current IoT security practices, with more than a combined half of respondents recognizing that they either need to make a lot of improvement (41%) or that a complete overhaul is needed (17%). Mid-sized businesses—those with 1,000-2,999 employees—are most likely to say that a complete overhaul is needed (21%).



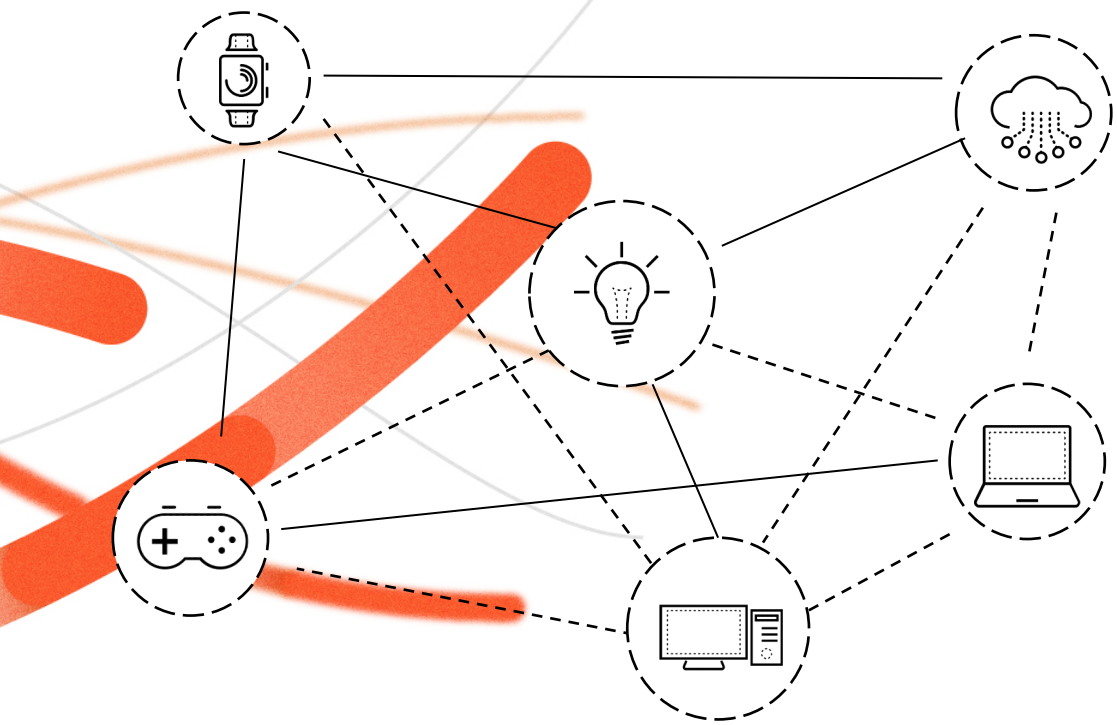
SLOW TO SEGMENT

The analysis shows that many businesses are struggling as they try to apply robust IoT security practices. Only one in five (21%) of the IT decision-makers surveyed reported having implemented best practices of using microsegmentation to contain IoT devices in their own tightly controlled security zones.

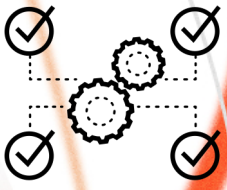
Conversely, nearly one in four (24%) reported that they have not yet segmented IoT devices onto a network separate from the one they use for primary devices and critical business applications—a cause for concern about the security of IoT networks in these organizations.

24%

of IT decision makers reported that they have not yet segmented IoT devices onto separate networks



Only **21%** of IT decision makers reported using micro-segmentation to contain IoT devices to their own tightly controlled security zones



CREATING A SECURE FUTURE

Organizations can take five steps to strengthen their IoT security:

1. Employ device discovery for complete visibility
   The first thing businesses need to do is get visibility into the exact number and types of devices on their networks, keeping a detailed, up-to-date inventory of all connected IoT assets, their risk profiles, and their trusted behaviors.

2. Apply network segmentation for stronger defense
   Businesses should divide their networks into subsections to enable granular control over lateral movement of traffic between devices and workloads, reducing the attack surface. Virtual local area network (VLAN) configurations and next-generation firewall policies should be used to keep IoT assets and IT assets separate.

3. Adopt secure password practices
   Strong password security is fundamental to securing IoT devices. As soon as an IoT device is connected to the network, the IT team should change the weak default password with a secure one that aligns with the organization's password policies.

4. Continue to patch and update firmware when available
   Most IoT devices are not designed to patch security flaws regularly, so it is critical that IT teams ensure devices are regularly patched for known vulnerabilities. To avoid data loss, add dedicated IoT-aware file and web threat prevention as well as virtual patching capabilities via intrusion prevention.

5. Actively monitor IoT devices at all times
   Traditional endpoint security solutions require software agents that IoT devices are not designed to take. organizations should implement real-time monitoring to continuously analyze the behaviour of all network-connected IoT endpoints by integrating existing security postures with their next-generation firewall.

paloalto NETWORKS

For more information on IoT security