Infoblox
NEXT-LEVEL NETWORKING

Shadow IoT A New Threat Portal

A Threat to Network Security

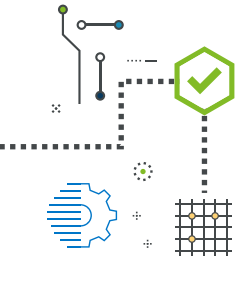
As enterprises evolve to include more remote locations and companies incorporate BYOD devices, Shadow IoT devices will present an ever-growing risk to network security and reliability.

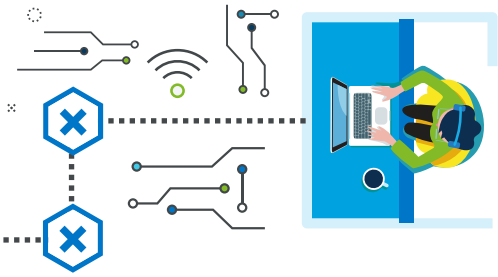
What is Shadow IoT?

Shadow IoT Devices are connected devices or sensors that are in active use within an organization's network without IT's knowledge—they include everything from personal computers and phones to personal health monitors and other "smart" devices.

How Big is the Threat?

80% of IT managers have found Shadow IoT devices on their networks





Shadow IoT Devices Pose a Real Threat to Network Security

Shadow IoT Devices can open enterprise networks to significant risk of malware and other cyberattacks

Early 2019

Large scale bot-net using more than 400,000 connected devices attacked an online streaming application for 13 days, producing almost 300,000 requests per minute.

April 2019

The STRONTIUM group—tied to GRU, the Russian intelligence agency—targets IoT connected devices—including a printer, VoIP phone, and video decoder—to gain access to corporate networks.

Awareness Has Grown

89%

of organizations **have security policies in place** for personal IoT devices, but is it enough?

So, What Can Be Done?

Implement robust security policies
for personal IoT devices

Gain full visibility
into which devices are connected to the network with services like BloxOne DDI

Use intelligent systems
to detect anomalous and potentially malicious communications to and from the network—like BloxOne Threat Defense