Treadmills, Lightbulbs and Pet Feeders -- Oh My! Non-Business Connected Devices Are Creating More Risk for the Enterprise

October 20, 2021

IoT survey from Palo Alto Networks highlights the need for shared responsibility among remote workers and IT teams to secure their enterprise

SANTA CLARA, Calif., Oct. 20, 2021 /PRNewswire/ -- Cyber adversaries know that one small IoT sensor can provide entry into a corporate network to launch ransomware attacks and more. According to a survey of IT decision-makers by Palo Alto Networks (NYSE: PANW), 78% of respondents (among those whose organization has IoT devices connected to its network) reported an increase in non-business IoT devices on corporate networks in the last year. Smart lightbulbs, heart rate monitors, connected gym equipment, coffee machines, game consoles and even pet feeders are among the list of the strangest devices identified on such networks in the study.

For the second year, survey responses warn of needed security changes to protect corporate networks from non-business IoT devices. This year, 96% of the same group above indicated their organization's approach to IoT security needs improvement, and 1 in 4 (25%) said it needs a complete overhaul with the greatest security capability needs around threat protection (59%), risk assessment (55%), IoT device context for security teams (55%), and device visibility and inventory (52%).

"IoT adoption has become a critical business enabler. It presents new security challenges that can only be met if employees and employers share responsibility for protecting networks," said Ryan Olson, vice president of threat intelligence, Unit 42 at Palo Alto Networks. "Remote workers need to be aware of devices at home that may connect to corporate networks via their home router. Enterprises need to better monitor threats and access to networks and create a level of segmentation to safeguard remote employees and the organization's most valuable assets."

Worth noting, of the 1,900 global IT decision-makers polled by Palo Alto Networks this year, half (51%) indicated that IoT devices are segmented on a separate network from the one they use for primary business devices and business applications (e.g., HR system, email server, finance system), and another 26% of respondents said that IoT devices are microsegmented within security zones — an industry best practice where organizations create tightly controlled security zones on their networks to isolate IoT devices and keep them separate from IT devices to avoid hackers from moving laterally on a network.

There are other worthwhile steps for mitigating IoT security risk at home and in the enterprise.

Top 3 IoT Security Tips for the Work-from-Home (WFH) Employee

1. **Get more familiar with your router.** All of your IoT devices likely connect to the internet through your router. Start by changing defaults — the settings every router comes with — to something unique. Then encrypt your network by simply updating your router settings to either WPA3 Personal or WPA2 Personal.
2. **Keep track of which devices are connected.** You can access your router's web interface and look for "connected devices," "wireless clients" or "DHCP clients" to see a list and disconnect older devices you no longer use, and disable remote management on the devices where you don't need it.
3. **Segment the home network.** Network segmentation is not only for large corporations. You can segment your home network by creating a guest Wi-Fi network. The easiest way to do this is to have IoT devices use a guest Wi-Fi network, while other devices use the main network. This helps to logically group devices in your home and isolate them from each other. Keeping them on a separate network makes it difficult to get to your computers from a compromised IoT device.

Top 3 IoT Security Tips for the Enterprise

1. **Know the unknowns.** Get complete visibility into all IoT devices connected to the enterprise. An effective IoT security solution should be able to discover the exact number of devices connected to your network, including the ones you are and are not aware of — and those forgotten. This discovery helps collect an up-to-date inventory of all IoT assets.
2. **Conduct continuous monitoring and analysis.** Implement a real-time monitoring solution that continuously analyzes the behavior of all your network-connected IoT devices to contextually segment your network between your IT and IoT devices — and their workloads. Securing and managing WFH setups as branch extensions of the enterprise requires a new approach.
3. **Implement Zero Trust for IoT environments.** An IoT security strategy should align with the principle of Zero Trust to enforce policies for least-privileged access control. From there, look for an IoT security solution that leverages your existing firewall investment for comprehensive and integrated security posturing. Running in conjunction with the capabilities of your firewall, the solution should automatically recommend and natively enforce security policies based on the level of risk and the extent of untrusted behavior detected in your IoT devices. Additionally, a point solution can extend a corporate network and bring unified security policy management and secure access service edge (SASE) to WFH employees.

Palo Alto Networks helps secure IoT devices in two ways.

Palo Alto Networks IoT Security combines machine learning with patented App-ID™ technology to provide the most accurate and deepest level of visibility into your IoT and OT devices for effective baselining of their normal behaviors. The solution empowers security teams to proactively prevent threats, monitor device risk, detect anomalies, and recommend then apply policies for enforcement.

Palo Alto Networks also recently introduced Okyo Garde ™, an enterprise-grade cybersecurity solution for the home, delivered through a premium mesh-enabled Wi-Fi 6 system. Okyo Garde is designed to address the new hybrid work environment in which the workplace is as likely to be a kitchen table or spare bedroom as an office cubicle. Whether you have a small business, are an employee working from home or you simply want your home to be more cyber secure, Palo Alto Networks' Okyo Garde secures all the devices on your network. Currently available in the United States for personal and small business use, Okyo Garde provides superior Wi-Fi speed and coverage, unparalleled protection from malware, ransomware, phishing attacks and more, all while visible and easily controlled through a simple mobile app on your smartphone. Okyo Garde Enterprise Edition, with Prisma® Access integration, is expected to be available in the U.S. in early 2022.

For more information:

- To read The Connected Enterprise: IoT Security Report 2021, please visit this page.
- To learn more about Palo Alto Networks IoT Security, please visit this page.
- To learn more about Okyo Garde, please visit this page.

Survey Methodology
Palo Alto Networks commissioned technology research firm Vanson Bourne, which polled 1,900 IT decision-makers at organizations in 18 countries: United States, Canada, Brazil, United Kingdom, France, Germany, Netherlands, Middle East (comprising of UAE and Saudi Arabia), Spain, Italy, Ireland, Australia, China (including Hong Kong), India, Japan, Singapore and Taiwan.

About Palo Alto Networks
Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

Palo Alto Networks, App-ID, Okyo, Okyo Garde, Prisma, and the Palo Alto Networks logo are trademarks of Palo Alto Networks, Inc. in the United States and in jurisdictions throughout the world. All other trademarks, trade names, or service marks used or mentioned herein belong to their respective owners.

About Vanson Bourne
Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.

Palo_Alto_Networks_Logo

View original content to download multimedia:https://www.prnewswire.com/news-releases/treadmills-lightbulbs-and-pet-feeders--oh-my-non-business-connected-devices-are-creating-more-risk-for-the-enterprise-301404167.html

SOURCE Palo Alto Networks, Inc.