The Connected Enterprise: IoT Security Report 2021

Table of Contents

Executive Summary

In 2021, cyberattacks against IoT devices have gotten bigger and bolder—from hacking water treatment plants to security cameras and more. For the second year, an IoT security survey from Palo Alto Networks highlights the need for shared responsibility among work-from-home (WFH) employees and IT teams to secure the enterprise.

According to the 2021 survey, 78% of IT decision-makers who have IoT devices connected to their organization's 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 this year's study.

Remote workers need to be aware that IoT devices could be compromised and used to move laterally to access their work devices if they're both using the same home router, which in turn could allow attackers to move onto corporate systems. Everything using the same Wi-Fi network creates more risk, whether in a living room or at a coffee shop. Enterprise IT teams need to better monitor threats and device access to networks and create a level of segmentation to safeguard remote employees and limit access to the organization's most valuable assets.

Key Findings

The COVID-19 Pandemic Has Made It Harder to Keep IoT Devices Secure

These findings show that IoT security remains a challenge for organizations, who feel the problem has gotten worse with the rise of working from home. 81% of those who have IoT devices connected to their organization's network said the shift to remote work during the COVID-19 pandemic led to greater vulnerability from unsecured IoT devices on their organization's network, and 78% of respondents in the same group admitted to an increased number of IoT security incidents for their organization.

Greater Visibility of IoT Devices Reveals Improvements Needed with IoT Security

Interestingly, when asked if they are confident that they have visibility of the IoT devices connected to their organization's network, 97% of IT decision-makers responded that they were. However, nearly all (96%) of those who have IoT devices connected to their network also reported their organization's approach to IoT security requires an improvement, with one in four (25%) indicating the need for an IoT security strategy overhaul. The most required security capabilities are threat protection (59%), risk assessment (55%), IoT device context for security teams (55%), and device visibility and inventory (52%).

The truth is while many organizations are putting measures and best practices in place to limit network access, digital transformation is not only changing the way we work but the way we secure the way we work. Safeguarding IoT devices from cyberattacks is an ongoing challenge. Therefore, we are skeptical that today's enterprises have a true picture of the number of non-business IoT devices that may actually be putting their organizations at risk. With most cyberattacks and malware/ransomware accessing corporate networks months before they are detected, device asset management should be a critical component of a corporate IoT security strategy.

Organizations Are in Various Stages of Their IoT Security Journey

According to the survey, half (51%) of IT decision-makers who have IoT devices connected to their organization's network 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 in the same group 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 prevent hackers from moving laterally on a network. Dividing your network into zones helps create a Zero Trust architecture that executes a security philosophy of trusting no users, devices, or applications and verifying everything. The end goal is to create a network that allows access only to the users, devices, and applications that have legitimate business needs and to deny all other traffic.

Technology Leaders Are Losing Sleep over IoT Attacks

Security cameras, in particular, have generated headlines for allowing hackers to access sensitive and private video surveillance footage.

According to Palo Alto Networks research, which examined 135,000 security cameras in March, 54% of the examined cameras had at least one vulnerability. Such vulnerabilities make it possible for cameras to be hijacked and subsequently weaponized by cybercriminals, setting up these devices as springboards to perpetrate attacks and access broader corporate networks.

For this year's survey, we asked a new question to determine what type of IoT incidents are keeping IT leaders up at night. While IIoT (55%) and DDoS (50%) attacks rise to the top of their concerns, we were more surprised to see that there isn't one but many types of attacks that they worry about all the time, including breaches of connected home devices.

Table 1: The Types of Attacks Worrying Enterprise IT Leaders

Industrial Internet of Things (IIoT) attacks	55%
Distributed Denial of Service (DDoS) attacks	50%
Breach of connected cameras	46%
Breach of Internet of Medical Things (IoMT)	42%
Breach of connected home devices	37%
Breach of connected wearables	32%

IIoT attacks are a worrisome trend as operational technology and manufacturing environments undergo digital transformation, where IIoT is enabling many previously "dumb" items to become "smart"—becoming equipped with sensors that gather data and connect to the internet so that data can be shared to enable new business models and opportunities. IT leaders must ensure they're able to identify and protect IIoT devices to mitigate supply chain risks.

Meanwhile, DDoS attacks are returning as a significant threat. In late September, the U.S. National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) released guidance on securing virtual private networks (VPNs) for remote access because of the rise in DDoS attacks on these attractive targets. However, with applications moving to the cloud, users don't need to connect as often to the remote access VPN. A newer approach, gaining adoption across organizations, is to use a secure access service edge (SASE), which replaces the mix of VPNs and point products with a combination of networking and network security delivered as a service.

Just as vaccinations keep us safer from COVID-19, proactive prevention measures will place organizations in a better position to combat the cybercrime pandemic.

Security Best Practices

Top 5 IoT security tips for the 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. You can 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.
4. **Use two-factor authentication.** If a device offers two-factor authentication (a password plus something else like a code sent to your phone or a thumbprint scan), use it.
5. **Enable security updates.** Optimize the protection for IoT devices, even your router, when prompted for security updates. Most IoT devices offer software updates that often patch known vulnerabilities and issues. Make sure to "accept" when a device prompts you for a scheduled update.

Top 5 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 aware and 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 require 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 SASE to WFH employees.
4. **Take swift action to prevent known threats.** The diverse nature of IoT devices creates a highly distributed environment in your network with numerous points of compromise. Look for a threat prevention mechanism that uses payload-based signatures to block advanced threats on your IoT devices. This will ensure the most up-to-date security posture and defense against known threats for rapid, real-time responsiveness to anomalous IoT device vulnerabilities and weaknesses across your network.
5. **Implement fast detection and rapid response to unknown threats.** An IoT security solution should be capable of drawing from a cloud-delivered threat intelligence engine that delivers real-time malware analysis and protections from zero-day attacks to your IoT devices. Tapping into this data saves your IT security team valuable time by leveraging IoT identity information, risk scores, vulnerability data, and behavioral analytics to investigate never-heard-before threats unique to your IoT environment right from the outset.

Security Protections

Palo Alto Networks helps secure IoT devices in two ways:

1. 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.
2. In response to the growing demand by individuals and organizations alike for better cybersecurity from home, Palo Alto Networks recently introduced Okyo Garde™, an enterprise-grade cybersecurity solution 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. Currently only available for personal and small business use in the United States, Okyo Garde combines hardware, software, and security services in one seamless, simple subscription. Okyo Garde Enterprise Edition, with Prisma® Access integration, is expected to be available in the U.S. in early 2022.

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

For more information on Palo Alto Networks, visit www.paloaltonetworks.com.

For more information on IoT Security, visit www.paloaltonetworks.com/network-security/iot-security.

For more information on Okyo Garde, visit www.okyo.com.

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.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com