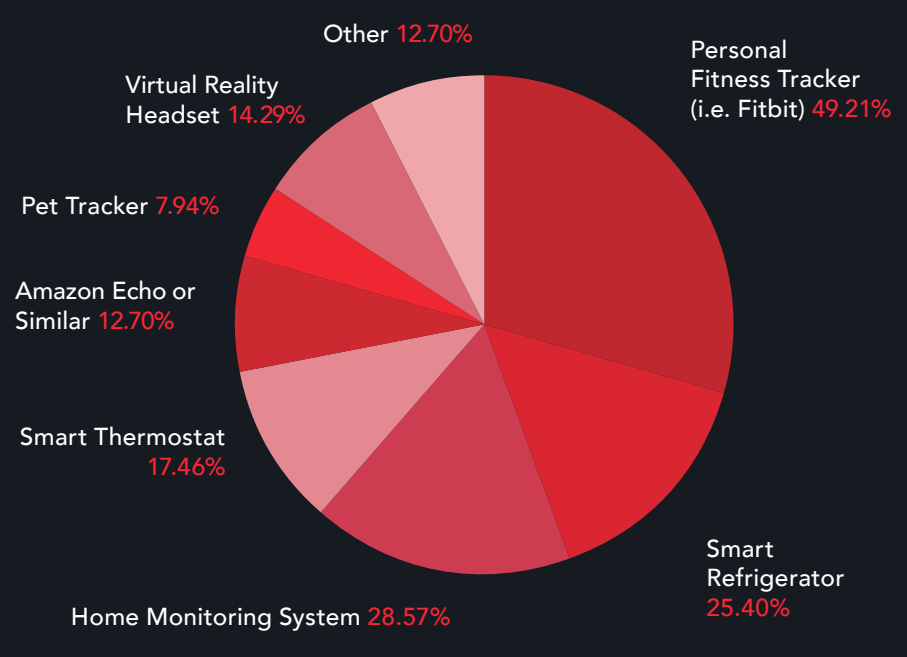
IOT SECURITY: *A COMING CRISIS?*

The proliferation of Internet of Things (IoT) devices in 2017 has been staggering, with 8.4 billion devices currently in use, and a total of 25 billion devices projected by 2020. As the use of these devices continues to increase, so do the associated risks. By 2020, it is estimated that 25% of cyber attacks will target IoT devices. We surveyed IoT users from around the world to better understand their behaviors and concerns. The results were concerning. Yes, consumers are concerned about the risks posed by IoT devices, but the lack of use of third-party security tools, as well as a general lack of knowledge of IoT's scale, are likely to be problematic for the future of IoT security.

ADOPTION OF IOT IS GROWING

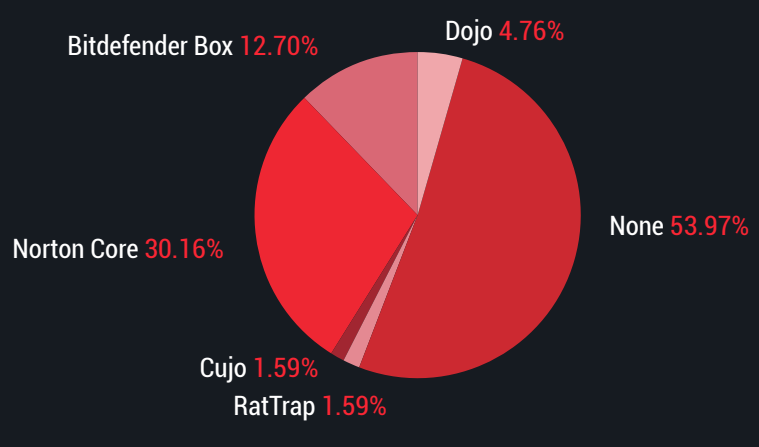
41% OWN AN IOT DEVICE



Q. DO YOU OWN AN IOT PRODUCT? IF SO, WHICH ONE(S)?

BUT SECURITY IS LACKING

54% HAVE NO ADDED SECURITY



Q. DO YOU USE ANY SECURITY PRODUCTS TO PROTECT YOUR IOT DEVICES?

35% DON'T CHANGE PASSWORD

Many IoT devices continue to use default administrator passwords, and as a result are the #1 attack vector for hacks.

Q. DO YOU REGULARLY UPDATE THE PASSWORD ON YOUR HOME ROUTER?

AND SO IS AWARENESS OF THE IOT'S VULNERABILITY

17% **KNOW OF MIRAI**
Last fall's Mirai botnet, which centered on IoT devices and shut down a large part of the Internet, is something unknown to the majority of IoT users.

KNOW HOW BIG
Many users guessed in the millions, but that is way off. With an estimated 25 billion IoT devices--from smart lightbulbs to self-driving cars--projected to be in use by 2020, the possibility of a security breach is huge.
22%

Q. ARE YOU FAMILIAR WITH THE MIRAI IOT HACK FROM 2016?

Q. HOW MANY IOT DEVICES ARE THERE ESTIMATED TO BE BY THE YEAR 2020?

HOW IOT USERS CAN PROTECT THEMSELVES

1. Access the device through an app or admin panel and immediately change its login and password.
2. Change both the default login password on your home router and your Wifi password every 3 months.
3. Ensure software for all devices and connected systems is up to date (including router firmware).
4. Ensure you understand what data is being collected and stored by your connected devices.
5. When it doubt, don't connect the IoT device to the internet.

TRUSTLOOK

September 2017 survey of 225 Trustlook users
For more information on IoT security, please visit www.trustlook.com