Enterprise IoT security that knows about the devices connecting to your network.

IBM Security

Gain visibility into IoT and unmanaged devices in your enterprise – on or off your network, and in your airspace.

IBM Security X-Force Threat Management for IoT

We don't just tell you what a device is, but what it is doing. We continuously track its behavior, its connections, and can identify if it is acting suspiciously or maliciously.

Machine Learning is used to learn about devices and monitor their behavior at enterprise scale. The IBM Security X-Force Threat Management for IoT threat management service helps eliminate the IoT security blind spot as you adopt connected devices to drive business innovation.

Get started today

Find out more about the benefits of fully managed IoT Threat Management service.
Download the Solution Brief at:
ibm.biz/XF-IoT-SolutionBrief

Contact IBM Security Services at:
ibm.biz/XF-IoT-Demo.

IBM

Six reasons CISOs are choosing IBM Security X-Force Threat Management for IoT for unmanaged and IoT device security

1 Device discovery & classification

Visibility into what is connecting to the network and where. IBM Security X-Force Threat Management for IoT discovers devices in your environment—managed AND unmanaged IoT devices, both on and off your network as well as in your airspace. We discover what is there, and what it is doing—what software it is running and how it is communicating.

2 Integrated threat intelligence

Clarity regarding the risks and vulnerabilities of each device. IBM Security X-Force Threat Management for IoT also discovers the risks and vulnerabilities associated with devices based on intelligence from external threat feeds, vulnerability databases, RSS feeds, and internal threat research and assigns a risk score to each device.

3 Continuous behavioral analysis

Continuous, real-time monitoring to quickly detect and respond to threats stemming from your IoT devices. IBM Security X-Force Threat Management for IoT continuously analyzes the behavior of devices in your environment and uses machine learning to identify if a device has deviated from the norm. The service has amassed a vast knowledgebase of over 10 million distinct device profiles. It's a large "crowd-sourced" knowledgebase, that is continuously learning from the devices in our customers' environments. This allows us to detect threats with a high degree of accuracy.

4 Agentless & passive

Addressing insufficient tools for monitoring unmanaged and IoT devices due to inability to accept a traditional security agent and / or concerns of causing equipment to go down. IBM Security X-Force Threat Management for IoT does not require agents or hardware, which makes it easy and rapid to deploy. It also means that it works with IoT devices that can't accommodate agents. Typically, 40% of all devices in an enterprise cannot accommodate an agent, and that number is only expected to grow substantially.[1] The service uses a virtual appliance called a "Collector" that sits on your network, out of band. We integrate with your Wireless LAN Controller (WLC), switches and other network infrastructure. Through these connections, we glean information from your network (100% passive monitoring). Our virtual appliance examines the packets, strips out all the data payloads, and sends the metadata to our cloud-based analysis engine. When our cloud-based analysis engine determines that there is an elevated risk or attack on your network, or a policy violation, it generates a security alert for triage and response.

5 See wired and wireless traffic

Addressing risks from devices networked via WiFi or Bluetooth which can lead to over-the-air attacks, or accidentally connecting to unsanctioned devices and networks, creating a so-called "shadow network." IBM Security X-Force Threat Management for IoT connects to your wired network via a SPAN port. It also connects to your WLC via a standard user account. We use your existing wireless infrastructure to tell us everything we need to know about devices on or off your network, in your airspace, including Bluetooth devices and other IoT wireless protocols that you currently have no way to monitor, making sure that you have visibility into devices on all networks.

6 Delivered as a managed service

You need a trusted security partner. IBM Security X-Force Threat Management for IoT is delivered as a managed service by dedicated security analysts with specialized IoT security expertise. Our in-house threat analysts will monitor, detect, and triage alerts from your environment for rapid detection and response of IoT related security incidents, helping you to protect your critical business information.

[1] Armis, https://go.armis.com/hubfs/Why%20Armis.pdf