Publication date:
11 June 2020
Author:
Tanner Johnson

Palo Alto Networks IoT Cybersecurity Report

IoT cybersecurity has evolved from an industry-focused problem into an essential investment

Brought to you by Informa Tech

Contents

Executive summary

Catalyst

Historically, IoT cybersecurity solutions have been sought only by select organizations reliant upon specialist devices within their environments. Many of these entities deployed dedicated teams of personnel to address the potential risks associated with the introduction of IoT components. Today, IoT devices have infiltrated nearly every industry and market imaginable. These organizations are often reliant upon the effective operation and productivity of connected devices, despite a shortage of vendors integrating security solutions into their IoT device production. Additionally, the proliferation and monetization of malware and ransomware have shattered the naive belief that only organizations large enough to afford endpoint security solutions are likely targets. As organizational reliance on IoT devices is becoming ubiquitous, the potential consequences of compromise stemming from insecure IoT devices can be financially crippling for entities of all sizes. This scenario has resulted in corporations slowly recognizing that IoT cybersecurity is no longer a luxury, but an essential investment in long-term operational sustainability.

Omdia view

As our IoT ecosystem continues to grow in size, connectivity, and complexity, the requirement to effectively secure the components, and the information shared by the devices themselves, becomes essential. This multifaceted challenge requires a comprehensive and concerted effort from all members of an organization in order to integrate IoT security into current operational strategic priorities. Security needs to be implemented on the device, throughout the network, within the cloud, and throughout the entire data management process.

Key messages

- Customers face unique challenges when wrangling IoT security.
- In the absence of comprehensive standards, it can feel like the “wild west.”
- Misconceptions surrounding the IoT allow these challenges to persist.
- The incredible diversity of devices creates an urgent IoT security challenge.
- Any solution should be accessible to existing security teams with minimal disruption.
- Deploying an integrated network solution can help address the frequent absence of agents onboard IoT devices.

- Current NET SEC and SOC teams can deploy methodologies for secure IoT environments:
  - NET SEC
    - Step 1: Understand your IoT assets through discoverability and visibility
    - Step 2: Establish effective risk assessment
    - Step 3: Define policies for acceptable device behavior
    - Step 4: Prevent any known IoT attacks
  - SOC
    - Step 5: Detect and respond to unknown IoT threats

IoT customer challenges

More nodes = more problems

Every connected IoT component provides a node of communication that data thieves seek to exploit. As the sheer volume of devices continues to grow, the threat landscape itself increases proportionately. One of the consequences of this new reality is that opportunities for cyber adversaries to gain unauthorized access to these devices are increasing throughout the IoT ecosystem, as there are no real limits to the type of device that can be granted internet connectivity. Furthermore, as cyber criminals evolve more sophisticated campaigns and tactics over time, the threats introduced as a result of advanced connectivity will ultimately require additional protective measures be deployed by the respective user.

IoT device disparity

An additional complication that arises when attempting to tackle IoT security is the near-limitless forms that the IoT itself can take. For example, in the traditional enterprise market, these devices can include cameras, thermostats, building automation, HVAC systems, televisions, point of sale systems, printers, Wi-Fi routers, connected vehicles, and everything in between. Despite the mass adoption of IoT connectivity, the convenience created by the diversity of viable applications also introduces the largest hurdle for effective security. The added variety of IoT devices in terms of type, nature, and functionality carries its own security challenge. In addition, these various devices can utilize a wide range of operating systems (if one is even onboard), adding even greater complexity to the security endeavor. Furthermore, the decision to adopt these technologies can take place with little to no input from traditional IT security personnel.

Absence of IoT standards

In traditional markets, one of the primary methods of implementing effective controls is to adopt some form of standardization. Dozens of markets have well-established guidelines, usually spawned from years of learning from the stumbling blocks of development, that help to shape the creation of policies that the entire market abides by. However, the IoT itself is such a nascent technology, it hasn't had the time to evolve into a comparably mature market. As we are collectively still learning to utilize this technology, it can be difficult for security teams to determine what is "acceptable" IoT device behavior. Moreover, the diversity of the devices themselves makes it difficult to universally apply any agreed-upon security policies, such as effective patch management and firmware upgrades. While IoT security legislation has begun to take shape, such as in the UK and California, the security requirements being imposed are quite elementary in nature and lack comprehensive enforcement of chip-to-cloud security measures.

Existing service challenges

Previous misconceptions

“Connect first, secure… if it’s cost effective.” Sadly, many original equipment manufacturers (OEMs) of IoT and OT continue to engage in this insecure practice when designing their respective devices. The reasons for this practice are numerous. Firstly, security can be costly, and many times the fastest way to get a product to market is to skimp on security measures. Secondly, many IoT device manufacturers lack the comprehensive security knowledge necessary to implement data protection solutions into the development process. Additionally, the simplest way to ensure customers can get their devices connected to the internet as quickly as possible is to use the same default credentials for each device manufactured. Unfortunately, for some devices, this default information can’t be changed by the customer. While this might be convenient for the OEM and the end user, it creates a nightmare for IT security teams in the enterprise.

Industry translation

The convenience that IoT device communication has introduced into the global technology ecosystem has managed to infiltrate every market imaginable. Consumers now have access to connected coffee makers, toasters, toothbrushes, refrigerators, and even washing machines. Internet-connected devices have deeply penetrated the transportation market, with several high-profile vehicle compromises taking place as a result of insecure IoT components. The medical field has adopted IoT technology in order to facilitate more accurate diagnosis and patient treatment plans. Industrial manufacturing equipment and critical infrastructure have also implemented IoT technologies as a means of increasing operational efficiency and control, while reducing downtime.

Changing device lifecycles

Additional IoT security challenges are often introduced when these connected devices outlast the manufacturer’s support. Continuing to offer support for legacy equipment can be quite costly for a manufacturer, and as research and development is directed toward more innovative product offerings, support for older components will be discontinued eventually. However, as these devices continue to be used, vulnerabilities are discovered with greater regularity. If the developer has discontinued service on the device, the device remains perpetually vulnerable until it is replaced. Unfortunately, many of the most mission-critical IoT components are often left operating in their environments well beyond their security lifecycle.

IoT-focused solutions

Existing solutions

The challenges that exist within the current landscape of IoT security solutions are quite numerous. The implementation of any IoT security strategy will likely be slow and complex, especially if the organization has never previously attempted to audit its IoT ecosystem. As environmental visibility is the first step in any security offering, this can often require the adoption of new network sensors and added equipment configurations in order to effectively integrate with an organization's existing security infrastructure. Additionally, many device classification solutions use a signature-based approach that requires consistent interaction to maintain accuracy. Furthermore, in the absence of automatically generated security policy recommendations, IoT networked environments can remain vulnerable.

Evolving requirements

As with any technology, the requirements for effective IoT security are in a regular state of flux. Because many IoT devices in use today lack an onboard agent with which to interact, there is growing demand for an agentless approach to IoT security. As a result, such solutions will likely need to rely on machine learning, signature-less approaches for device classification. Moreover, as organizations will need to establish a baseline of normal behavior, they will require automated policy suggestions and comprehensive enforcement strategies. Modern solutions will have to be able to apply context-aware responses to security incidents, such as network segmentation. Lastly, solutions need to be able to integrate seamlessly with an organization's current security investments.

Enhancing operations

Ultimately, the primary benefits surrounding the deployment of any IoT focused solution should grant the Network Security and SOC teams within an organization enhanced operational capabilities. Any adopted IoT security solution should be capable of being seamlessly deployed by both Network Security and SOC groups, without the need to establish an exclusive team specifically dedicated to addressing IoT system security. When properly deployed, IoT focused security solutions should allow Network Security teams to easily discover and monitor unmanaged IoT assets on the network, establish a comprehensive risk assessment, and generate recommended security policies based upon acceptable device behavior to help mitigate any known IoT attacks. To be truly comprehensive, the same IoT focused security solution should also enable the corresponding SOC teams to detect and prevent unknown IoT threats.

The Palo Alto Networks IoT Security solution

One such solution capable of addressing these developing IoT security demands is the Palo Alto Networks IoT Security solution. The cloud-delivered, firewall-attached, subscription-based solution goes beyond providing baseline network traffic visibility by offering comprehensive IoT endpoint device identification and security for any enterprise environment. This solution empowers the enterprise networking security team to take proactive actions to secure their IoT ecosystem. The solution provides seamless integration with an organization's current security posture and security operations center (SOC) processes, while providing automated policy recommendations based on contextualized device behaviors and risk assessments.

Additionally, the Palo Alto Networks IoT Security solution can merge with a customer's current network security infrastructure, regardless of which vendor provided the legacy equipment. This agnostic approach negates the costly requirement for additional monitoring components. The network monitoring solution associated with the NGFW allows for fast and accurate identification of IoT devices in order to effectively distinguish between legitimate new and existing network-connected IoT devices, and those that don't fall under the classification of IoT by sporting the largest number of integrations for asset inventory, logging, and policy enforcement. Moreover, this solution can be deployed in environments that lack traditional firewalls, providing comprehensive IoT protection while removing the need to continuously fill security gaps with single-purpose solutions.

Appendix

Author

Tanner Johnson
Senior Cybersecurity Analyst, Connectivity and IoT
tanner.johnson@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.