SOLUTION OVERVIEW

Tenable for IBM MaaS360®

Reduce Cyber Risk with Mobile Device Management

IBM Security

Business Challenge

Security teams are constantly challenged with the ability to monitor their changing fleet of mobile devices and associated vulnerabilities for the organization. Without integrating the Tenable plugin with IBM MaaS360®, scanning and gaining additional vulnerability data becomes increasingly complex. If devices are unaccounted for or fail to have the correct policies, personal and enterprise data is at major risk.

Solution

The Tenable® plugin for IBM MaaS360® provides a way for security teams to understand the cyber exposure of their mobile devices being managed by IBM. Tenable collects mobile device hardware and software information by importing asset lists and asset data from IBM MaaS360® and runs its plugins against the collected data to determine vulnerabilities. Comprehensive reports are then generated for security teams to better understand their Cyber risk to help ensure compliance across their mobile environment.

Value

The Tenable plugin for IBM MaaS360® provides the ability to:

- Gather all known information for your organizations iOS and Android devices
- Receive vulnerability information for your organizations mobile devices
- Report on vulnerability findings within Tenable for your organizations mobile devices

Technology Components

- Tenable.io/Tenable.sc
- IBM MaaS360®

ABOUT TENABLE

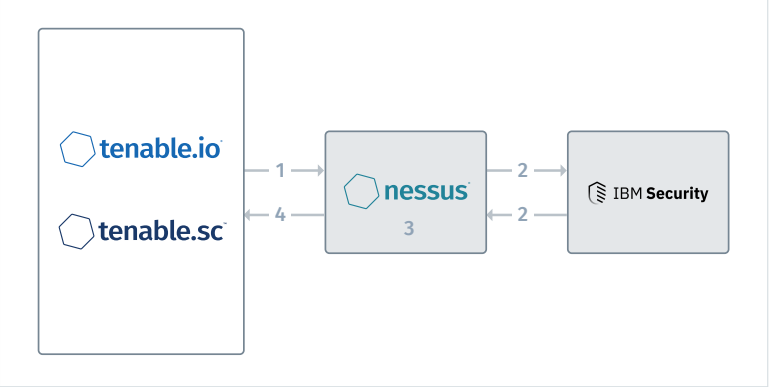
Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at **www.tenable.com**.

ABOUT IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 70 billion security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. Learn more at **ibm.com/security**

How It Works

1. Tenable launches Mobile Device Management Scan process.
2. Nessus® connects to IBM MaaS360® and gathers all known information about Android and iOS devices.
3. Nessus® uses the data collected from IBM MaaS360® to discover vulnerabilities.
4. Findings are returned to and reported within Tenable.



More Information

Tenable Installation Links:
https://www.tenable.com/products/tenable-io
https://www.tenable.com/products/tenable-sc

Configuration Documentation:
docs.tenable.com

For support please contact: **support@tenable.com**