

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.



	ontact List: Branch Office Security	Settings: Medium	Monit	oring: Gateway Chang	es, New Devices 😥 Disabled	2 192.0.2.149	>				
Search for devices					+ Add New Device Mark A	All As Known Expor	t Devices as CSV				
CONNECTIVITY	IP ADDRESS (HOSTNAME)	DEVICE NAME		MAC ADDRESS	DEVICE VENDOR	LAST SEEN	STATUS				Q Search
•	192.0.2.41 Contact Content Content of Conten	(Set Device Name)	Ľ	00:00:5e:00:53:0a	WatchGuard Technologies, Inc.	10/12/20, 3:11 PM	Known ···	Event			
•	192.0.2.10 (This Probe	Thinix Ames Office	ß	00:00:5e:00:53:ab	iStatus®	10/12/20, 3:11 PM	Known	Lven			
•	192.0.2.50	(Set Device Name)	ß	00:00:5e:00:53:5f	G-PRO COMPUTER	10/12/20, 3:11 PM	(New)				
•	192.0.2.53	(Set Device Name)	ß	00:00:5e:00:53:37	Motorola Mobility LLC, a Lenovo Company	10/12/20, 3:11 PM	New ···	fice red	Ongoing	Sam's House at What Happened	Branch Office (Probe) Ongoing A new device has been discovered on this probes Local Are
•	192.0.2.44	(Set Device Name)	ß	00:00:5e:00:53:cf	IEEE Registration Authority	10/12/20, 3:11 PM	Known		Ongoing	Common Causes	A new device has been discovered on this probes Local Are Network. This normally occurs when you introduce a new device, suc
•	192.0.2.45	(Set Device Name)	ß	00:00:5e:00:53:2d	Panasonic Communications Co., Ltd.	10/12/20, 3:11 PM	Known		Ongoing	and Potential Solutions	workstation, printer or PoS machine into the L.A.N.
•	192.0.2.46	(Set Device Name)	ß	00:00:5e:00:53:18	IEEE Registration Authority	10/12/20, 3:11 PM	Known	h Ofice went	_	Monitoring Type	(B) New Device Monitoring
•	192.0.2.47	(Set Device Name)	ß	00:00:5e:00:53:17	Panasonic Communications Co., Ltd.	10/12/20, 3:11 PM	New		Ongoing	Discovered	Aug 5, 2020, 4:38:46 PM
•	192.0.2.48	(Set Device Name)	ß	00:00:5e:00:53:5d	Panasonic Communications Co., Ltd.	10/12/20, 3:11 PM	Known	lice	Ongoing	Acknowledgeme	ent 🛛
•	192.0.2.49	(Set Device Name)	ß	00:00:5e:00:53:d7	Dell Inc.	10/12/20, 3:11 PM	Known ····		Ongoing	Message	Enter a description of how the event is being resolver (Optional)
•	192.0.2.34	(Set Device Name)	ß	00:00:5e:00:53:d0	Panasonic Communications Co., Ltd.	10/12/20, 3:11 PM	Known ···		Ongoing		Ackr
	192.0.2.42	(Set Device Name)	ß	00:00:5e:00:53:2d	Panasonic Communications Co., Ltd.	10/12/20, 3:11 PM	Known		Chigoing	Additional Detai	ls
	192.0.2.35	(Set Device Name)	ß	00:00:5e:00:53:e5	ASUSTek COMPUTER INC.	10/12/20, 3:11 PM	Known			Device IP	192.0.2.41
	192.0.2.23	(Set Device Name)	8	00:00:5e:00:53:17	Panasonic Communications Co., Ltd.	10/12/20, 3:11 PM				Device MAC	00:00:5E:00:53:00
-	132.0.2.2.3	(Set Dence Name)		00.00.36.00.33.17	ranasone communications co., etc.	10/12/20, 3.1111	(KIIOWI)			Device Vendor Probe	Panasonic Communications Co., Ltd. Sam's House

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

