SOLUTION BRIEF

Fortinet and Intel® Secure Device Onboard Security Solution

Establishing Trust to Enable Secure IoT Endpoint Onboarding

Internet-of-Things (IoT) devices can deliver great efficiencies, insight, and control when deployed into networks, but they can also create headaches for the security team. Frequently headless, these devices are often connected to networks without full identification or validation of their function. Security teams are forced to guess or make assumptions about devices and what network access they should receive. In short, security teams need a way to know which devices they can trust and which devices they need to keep a close eye on.

Intel and Fortinet recently established a technology partnership to address the above challenge by combining an automated onboarding service with network access control solutions that can dynamically configure edge security policies for IoT.

Joint Solution Description (Steps to Complete Implementation)

The Intel® Secure Device Onboard (Intel® SDO) service and the Fortinet FortiNAC SDO onboarding solution address the issue of onboarding trust by providing a means of validating the device identity and then using that information to determine the level of network trust.

With the Intel® SDO solution, devices using the Intel® SDO process are able to provide validation to the network. On the manufacturing line, a device's hardware root of trust (Intel or ARM-based) is imaged with software and credentials to enable authentication and onboarding with the Intel SDO service. The devices can be built using Intel or ARM-based processors and do need preregistration with Intel's SDO service. As the device changes ownership in the supply chain, a credential tool is used to prove ownership and preregister with the device's management system. Networks that are deploying these SDO-based devices can then use a FortiNAC to deliver the appropriate level of trust and security to those devices.

When a device connects to the network, FortiNAC can profile the device and initially place it in a low-security or internet-only segment of the network. The device can then call home to its vendor cloud, which will then verify to the Intel® SDO service. With that verification information, the FortiNAC can elevate the device to a trusted segment of the network, configuring the switches, access points, and firewalls appropriately.

This cloud-based verification is tied to the hardware security of the device and is automated by the enablement for Intel® SDO through the manufacturing process. The result is a more secure deployment of IoT devices that can scale using automated processes without involving high cost.

Joint Solution Benefits

- Fast and secure onboarding of IoT endpoints
- Ability to assert to trust posture of the endpoint
- Ability to use trust posture to define granular network access policies
- Zero-touch onboarding experience with automated security

FORTINET FABRIC-READY

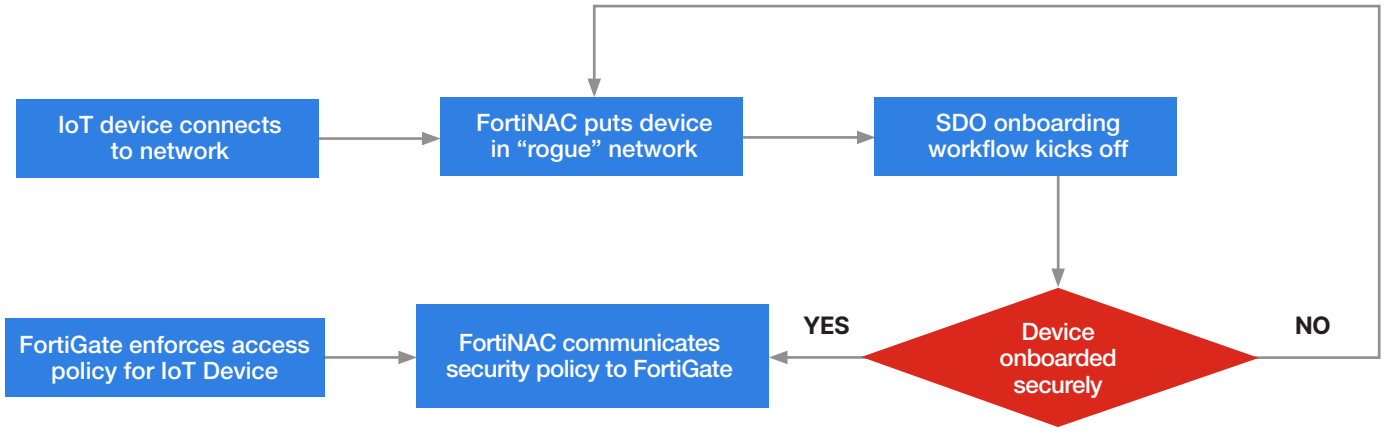

Figure 1: Secure Device Onboarding workflow with Intel SDO and FortiNAC—extending IoT security to the network perimeter.

Joint Use Cases

- Securely onboard IoT endpoints to the network
- Use secure onboarding information to define granular security policies on the FortiNAC for the IoT endpoints.

Fortinet FortiNAC

FortiNAC is Fortinet’s network access control solution that enhances the Security Fabric with visibility, control, and automated response for everything that connects to the network. FortiNAC provides protection against IoT threats, extends control to third-party devices, and orchestrates automatic responses to a wide range of networking events.

Solution Components

- Fortinet Security Fabric: FortiGate, FortiNAC
- Intel® Secure Device Onboard (Intel® SDO)

Intel® SDO

A service that enables a device to be powered on to dynamically provision to a customer’s IoT platform of choice in seconds—with a zero-touch, automated process secured by the device’s hardware root of trust.

About Intel

At Intel, building a better world is our business. Our mission is to utilize the power of Moore’s Law to bring smart, connected devices to every person on earth while serving as a role model for how companies should operate. We power amazing experiences through a diverse product line and exciting partnerships. Our strategy is a virtuous cycle of innovation—the cloud and the data center, the Internet of Things, memory and FPGAs all bound together by the goal of greater connectivity and enhanced performance. Our global team, over 107,000 strong across 58 countries, is a powerhouse of engineering and technological excellence that empowers solutions to the world’s toughest problems while creating the technology of tomorrow. We are Intel, and Amazing Works Here.

FORTINET

www.fortinet.com

June 8, 2021 9:42 AM

sb-fortinet-and-intel-security-device-onboard-solution-1071054

648821-A-0-EN