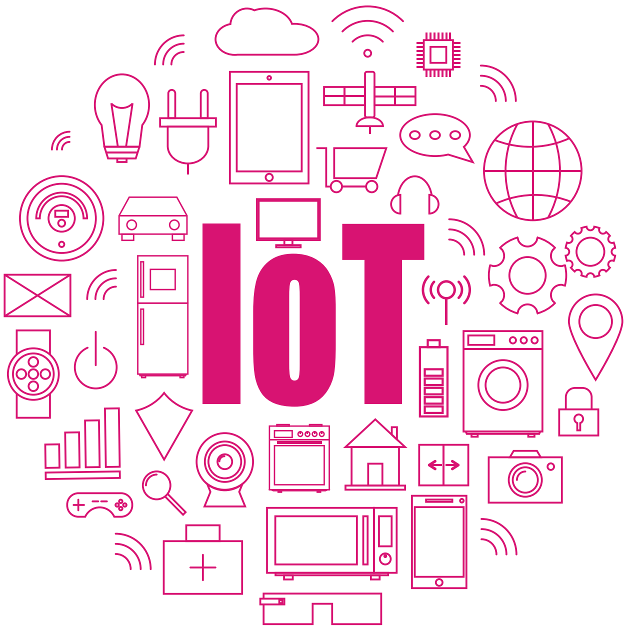
YOU DESERVE THE BEST SECURITY

IS YOUR NAS SECURE?

IOT'S ACHILLES HEEL WITH NETWORK ATTACHED STORAGE DEVICES AND HOW TO BEST PROTECT YOUR BUSINESS



IoT has revolutionized the way we interact with technology and has become an integral part of our lives, both in personal and professional environments. From smart home appliances to wearables and even medical devices, IoT has made our lives easier and more convenient. However, with the increase in the number of IoT devices and advances in technology, security concerns have become a major issue for all. IoT devices are susceptible to various vulnerabilities that can leave them open to attacks by cyber criminals.

> The first two months of 2023 have seen a 41% increase in the average number of weekly attacks per organization targeting IoT devices, compared to 2022.[1]

In this paper, we will explore some of the common security vulnerabilities associated with IoT devices and how you can best keep them protected. Throughout the paper we will continuously refer to a specific scenario where our autonomous IoT security solution, **Quantum IoT Protect**, identified suspicious activity and communication with a network attached storage (NAS) system, properly recognized the activity as malicious behavior, and enforced protection without any hitch in production.

[1] "Ransomware now impacts 1 out of 40 organizations a week," Check Point Research 2023

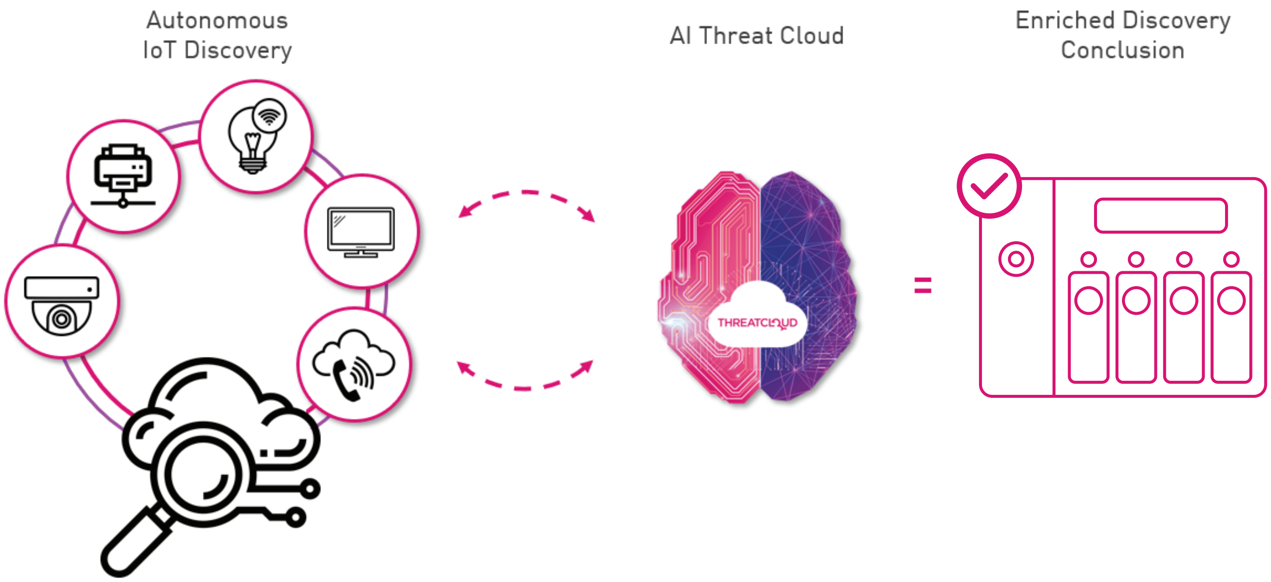
Let’s Talk About NAS Devices Specifically, What Are the Risks?

NAS systems have become increasingly popular in recent years due to their ease of use and ability to store and share large amounts of data quickly. Some NAS providers also have their very own App Stores to provide customers convenience, updates, customization, and more. However, when any device connects to the Internet, there’s an extremely good chance that there exists an open door for attackers to infiltrate.

NAS devices can be used as an entry point for hackers to access the organization's network and other devices connected to it if not properly secured. Once they gain access to the NAS device, hackers can use it to launch further attacks on the organization's network, like spread malware, ransomware attacks, and more. In addition, there is the risk of data breaches, where sensitive data stored on the NAS device is accessed by unauthorized users. This can lead to the theft of personal information, intellectual property, or other sensitive data, causing significant harm to the organization.

So, What Does This Have to Do With Check Point?

Our team of experts at Check Point regularly run tests and analyses to improve product innovations. In this specific case, the team gathered statistics from IoT devices around the world and enriched it with domain reputation data from our Check Point Threat Cloud. The assumption was that we’d be able to identify devices with suspicious behavior/malicious activity. During the analysis, our team encountered a NAS device that was connecting to known malicious domains classified as “scanners.” The accuracy of this discovery as a NAS is extremely important to note here. There is a big difference between a NAS that is attempting to reach suspicious sites (which is very high-risk) versus a laptop that is attempting to reach “suspicious” sites that aren’t always for nefarious reasons. Oftentimes, laptops and other mobile/endpoint devices can be easily mixed with, and labeled, as “NAS devices” (or vice versa) by traditional detection engines, thus missing the suspicious activity altogether. However, Quantum IoT Protect leverages a best-of-breed AI engine to enrich the discovery conclusion – which in this specific case was indeed a NAS device.



Upon further analysis, the team was able to detect that there was a link to a website by the name of "Shodan.io". Shodan is a search engine that scans and indexes internet-connected devices, including IoT devices, and makes the information available for anyone to search. It is important to note that Shodan itself is not malicious or suspicious. However, hackers often leverage the website's search engine to quickly look for specific devices or vulnerabilities that they can exploit for malicious purposes. Shodan provides information about the device's operating system, firmware version, and other technical details that can be used to identify vulnerabilities or weaknesses in the device's security. This information can be used by hackers to develop targeted attacks against specific devices or device types.

The following bullet points are known malwares that leverage Shodan to scan for vulnerable devices on the Internet (just as the NAS in our example became an IoT scanner for the attacker:

- **Mirai:** This malware was responsible for one of the largest DDoS attacks in history, which targeted Dyn DNS in 2016. Mirai scans the internet for IoT devices that use default login credentials and exploits known vulnerabilities to infect them and use them as part of a botnet.
- **Reaper:** Also known as IoTroop, Reaper is a newer botnet malware that is designed to infect IoT devices and use them to launch DDoS attacks. It scans the internet for devices with known vulnerabilities and exploits them to gain control of the device.
- **Hajime:** This malware is similar to Mirai and Reaper but takes a more sophisticated approach. It uses a peer-to-peer (P2P) network to communicate with other infected devices, making it more difficult to detect and shut down. It also patches the vulnerabilities that it exploits, making it harder for other malware to infect the same device.
- **Satori:** This malware targets specific IoT devices, including routers and DVRs, and exploits vulnerabilities in their software to gain control of them. It has been used to launch DDoS attacks and mine cryptocurrency.

What's the Secret to Protecting These Attacks?

There are many IoT security solutions available today, each with its own set of strengths and weaknesses. With so many IoT security solutions available, it can be challenging to determine which one is the best fit for your organization's needs. Some solutions focus on providing basic security features, such as encryption and access control, while others employ more advanced techniques such as machine learning and behavioral analysis to detect and respond to threats in real-time.

Quantum IoT Protect is our offering that provides comprehensive protection against a wide range of cyber threats, including malware, botnets, and DDoS attacks. It enables customers to see all the connected IoT devices in their organization's network and tracks IoT device communications, within the network and externally to the internet. This is accomplished with profiles that are learned from understanding the expected behavior of IoT devices. Based on these profiles, customers are provided with zero-trust access policies that only allow communications needed for normal IoT operations. Other connection attempts that are unnecessary for such a device's purpose can be labeled as suspicious and therefor detected and blocked.

In this rapidly evolving landscape of IoT security, it is critical to stay up-to-date with the latest security trends and technologies to ensure the safety and reliability of your IoT ecosystem. A robust IoT security solution like Quantum IoT Protect can help you achieve this goal and provide you with the peace of mind you need to focus on your core business operations.

For more information on how you can start protecting your organization from cyber threats, head to the Quantum IoT Protect website or evaluate your IoT environment now!

Quantum
IoT Protect

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391
www.checkpoint.com