iStatus ArpWatch™

Easily Detect New & Rogue Devices On Your Network

Challenges Of Protecting Your Network From Rogue Devices

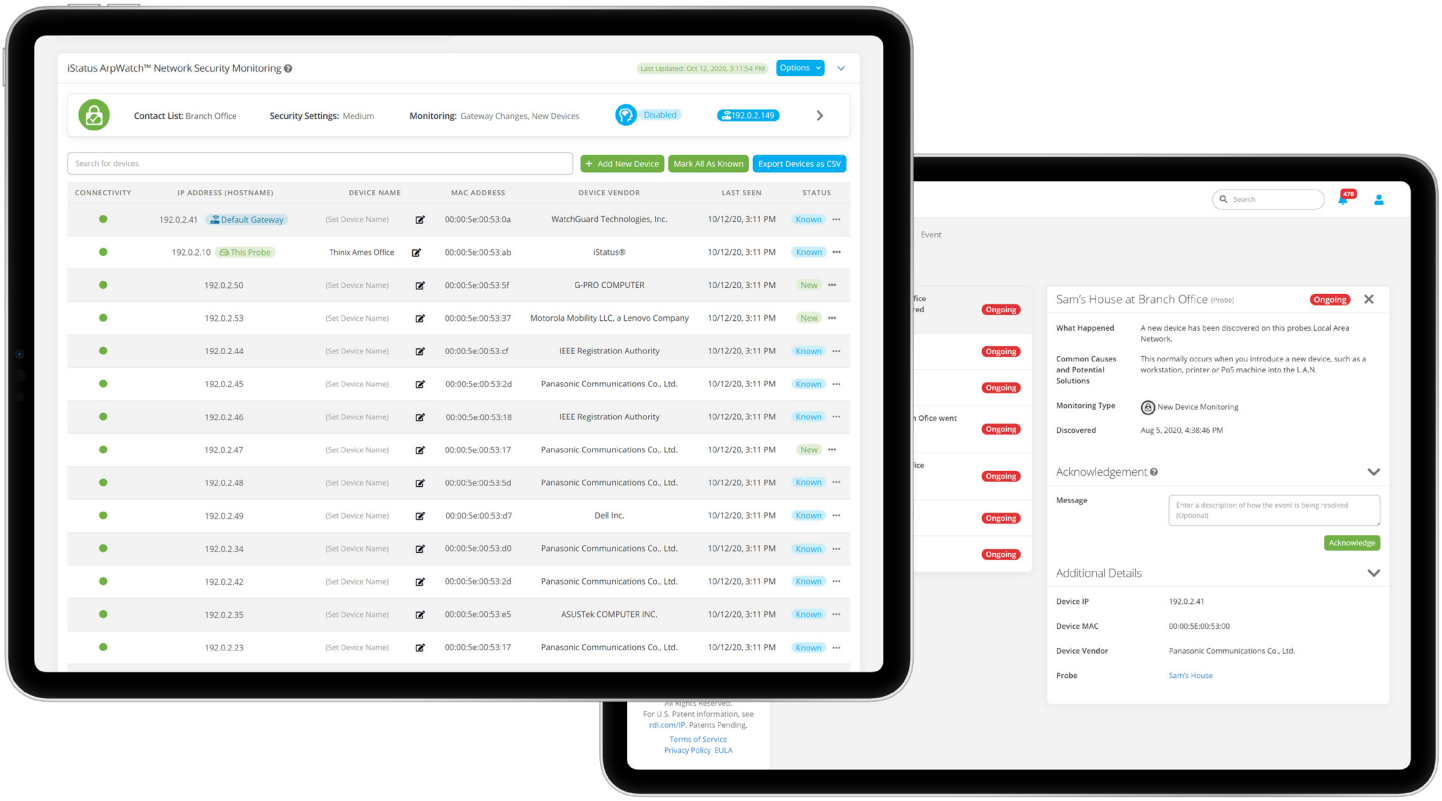
As your company grows and relies on technology and IoT devices even more, your network size increases. Between company devices and employee devices, there are multiple points for cyber threats to enter your network. The number of potential attack points increases with each branch office and Work From Home (WFH) employee your company has. Although you likely have network security in place, it is difficult to notice new devices accessing your company's network. Your security risk is further compounded if you have a large network or one with many segments. With multiple attack points, a rogue or compromised device can easily slip through and connect to your company's network – which can result in data and financial loss.

Existing device detection solutions, such as a Network Access Control (NAC) system or an Intrusion Detection Solution (IDS), on average, require you to have a six-digit budget. In addition to the high cost, these solutions are often difficult to manage over long periods of time. Akative aims to address these limitations head on and deliver critical security technology with ArpWatch.

Enter iStatus ArpWatch™

iStatus ArpWatch is an affordable add-on license to iStatus® that allows our iStatus monitoring probe to detect new devices as they appear on your network. ArpWatch also detects ARP poisoning and man-in-the-middle attacks to offer further insight. Easily monitor all of your network segments (while they remain isolated) without violating network security.

Akative™



How It Works

Once the iStatus monitoring probe is installed and ArpWatch is enabled, ArpWatch begins to proactively monitor for devices that appear on your network. Any devices detected within the defined initial discovery interval (default set at 48 hours) are automatically approved. After this interval, ArpWatch immediately sends an alert to your network administrator when it detects a new device or discovers a known device was altered (such as its IP address was changed). This enables your network administrator to know device activity in real-time and validate it or halt it – protecting your network from unsafe, rogue devices and compromising activity.

Key Features

Proactively monitor, track, & detect endpoints

Add trusted devices before they are physically connected

Generate alerts when unapproved endpoints are added

Mark known/trusted devices

ARP spoofing detection

Monitor default LAN gateway

Sales@Akative.com | Akative.com | (866) 950-3392