SOLUTION OVERVIEW

Tenable for MobileIron UEM

Reduce Cyber Risk with Mobile Device Management

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 MobileIron Unified Endpoint Manager (UEM), scanning and gaining additional vulnerability data becomes increasingly complex and 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 MobileIron UEM provides a way for security teams to understand the cyber exposure of their mobile devices being managed by MobileIron. Tenable collects mobile device hardware and software information by importing asset lists and asset data from MobileIron UEM and runs its plugins against the collected data to determine vulnerabilities. Comprehensive reports are then generated for security teams to better understand their Cyber Exposure and risk and help ensure compliance across their mobile environment.

Value

The Tenable plugin for MobileIron UEM 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
- Run policy audits for iOS and Android Devices

Technology Components

- Tenable.io/Tenable.sc 5.11 or higher
- MobileIron UEM

ABOUT TENABLE

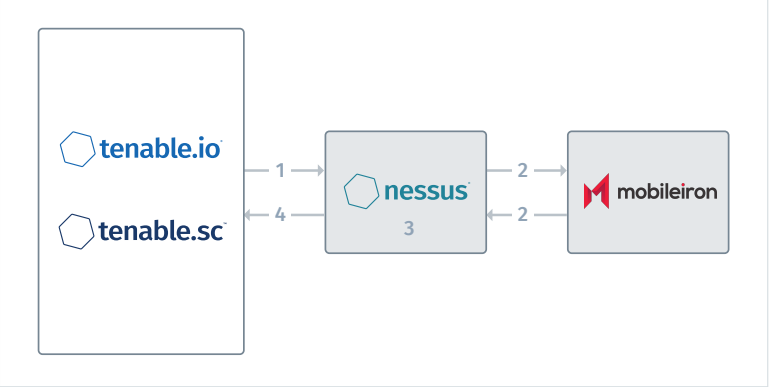
Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing 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 MOBILEIRON

Since 2007, MobileIron has been the leader in mobile enterprise security. MobileIron is software that companies use to secure and manage business apps, documents, and other business content on mobile phones and tablets. MobileIron software includes an administration console for the IT department and an app that employees download onto their devices from the app store or Google Play. IT uses the MobileIron console to set security and management rules. The MobileIron app provides the IT department with information about the device and its security state. This includes things like carrier, country, device make and model, operating system (OS) version, phone number, and corporate email. Learn more at **Mobileiron.com**

How It Works

1. Tenable launches Mobile Device Management Scan process.
2. Nessus® connects to MobileIron UEM and gathers all known information about Android and iOS devices
3. Nessus® uses the data collected from MobileIron UEM 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**