GLOBAL X

How Cybersecurity Will Accelerate IoT's Growth

We expect the 2020's decade to be defined by near-ubiquitous connectivity. All types of devices in our homes, workplaces, and cities are expected to be internet-enabled to seamlessly capture and transmit data. Semiconductors costs have declined over 90% over the last decade, making such connections remarkably inexpensive. And the rollout of 5G will allow data to transfer between devices and the cloud virtually instantaneously, at speeds up to 100 times faster than 4G.

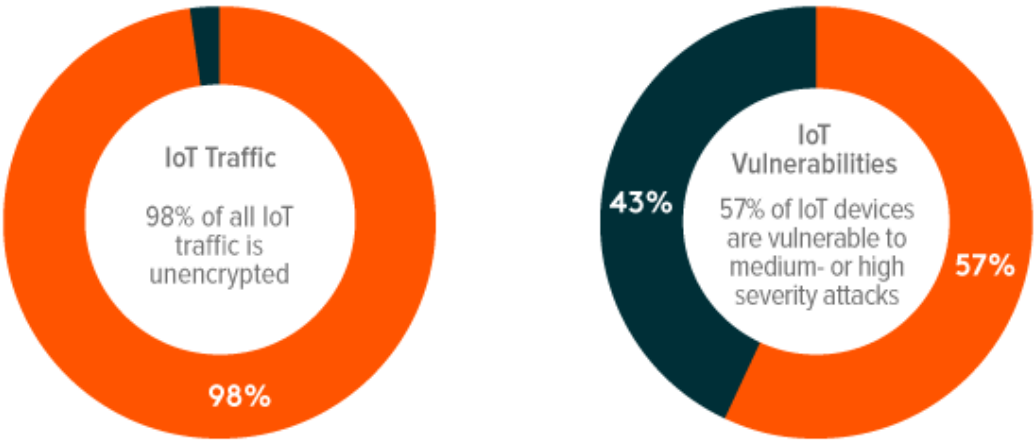
As the Internet of Things (IoT) brings millions of devices online, it creates vast opportunities for individuals and corporations, but it also introduces new types of risks and vulnerabilities. Each of these millions of devices presents new entry points for hackers, adding challenges and complexity to effectively manage security for firms and individuals. Successful IoT deployments will require multi-layered, end-to-end security that ranges from up front baked-in security requirements to the ongoing management and protection of sensitive machine-generated data.[1] There will be no one-size-fits-all solution, but the world's leading cybersecurity firms are preparing to protect this vast expansion in a new era for the internet.

New Devices, New Threats

The Internet of Things is central to many emerging technologies and themes, including autonomous vehicles, smart cities, smart factories, and health devices. But internet-enabled devices also create new targets for hackers who want to steal or ransom valuable private data. Today, 98% of all IoT device traffic is unencrypted, causing 57% of IoT devices to be highly vulnerable to cyberattacks, exposing personal and confidential data on a network.[2] We can expect the number and degree of incidences to increase with the proliferation of connected devices.

IOT'S CYBERSECURITY

Source: Palo Alto Networks

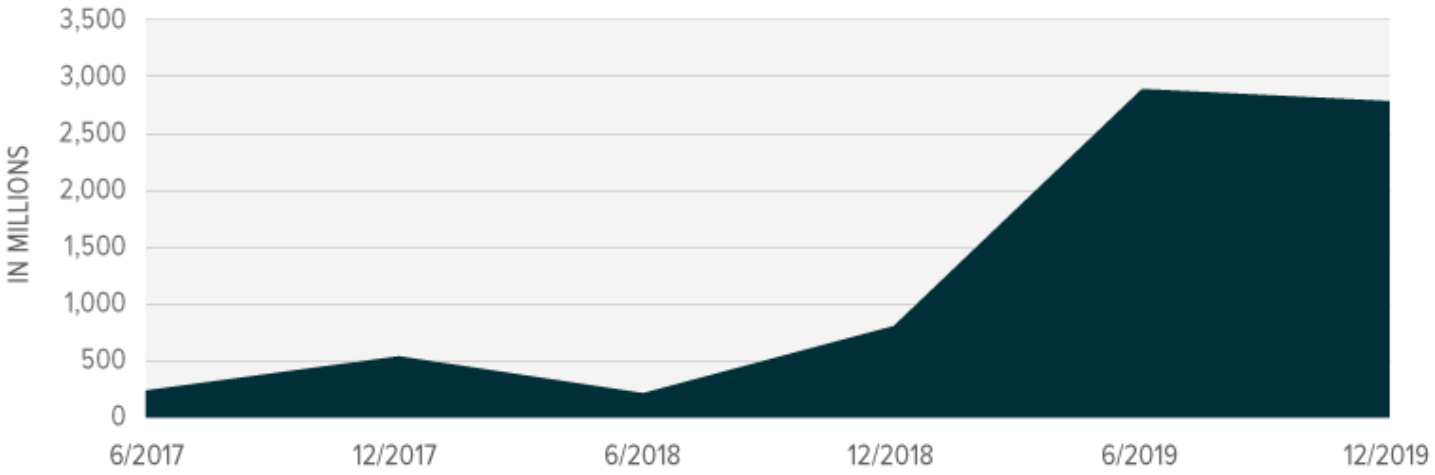


Take smart speakers, for example – a relatively new market that grew from internet giants looking to enter our homes via virtual assistants. In 2018, a weakness in Amazon's Alexa code enabled hackers to eavesdrop on users. Typically, Alexa is supposed to start recording only after detecting the wake word "Alexa," and terminate recording after a receiving a command ("Turn off the lights!"). Yet hackers programmed Alexa to continue listening well after a command, effectively allowing them to record users' conversations. Fortunately, the hackers were actually researchers without malicious intent and alerted Amazon of their findings.[3] The company pushed security fixes immediately.

Many hackers, however, do have malicious intentions, and their prevalence is on the rise. To help plan defenses, cybersecurity firms use honeypots as decoy servers to gauge trends and patterns of a cyberattack. Honeypots, which are set up all over the world, can receive attacks from connected devices such as a malware-infected smartwatch or a connected toothbrush. In 2019, security researchers found that honeypots documented a 446% year-over-year increase in attack traffic, with the number of hits rising from 1.0 billion to 5.7 billion.[4]

TOTAL GLOBAL HONEYPOT ATTACKS PER PERIOD

Source: F-Secure, Attack Landscape H2 2019



Note: Estimates include traditional connected devices

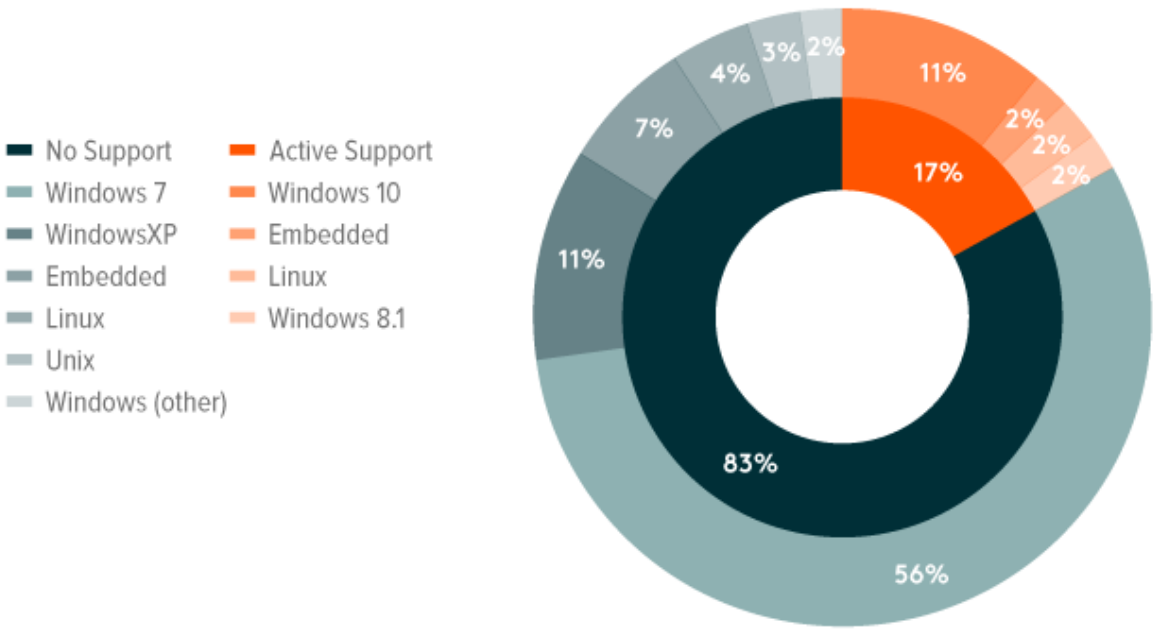
Your Health Can Be Hacked

The advent of connected cars, smart cities, and next-generation health devices mean hackers may not just steal private data in the virtual world, but also target devices that bridge the digital and physical world. Devices that comprise the Internet of Medical Things (IoMT) are particularly sensitive entry points for hackers. In 2013, hacking fears caused doctors to replace former US Vice President Dick Cheney's WiFi-connected pacemaker with one without WiFi capacity.[5] Four years later, the Food and Drug Administration (FDA) recalled nearly half a million connected pacemakers due to the potential for hacking.[6] Digital pills are another potential target. While they have chips that can capture diagnostic information as they travel along the gastrointestinal tract, such information could be intercepted by hackers.[7]

Recent research on IoT medical imaging devices found that 83% are running on unsupported operating systems.[8] Healthcare organizations that use these devices may be increasingly vulnerable to attacks that can expose sensitive medical information.

BREAKDOWN OF OS SUPPORT FOR MEDICAL IMAGING DEVICES

Source: Palo Alto Networks. As of Dec 31, 2019.



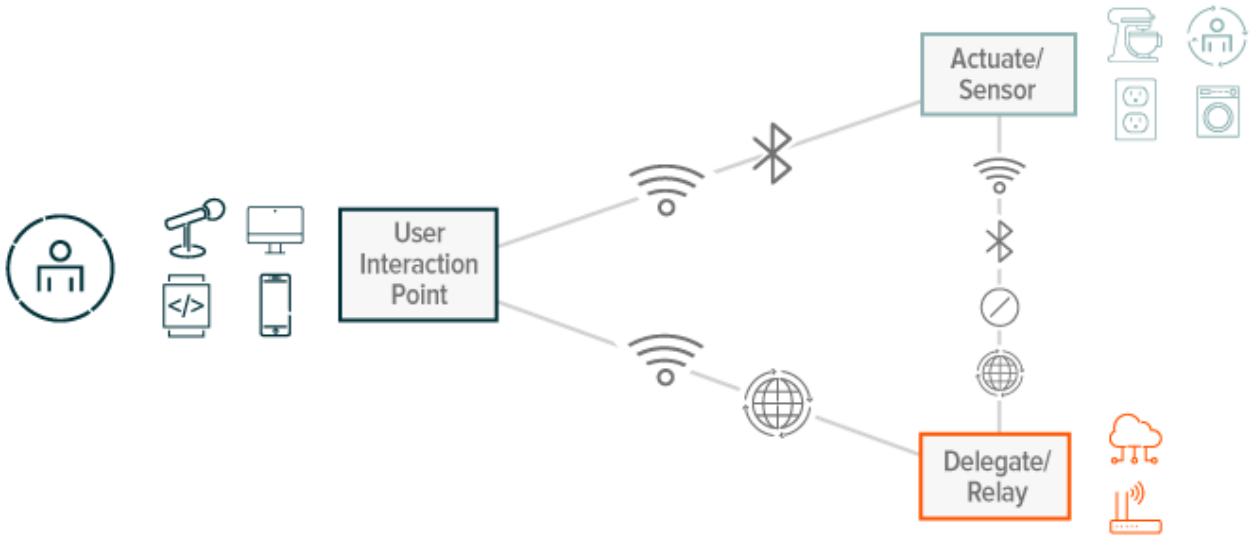
Answering questions about how to secure connected devices like these are of utmost importance for medical providers and patients to use this technology safely. The stakes are particularly high for IoMT device manufacturers. According to FDA guidelines, the manufacturers bear total responsibility for safety and performance.[9]

Securing Endpoints

The earliest endpoint security firms initially focused on laptops, PCs, and smartphones, but their focus often now extends to connected IoT devices. Endpoints consist of two main categories. A user interaction point is where users input commands and their device displays the requested information, for example, your smartphone. The second category includes actuator or sensor devices, such as a smart speaker or smart bulb, that responds to the commands from the user.

INFRASTRUCTURE OF IOT ECOSYSTEM

Source: Nan Zhang, Soteris Demetriou, et al. Understanding IoT Security Through the Data Crystal Ball: Where We Are Now and Where We Are Going to Be



IoT architecture is typically bidirectional, allowing data to be generated from an actuator or sensor and then sent to both the user interaction point and to cloud storage. For example, a smart security camera may sense motion, sending a notification to one's phone and capturing images that are stored in the cloud.

Given this architecture, IoT devices, user interaction points, and cloud storage require security measures to protect data. For IoT devices, there must be protections within the operational software known as microcode that is patched to the hardware. Therefore, today's cybersecurity firms work hand-in-hand with IoT device manufacturers in device design and testing, incident response, and threat modeling.[10]

Controlling access to networks is also critical, a role taken on by network firewall companies. These companies identify and profile every device on a network. They monitor the devices continuously to ensure that they are not compromised and mobilize to take immediate action if they are.[11]

AI in the Fight

Increasingly, cybersecurity firms and device manufacturers are using artificial intelligence (AI) and machine learning (ML) applications to provide customized endpoint security solutions. Because IoT devices are so numerous in volume and variety, AI can help provide a scalable, customized cybersecurity systems. Such algorithms are trained to identify devices based on their hardcoded attributes and behavior. They may also use sensing engines to autonomously learn the 'normal' behavior for these devices once they are on the network. For example, with pacemakers or smart

pills, AI can predict performance based on previous results and then detect when the devices behave abnormally. When behavior does change, it's a potential indicator of a corrupted or attacked device.

While AI is used for cybersecurity defenses, hackers are also using it to create new, sophisticated, cyberthreats, such as data-poisoning. It's expected that through the next two years, 30% of all AI cyberattacks will leverage training-data poisoning.[12] Data poisoning consists on feeding IoT or connected devices with compromised and malicious data, tricking the systems to mistakenly classify data. To thwart new AI-based cyberattacks, cybersecurity firms continue to enhance their own AI applications in an ongoing arms-race.

Conclusion

A one-size-fits-all cybersecurity solution doesn't exist for the continued wave of connected devices. But the world's leading cybersecurity firms and IoT manufacturers continue to evolve their strategies and leverage the latest technology to implement protective measures. As the IoT continues to expand to new avenues, including infrastructure, health care, and transportation, it is critical that cybersecurity firms play a central role in securing these devices so digital attacks do not result in real world consequences.

Related ETF

BUG: The Global X Cybersecurity ETF seeks to invest in companies that could benefit from the increased adoption of cybersecurity technology. Companies include those whose principal business involves the developing and managing security protocols to prevent intrusion and attacks on systems, networks, applications, computers, and mobile devices

SNSR: The Global X Internet of Things ETF (SNSR) enables investors to access a potential high growth theme through companies at the leading edge of IoT, an approach which transcends classic sector, industry and geographic regions to target this emerging theme. In a single trade, SNSR delivers access to dozens of companies with high exposure to emerging IoT technology.

AIQ: The Global X Future Analytics Tech ETF (AIQ) seeks to invest in companies that potentially stand to benefit from the further development and utilization of artificial intelligence (AI) technology in their products and services, as well as in companies that provide hardware facilitating the use of AI for the analysis of big data.

Authored by:
Pedro Palandrani

Date:
Apr 15, 2020

Category:
Insights

Topics:
Technology

Share this:

FOOTNOTES

1. IoT Cybersecurity Alliance, “Demystifying IoT Cybersecurity,” 2017.

2. Palo Alto Networks, “2020 Unit 42 IoT Threat Report,” Mar 10, 2020.

3. Wired, “Hackers Found a (Not-So-Easy) Way to Make the Amazon Echo a Spy Bug,” Aug 12, 2018.

4. F-Secure, “Attack Landscape H2 2019: An unprecedented year for cyber attacks,” Apr 3, 2020.

5. Forbes, “What Is The Internet Of Bodies? And How Is It Changing Our World?,” Dec 6, 2019.

6. Business Insider, “The FDA has recalled about 500,000 internet-connected pacemakers over hacking fears,” Sep 1, 2017.

7. Alliance of Advanced BioMedical Engineering, “Smart Pills Enable Convenient Diagnostics and Accurate Therapy,” 2017.

8. Palo Alto Networks, (n2).

9. FDA, “ FDA informs patients, providers and manufacturers about potential cybersecurity vulnerabilities for connected medical devices and health care networks that use certain communication software,” Oct 1, 2019.

10. Rapid 7, “IoT Security Testing Services,” Accessed on Mar 31, 2020.

11. Fortinet, “Protect networks with IoT deployments,” accessed on Mar 31, 2020.

12. Business Chief, “Gartner: Top 10 technology trends,” Mar 11, 2020.

risks associated with additional regulatory oversight with regard to privacy/cybersecurity concerns. Declining or fluctuating subscription renewal rates for products/services or the loss or impairment of intellectual property rights could adversely affect profits. Information Technology Companies can be affected by rapid product obsolescence and intense industry competition. International investments may involve risk of capital loss from unfavorable fluctuation in currency values, from differences in generally accepted accounting principles or from social, economic or political instability in other nations. The funds iare non-diversified.

Shares of ETFs are bought and sold at market price (not NAV) and are not individually redeemed from the Fund. Brokerage commissions will reduce returns.

Carefully consider the Fund's investment objectives, risks, and charges and expenses before investing. This and other information can be found in the Fund's summary or full prospectuses, which may be obtained by calling 1.888.493.8631, or by visiting globalxetfs.com. Please read the prospectus carefully before investing.

Global X Management Company LLC serves as an advisor to Global X Funds. The Funds are distributed by SEI Investments Distribution Co. (SIDCO), which is not affiliated with Global X Management Company LLC or Mirae Asset Global Investments. Global X Funds are not sponsored, endorsed, issued, sold or promoted by Indxx, nor does Indxx make any representations regarding the advisability of investing in the Global X Funds. Neither SIDCO, Global X nor Mirae Asset Global Investments are affiliated with Indxx.