CHECKLIST

5 Key IoT Capabilities to Look for in a Networking Solution

Organizations are increasingly relying on Internet-of-Things (IoT) devices to achieve business goals. Unfortunately, these devices are inherently insecure and often targeted by cybercriminals to gain entry into the network and launch attacks. As IoT devices become more important and pervasive, they must be secured.

To get the most benefit from IoT devices while minimizing their risks, you need to ensure your networking equipment has the following capabilities:

☑ **Visibility and Device Details**

You need to know more than the number and type of devices on your network. Look for solutions that can provide complete information about the manufacturer, the firmware, and known vulnerabilities for each device. This is critical to maintaining a well-functioning network.

☑ **Easy IoT Onboarding**

Joining the network may be easy for users but is often challenging for headless IoT devices. Without a user behind a device making network choices or logging in, it can be difficult for the network to place these devices in the correct security posture. Often, this is solved by network access control software that can recognize devices as they attach and configure network security settings accordingly.

☑ **Protection**

Protecting IoT devices can be problematic. IoT devices are often embedded in the network in a way that makes immediate software updates to get the latest security patches problematic. But, leaving a known vulnerability in the network is very risky. Technologies such as virtual patching can implement compensating controls over the top of devices with known vulnerabilities.

☑ **Quarantine**

Ideally, the onboarding and protection methods mentioned above will be able to keep a device from being compromised, but it's not always enough. Your solution should be able to quarantine a device into a walled garden if it becomes infected.

☑ **Automation**

With so many IoT devices in today's networks, it's crucial to automate onboarding, protection, and quarantine capabilities to reduce overhead for the IT group.

IoT devices will only continue to grow their footprint in modern networks. To mitigate the risk, any network solution must include full visibility, onboarding, protection, quarantine, and automation capabilities. IT groups can avoid being overwhelmed by IoT by deploying secure networking equipment capable of these features. Learn more about the Fortinet LAN Edge solution.

June 27, 2024 3:10 PM / 2757363-0-0-EN