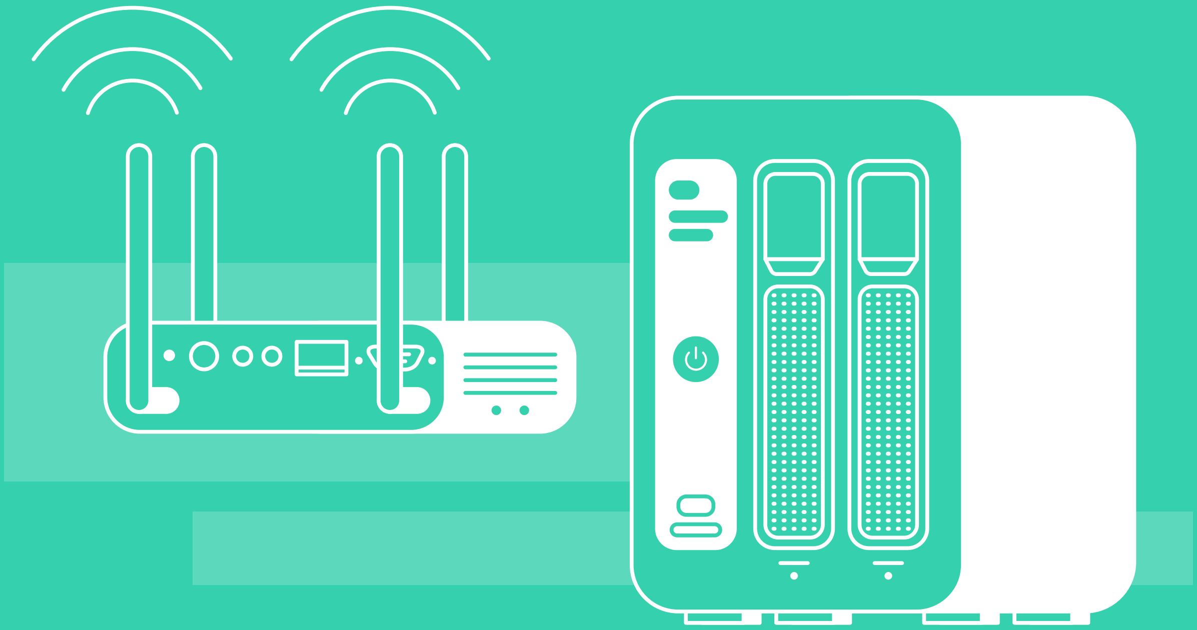
VDOO

IoT Security Platform for Network Devices



Introduction

Network devices such as routers, gateways, and switches are the heart and soul of a network. They hold a dual purpose: securing other devices in the network and managing all network communication. Network devices will continue to be a key component as more and more devices become connected to home and office networks.

Among IoT devices, routers and gateways are extremely attack-prone devices. Such devices have an external IP address, making them susceptible to attacks. Therefore, it's not surprising that routers are one of the most hacked devices in recent years. A study by the American Consumer Institute shows that 83% of routers in the United States are vulnerable to cyber attacks.

Routers were one of most attacked devices in the infamous Mirai attack of 2016. That attack used one of the simplest, yet incredibly efficient, modus operandi: default passwords. Since 2016 there has been an influx of attacks using default passwords, where recent attacks added sophistication to the utilized attack methods. Attacks targeting routers include brute force, command injection, open ports, unsecured web services, and more. In the past three years, attacks against network devices caused major DDoS of key websites, ISPs, and vital internet based services. Owners of the infected devices had higher bills and slow internet access.

In 2018 there were more than 10 different attacks against network devices, among them: OMG Mirai, Omni, UPnProxy, OWARI, SORA, DoubleDoor, JenX, and Pure Masuta. The biggest attack of 2018 was VPNFilter, a botnet attacking mostly routers, which quickly got to the magnitude of Mirai in terms of affected devices, infecting over 500,000 devices. The attack caused the FBI to put out a warning about the attack, as well as offer a mitigation guideline to home users and ultimately locate and shut down the C&C servers.

Infected network devices pose a serious threat to all other IoT devices in the network. Many of the most efficient attacks require some network manipulation or man in the middle ability. Since network devices are so easily attacked, they are a fertile ground to gain an attack vector on other IoT devices, one which has an effect on the user's security and safety.

VDOO's Solutions for Network Devices

By using Vision™, VDOO's analysis solution, device makers can analyze device firmware, regardless of its type or purpose, and receive an accurate description of the device's security status. Vision™ can locate known vulnerabilities or malpractices in the device, such as hardcoded passwords, non-required libraries, and others that are commonly used in attacks such as VPNFilter and other Mirai based malware. The mitigation guidance minimizes the time spent on security, thus allowing a competitive advantage of quickly delivering a secure device to the market. VDOO CertIoT™ provides makers with a competitive edge in a market where differentiation is a challenge. Users can make sure any device installed in the network is certified by VDOO CertIoT™, which proves it has met a rigorous set of security requirements. By using ERA™, VDOO's Embedded Runtime Agent solution, the device maker as well as the organization deploying the network devices can make sure they will remain safe and secure after deployment. Since network devices are the heart of a network, the added security helps the entire network stay secure. ERA™ adds another layer of protection to secure the device against new attacks. Network managers can rely on proactive solutions like Quicksand™, a threat detection honeypot that lures the attacker and provides real-time monitoring and alerts, and Whistler™, a device-specific push alerts system on any new threat. This end-to-end solution was built to handle known or unknown threats to connected devices, to allow laying the foundations for a secured network.