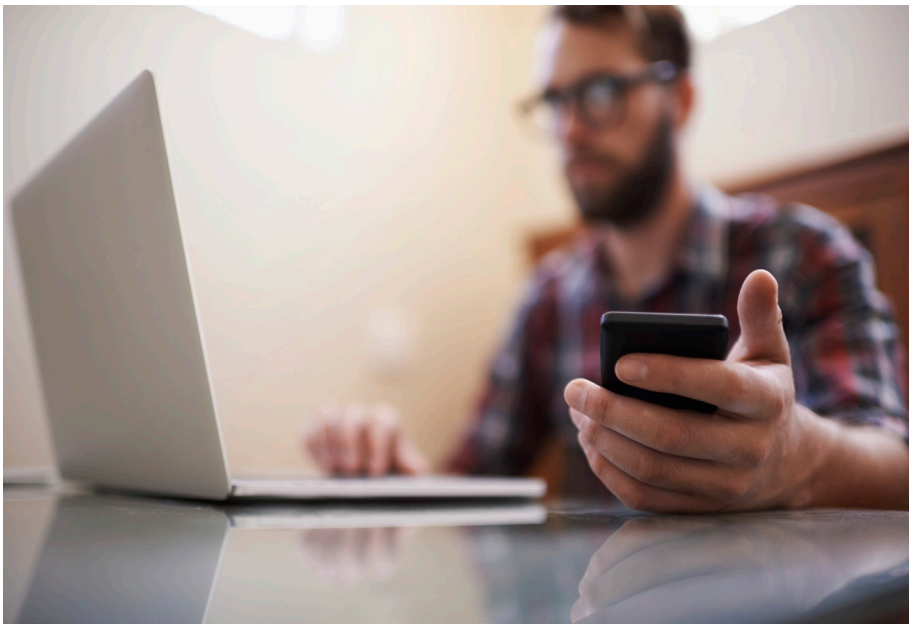
IBM **MaaS360**

IBM Security QRadar Integration with IBM MaaS360

Continuous visibility into mobile threats and events



Keep external and internal mobile threats on the radar

System administrators know that keeping workers productive while preserving enterprise data security is critical, and to do it they'll need a regularly updated, centralized view of devices and applications interfacing with the corporate network.

Today's workers look to smartphones and tablets as a preferred way to remain productive on the go. Coupled with this trend is IT's critical need to maintain constant visibility of the threats from mobile devices and apps. Without a means to monitor these threats alongside the other components interfacing with the network, IT cannot execute the textbook threat assessment and response processes needed to uphold network security and maintain regulatory compliance.

IBM® Security QRadar® and IBM MaaS360® have answered the call of enterprise CIOs and CSOs with a pre-integrated and tested solution that displays information about relevant mobile threats and compliance rule violations moments after they've occurred from a single pane of glass. Administrators can receive actionable intelligence and take informed steps to respond with speed and efficiency.

IBM MaaS360 is the first EMM App on the IBM Secure App Exchange

ConRes 50 YEARS IT SOLUTIONS

QRadar | IBM MaaS360

The QRadar / MaaS360 integration provides system administrators actionable intelligence of mobile threats and events, highlighting activities that could pose a risk to corporate assets and information.

Key benefits

- End-to-end risk protection and analysis within the QRadar dashboard
- Ongoing mobile event detection
- Access to detailed, customizable reports on events and user activity
- Option to drill down to individual events to evaluate the severity of threats

Continuous mobile visibility

- Detect when smartphones and tablets are attempting to connect to the network
- Monitor enrollment of personally owned and corporate-liable devices
- Gain awareness of unauthorized devices
- Learn when users install blacklisted apps and access restricted websites

Compromised device remediation

- Identify jailbroken iOS devices and rooted Android devices
- Uncover devices infected with malware before they compromise your enterprise data
- Set security policies and compliance rules to automate remediation
- Block access, or perform a selective wipe or full wipe of compromised devices

IBM MaaS360

QRadar® / MaaS360® Integration

Simple, yet powerful, addition to QRadar

Each time a mobile user attempts to connect to the corporate network, there is a risk that the device is jailbroken (iOS), rooted (Android), running on an outdated OS version, or infected by malware.

The integration between QRadar and MaaS360 empowers system administrators to monitor events—such as device enrollments and when malware or compromised devices are detected—alongside other network activity. This visibility enables administrators to prioritize actions that should be taken to address potential threats, all from a single window.

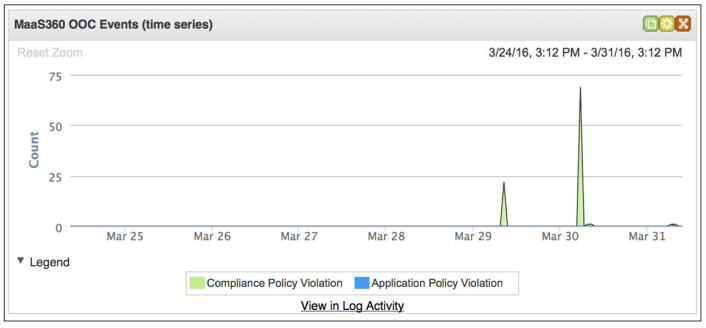
With its extensive reporting capabilities, QRadar gives administrators the ability to analyze a series of mobile threats or audit a specific mobile user's activity. This is particularly useful when evaluating the measures that need to be taken to address specific behaviors, or determining whether the activity puts the organization at risk of compromising data security or falling out of compliance with industry regulations.

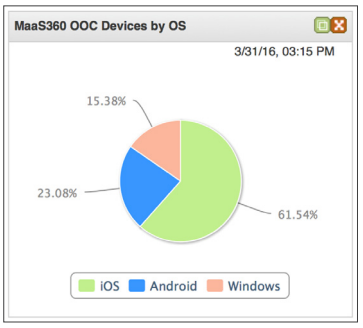
Administrators can use this intelligence to take immediate action or set up automated actions when security policies and compliance rules are violated.

MaaS360 App for QRadar on IBM Security App Exchange

The first enterprise mobility management (EMM) solution to feature an app on the App Exchange, MaaS360 now makes it possible for QRadar administrators to view thousands of mobile events from a single dashboard.

An extension from the QRadar / MaaS360 integration, the app features two new widgets that help simplify otherwise complex data. Now visualize out-of-compliance devices by operating system, or events by frequency, making it possible to react with confidence when an irregularity is spotted.





For More Information

To learn more about our technology and services visit
www.ibm.conres.com
800.237.6091