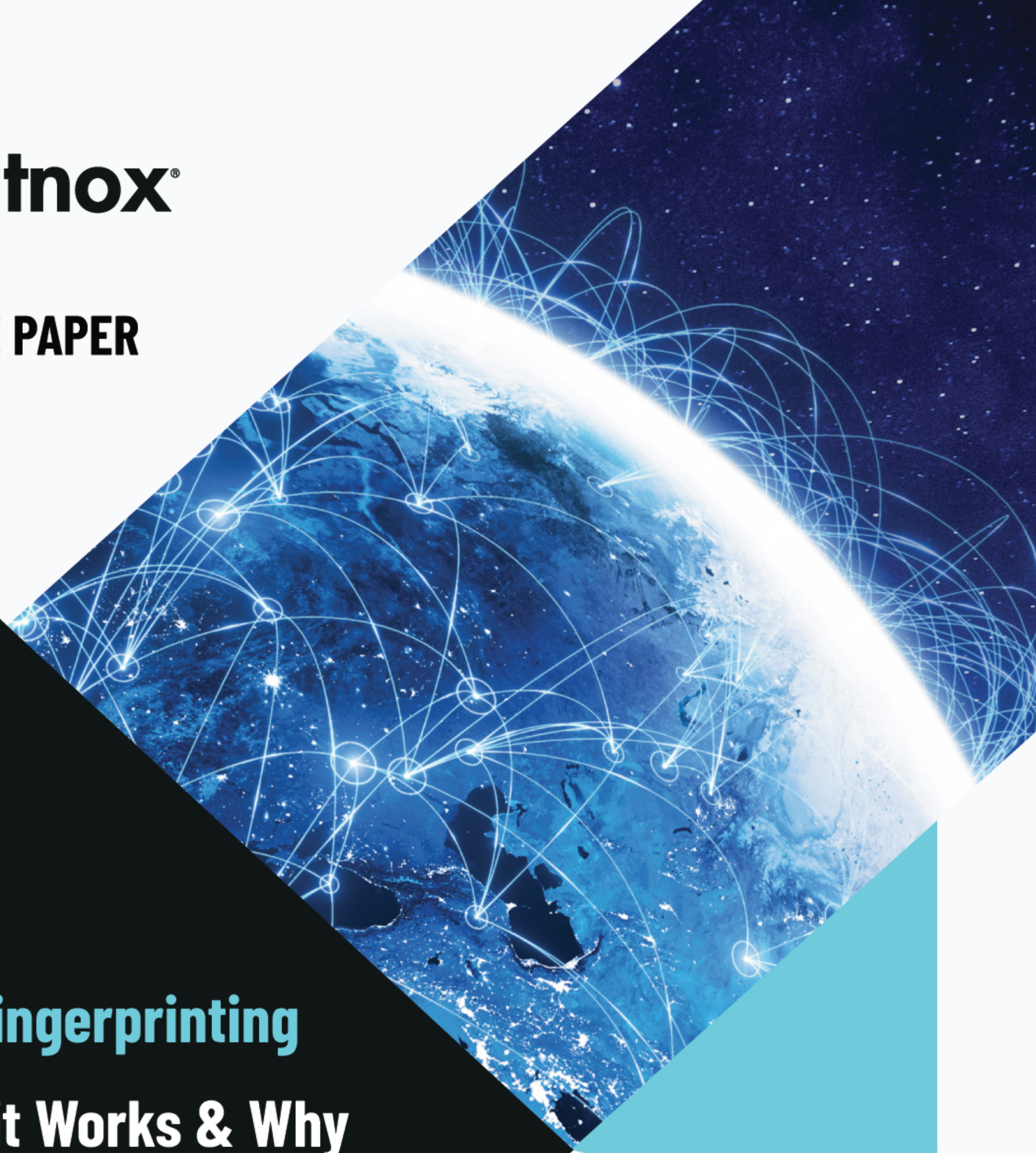
portnox®

WHITE PAPER



IoT Fingerprinting

How it Works & Why it's Eliminating IoT Security Blind Spots

www.portnox.com

Table of Contents

The Rise of IoT

In the early 1980s, long before the internet was a part of our daily lives, a computer science professor at Carnegie Mellon discovered a vending machine that could connect to ARPANET. Tired of finding the machine empty, or the soda warm right after being restocked, the professor and a couple of students wrote a program that would report on the contents of the machine and whether or not the drinks had been there long enough to be cold....and thus, the very first Internet of Things device was born.

An IoT Device Sample Set

ATMs

CCTV

Medical Devices

Robotic Assembly

Printers

Two important developments followed in the history of IoT. First was the proliferation of residential broadband and always-on connections. Once upon a time, having a dedicated phone line for the internet was a luxury; if you were around for the dial-up days you probably remember trying to use the phone only to be met with 56k modem screeches. You would hardly want your fridge to be tying up the phone line! However, by 2010, 65% of all US households had a broadband connection, with that number increasing to 85% by 2018.

The second significant innovation was cloud computing - IoT requires a lot of data storage (all those Ring doorbell videos of possums have to live somewhere) so when Amazon and Google began offering cloud storage services in the mid-2000s, it was possible to store and readily access large amounts of data without having to pay for all the infrastructure of a data center.

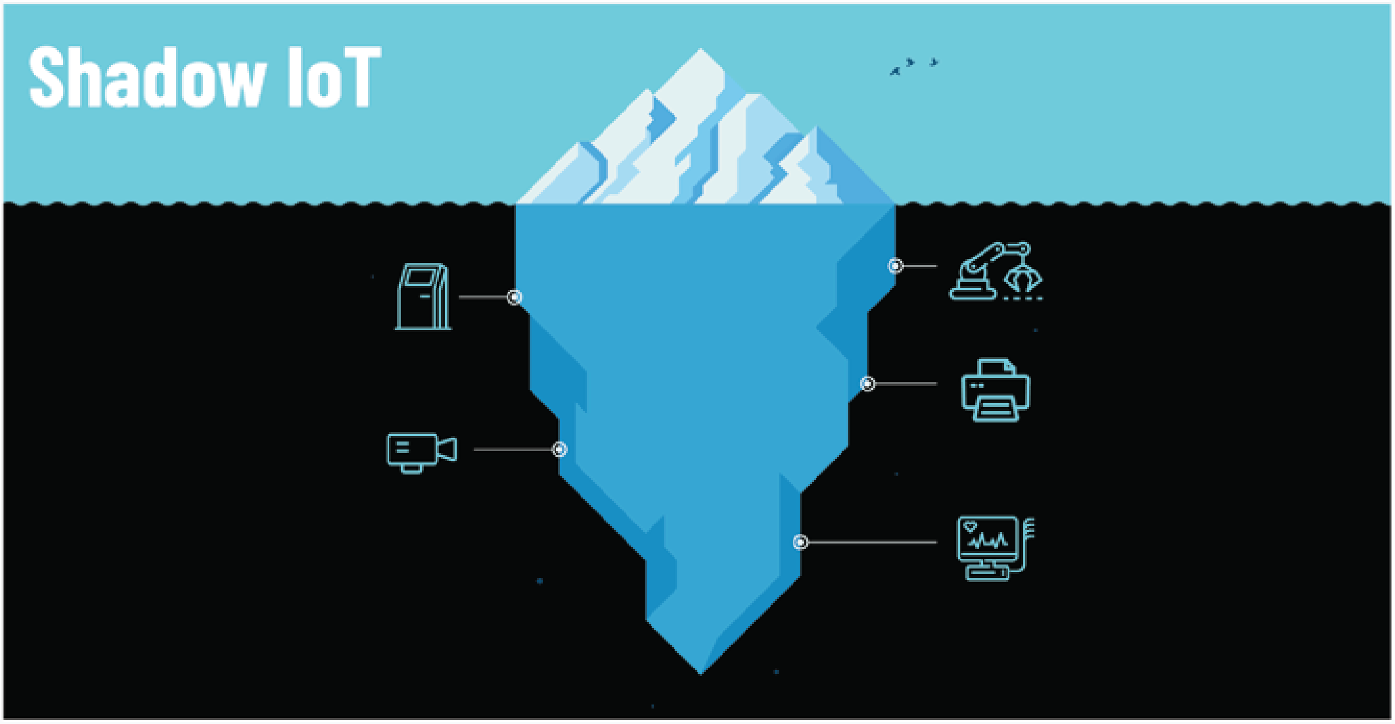
Now that the conditions were right, IoT began to be more widely adopted across many industries. Companies like Walmart, Amazon, and Target widely incorporated IIoT in RFID tagging for inventory, which led to them not only being able to react much faster to changes in consumer needs but also allowed them to collect and store massive amounts of data on the general public's shopping habits. Target famously created an algorithm that allowed them to predict not only when a shopper was pregnant, but roughly when they were due.

The medical industry was another fast adopter of IoT, branching into IoMT (Internet of Medical Things) - smart devices can monitor important statistics like your blood sugar levels for diabetics or the effectiveness of a specific type of inhaler for asthmatics. This allows medications to be adjusted more precisely and quickly. Personal wearable devices are also becoming very common with a variety of medical-related functions - Apple released an ECG feature on the Apple Watch in 2018 and there are many testimonials about people getting early treatment before it became a cardiac event.

And of course, the number of connected consumer devices grows larger every day. Everything in your house can be controlled by Alexa, Siri, or Google, from the temperature, to when the curtains open, or how long you microwave your lunch. And the proliferation continues - by 2025 there will be an estimated 27 billion IoT devices connected to the internet. At this point it's hard to imagine what isn't connected, but undoubtedly there will be new and surprising devices for the smart homes of the future.

Addressing New IoT Security Challenges

IoT (Internet of Things) has brought many beneficial changes to the world. Companies can track inventory in real time, your doctor can get detailed information on your medical conditions, and you can control everything in your house from the thermostat to the curtains with the help of a virtual assistant. Unfortunately, IoT is not without its failings and oftentimes a glaring fault is the lack of proper security measures.



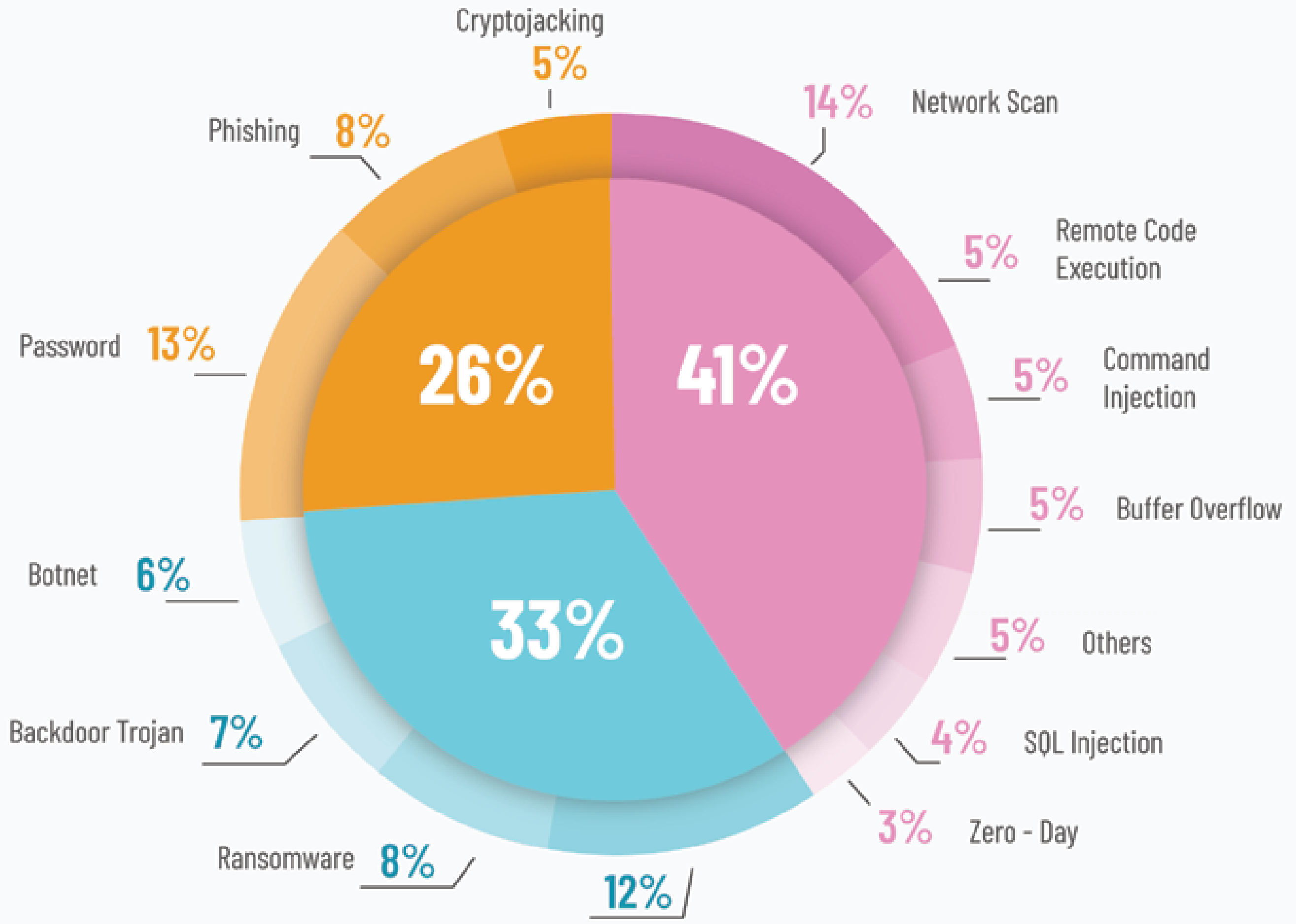
Some of the common issues with IoT security include :

- **Lack of Visibility:** IoT devices are designed to be easy to implement with just an internet connection, which means users can deploy them in a corporate environment without authorization from IT. Consequently, 80% of IT leaders found IoT devices on their networks they were not aware of.

- **Lack of Monitoring:** Typically IoT devices run very lean operating systems and they don't allow for the installation of additional software like monitoring agents, nor do they support traditional monitoring protocols like SNMP and WMI.

- **Poor Testing:** Sadly, IoT manufacturers generally do not prioritize security, so devices are often shipped with exploitable vulnerabilities. They often use APIs that are vulnerable to SQL injections, DDoS (Dedicated Denial of Service), and MITM (Man in the Middle) attacks. A group of hackers famously used a fish tank temperature monitor to breach a Las Vegas Casino in 2017.

- **Lack of Patching:** Upgrading the OS or firmware, if it's even possible, is generally a complicated, inconvenient process - and that's if the manufacturer releases patches. There is generally no option for automatic updates like you would see with a more traditional OS.



Source: 2020 Unit 42 IoT Threat Report

- Know what's out there: Solutions like Portnox's zero trust access platform offer IoT fingerprinting so you can detect and identify the devices on your network. Knowing what is on your network is crucial to keeping it secure.
- Segment: Dedicate specific VLANs to IoT devices and limit their access as much as possible. That way if disaster strikes and a device on your network is breached, you will not be fully exposed.
- Keep Software Updated: Manufacturers may not release security updates as often as we'd like, but it's important to check for updates and keep everything updated as much as possible.
- Change the Password: Make sure to change any default passwords and turn off any features you're not using like API access.

IoT will always present some unique challenges, but with solutions like Portnox's cloud-native zero trust platform and some preparation, it is possible to reap the benefits without increasing your attack surface.

What is IoT Fingerprinting & How Does it Work?

IoT fingerprinting is the active or passive methodologies of identifying IoT devices on a network. The goal is to accurately identify the devices manufacturer and model along with the operating system and operating system version.

Active methods of identifying a device include using protocols like SNMP and HTTP to actively request the device information from the device itself. Passive methods for identifying the device include looking at network traffic the device produces in order to learn this information. This type of data can include data like MAC addresses, DHCP options, and HTTP requests.

By gathering data from the device and then referencing public and private data sources, an IoT fingerprinting service can identify a device based on the output from the various interrogation methods.

Traditional IoT Fingerprinting Limitations

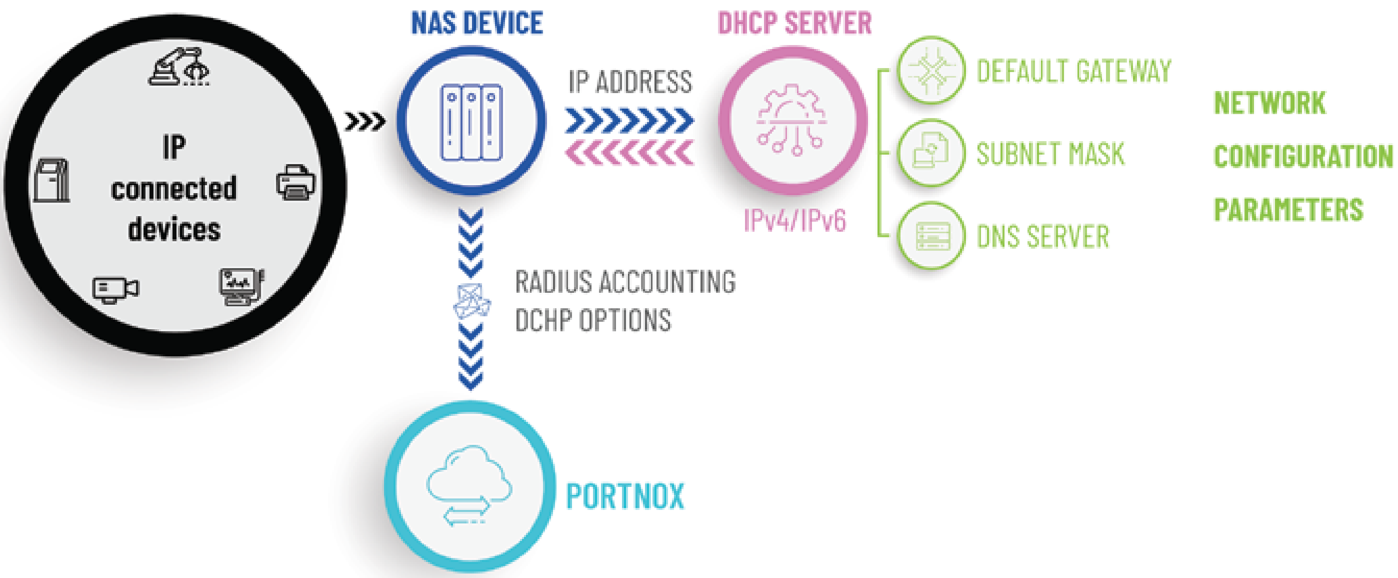
Traditional IoT fingerprinting typically requires an on-premises footprint with a server and database. Then an administrator typically needs to make sure that all the protocols and credentials are configured properly for all of the devices on the network that need to be identified. This is limiting in that the administrator basically needs to know what the device is, or at least what protocols it communicates with prior to being able to perform a fingerprint. On-premises fingerprinting solutions also typically need to perform network scans to look for devices on the network requiring repeated scans to regularly know what is on the network reliably.

More and more, IoT devices don't allow older protocol agents like SNMP to readily gather information about them actively. Instead, these devices simply perform their operations and report their data to a given endpoint. Therefore, it is becoming increasingly difficult to ask a device what it is with older protocols supported by traditional networking tools.

IoT Fingerprinting with Portnox

Portnox's IoT fingerprinting solution requires no on-premises components that don't already exist in the environment today. By utilizing information that is already in RADIUS authentication packets, Portnox can identify devices as they access your network. Since the wireless and wired networking devices already see the network traffic, there is no need to interrogate or discover networking devices.

Network Access Control already provides a way to send the necessary data from the network to our IoT fingerprinting software where we can identify the device and then utilize customizable network access policies to determine what device types belong on what VLANs or other network segments.



What's Next for IoT Security?

As much as we love the convenience of IoT devices, and as essential as they have become across many industries, it's well known that these devices often increase the attack surface of companies that implement them due to less-than-stellar security practices.

As the number of connected devices continues to rapidly expand (an estimated 27 billion will connect by 2027), here's what's next for IoT in the security realm:

- Security Standardization: As more big stories of IoT related hacks become public (like the Mirai Botnet that almost crippled the entire internet), companies will begin prioritizing manufacturers that take security seriously. This will likely lead to some standard practices like regular patches and notifications about serious flaws.

- Increased Regulatory Pressure: California passed SB-327, aka the "Default Password Law", which requires devices that connect to the internet to either implement unique passwords or require them to be changed on first login. There is similar legislation in the UK under the Product Security and Telecommunications Infrastructure bill. Outside of government agencies, industry-specific groups like the International Medical Device Regulators Forum are emphasizing the need for greater security measures amongst all connected devices.

- Emphasis on Certificate-Based Authentication: Compromised credentials are responsible for 80% of data breaches. More and more companies will turn to solutions like a NAC that allow for certificate-based authentication along with 802.1x encryption; this combination requires the device itself to be authenticated rather than just the user.

- Innovative Monitoring: Since traditional monitoring methods like agents and SNMP generally are not supported by IoT devices, companies will look for out-of-the-box solutions like Portnox's zero trust security platform that can detect and identify every IoT device on their networks.

Undoubtedly, these measures will lead to welcome IoT security innovations to keep both our personal and enterprise networks safer.

About Portnox

Portnox offers cloud-native zero trust access control and cybersecurity essentials that enable agile, resource-constrained IT teams to proactively address today's most pressing security challenges: the rapid expansion of enterprise networks, the proliferation of connected device types, the increased sophistication of cyberattacks, and the shift to zero trust. Hundreds of companies have leveraged Portnox's award-winning security products to enforce powerful network access, endpoint risk monitoring and remediation policies to strengthen their organizational security posture. By eliminating the need for any on-premises footprint common among traditional information security systems, Portnox allows companies - no matter their size, geo-distribution, or networking architecture - to deploy, scale, enforce and maintain these critical zero trust security policies with unprecedented ease. Portnox has offices in the U.S. and Israel.

For more information visit www.portnox.com