IBM Security
Solution Brief

X-Force Threat Management for IoT

Agentless threat management for unmanaged and IoT devices

Highlights

- The unmanaged and IoT device security gap for enterprises
- Automatically discover managed, unmanaged, and IoT devices
- Detect threats by continuously and passively monitoring the devices
- Integrate with existing networking and security solutions

The Unmanaged and IoT Device Security Gap for Enterprises

Gartner estimates there will be 25 billion IoT devices in use by 2021.[1] And by then, up to 90% of devices will be unmanaged and unprotected.[2] Moreover, 84% of security professionals believe that unmanaged and IoT devices are more vulnerable to cyberattacks than corporate-managed computers, according to a recent Forrester-commissioned report "The State of Enterprise IoT Security."[3]

While this explosion of unmanaged and IoT devices in the workplace is driven by business needs for increased productivity and data insights, it has created a significant challenge for organizations as these devices have little to no security, can't host an agent, and are difficult or impossible to update. In many cases, there's no effective way to fully identify or manage these devices, as traditional security solutions such as firewalls, network security and endpoint detection and response are not adequate to discover and protect these types of connected devices.

Introducing IBM Security X-Force Threat Management for IoT

IBM Security X-Force Threat Management for IoT provides the agentless device security platform for enterprises to address the new threat landscape of unmanaged and IoT devices. It is a passive yet comprehensive threat management platform which provides complete asset discovery and classification, behavioral tracking, continuous threat assessment and response across all industries.

From traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial control systems, medical devices and more, X-Force Threat Management for IoT can discover, analyze, and secure them all.

A cloud-based managed and agentless service, X-Force Threat Management for IoT helps enterprises identify devices, analyze attacks and malicious behavior, and take action to protect unmanaged and IoT devices without disruption to your business.

Identify and Classify

X-Force Threat Management for IoT automatically discovers managed, unmanaged, and IoT devices in your environment on or off the network. Our threat management platform monitors wired and wireless traffic on your network and in your airspace to identify every device and to understand each device's behavior without disruption. Our agentless, passive solution identifies device type, manufacturer, model, serial number, location, username, operating system, installed applications, and tracks connections over time.

In addition to discovering and classifying a device, X-Force Threat Management for IoT calculates a risk score based on factors like vulnerabilities, known attack patterns, and the behaviors observed of each device on your network. This risk score helps your security team assess your attack surface and meet compliance with regulatory frameworks that require identification and prioritization of vulnerabilities.

This visibility and inventory can help fulfill critical security controls for frameworks like, PCI-DSS, HIPAA, the NIST Framework, or the CIS Critical Security Controls.

Detect Threats - Manage and Contain

X-Force Threat Management for IoT goes beyond device and risk identification. It can detect threats by continuously and passively monitoring the devices within the environment and detects behavioral anomalies in real-time. If a threat is exposed, X-Force Threat Management for IoT will alert your security team and send an automated action to stop an attack.

X-Force Threat Management for IoT is able to identify suspicious and malicious device behavior because it leverages the largest device knowledge base available. It is a giant, crowd-sourced, cloud-based device behavior knowledgebase—the largest in the world. It tracks over 110 million devices broken out into 10 million distinct device profiles. Through AI and machine learning, it classifies devices and detects threats with a high degree of accuracy. It compares real-time device state and behavior to "known-good" baselines of similar devices seen in other environments. When a device operates outside of its baseline, X-Force Threat Management for IoT can issue an alert or it can automatically take action and disconnect or quarantine a device. Alerts can be triggered by a misconfiguration, a policy violation, or abnormal behavior like inappropriate connection requests or unexpected software running on a device.

Integrated and Powerful

X-Force Threat Management for IoT can integrate with existing networking and security solutions, such as firewalls, network access controls, SIEMs, or IBM Managed Security Services to restrict access or quarantine suspicious or malicious devices.

Also, a simple, cost-effective deployment is combined with the ease of on-going management as a cloud-delivered managed service.

With IBM Managed Security Services, the IoT devices discovered on your network are monitored and managed 24x7x365. Our global team of threat analysts and responders can leverage the information from X-Force Threat Management for IoT discovery combined with world-class threat intelligence feeds to provide highly accurate detection and containment within your environment.

[1] https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends

[2] https://www.armis.com/resources/iot-security-blog/growth-of-un-agentable-devices-in-the-enterprise/

[3] https://www.armis.com/resources/iot-security-blog/forrester-state-of-enterprise-iot-security-in-north-america-unmanaged-and-unsecured/

Why IBM?

IBM Security Services professionals can offer virtually unparalleled IoT security expertise, broadened by their access to IBM’s research and development team. Available worldwide, IBM experts can tailor their recommendations to your industry and your region’s unique circumstances. IBM's approach to managed services examines impact at every level of your organization—from business strategy to applications to infrastructure—to help you address each step of your security journey, aligned to your future business and security goals.

Next steps

→ Schedule a Demo of X-Force Threat Management for IoT

→ Visit IBM Managed Security Services

For more information

To learn more about the IBM Security X-Force Threat Management for IoT, please contact your IBM representative or reach out to us for a demo: http://ibm.biz/XF-IoT-Demo

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.