IBM Security MaaS360 with Watson

A guide to how MaaS360 establishes effective device and user security

IBM Security

IBM

UEM security at a glance

What should unified endpoint management (UEM) mean to your organization? Many readers may answer that UEM is simply a label near-synonymous with the preceding terms of mobile device management (MDM) and enterprise mobility management (EMM).

That is, however, only telling a *fraction* of the story. While basic device management is a fantastic base, major analysts point out that UEM needs to be more user- and security-centric—paying attention to how a user behaves and what that user accesses throughout the day and distributing security measures accordingly. This builds Digital Trust, promotes Zero Trust, but must ultimately be done in a way that does not inhibit user productivity.

In this report, we will outline the key capabilities that IBM provides to support these needs and that truly put “Security” in the name IBM Security MaaS360 with Watson.

Contents

AI & security analytics

MaaS360 Advisor with Watson

User-based risk management

Granular reporting

Data loss prevention

Security containment of sensitive data

OS developer methods

Policies and compliance rules

Basic device actions

Network and VPN configuration

Compliance actions

Threat detection and remediation

Mobile Threat Management (MTM) should be the baseline

Mobile Threat Defense (MTD) is the full defense package

Identity and access management

AI & security analytics

MaaS360 Advisor with Watson

Insights

Before we dive into some of the deeper security capabilities MaaS360 has to offer, let's start at the beginning—the console home screen itself. There, an administrator will find Advisor Insights. These insights are real-time alerts provided by Watson alerting the admin to potential security risks and vulnerabilities that could impact the organization—whether those risks are as easily-corrected as a dozen Android tablets running an older operating system (OS) version or something more urgent, such as a news brief on the latest malware threat in the enterprise with information on how to protect your enrolled users and devices from being impacted.

Policy Recommendation Engine

When defining devices policies, MaaS360 will use customer analytics to recommend individual changes to policies that may better suit your organization. These same analytics are used to develop policy templates based on industry needs as well as customer use cases—a template that can help support a high security use case or HIPAA compliance, for example.

AI & security analytics

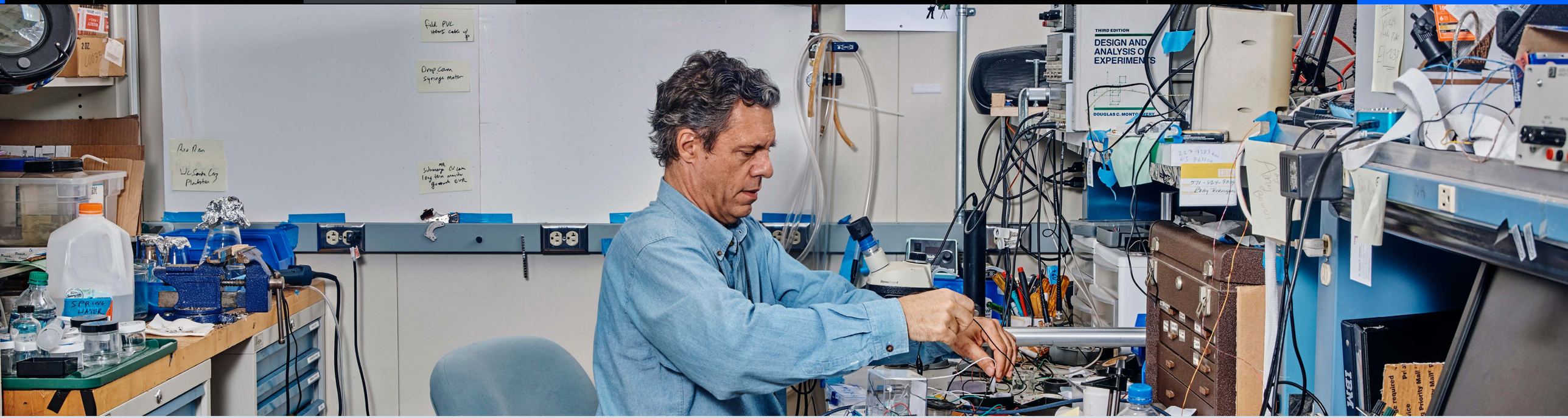
User-based risk management

By utilizing AI to assess multiple risk factors, spanning device attributes to user behavior, MaaS360 can build comprehensive risk profiles assessing the potential adverse impact a user may have on the organization. This analysis uses specific risk levels to categorize users, defining whether that user presents no issues, is potentially a risk, or appears to be an immediate threat to the organization—whether knowingly or unknowingly.

AI & security analytics

Granular reporting

Nearly everything within MaaS360—from device activity to application and data usage to installed software such as antivirus or anti-spyware—can be condensed into a downloadable report. An automated email can also be scheduled to send reports on specific parameters on a daily, weekly, or monthly basis to keep up-to-date on important organizational statistics.



Interested in learning more about how AI and security analytics through MaaS360 can enhance your UEM strategy? Request a demo today.

Start a trial

Data loss prevention

Secure containment of sensitive data

Whether a secure application provided by your UEM vendor or an operating system (OS) developer program that can be configured upon enrollment, a key goal of an effective device management deployment is to establish data loss prevention (DLP) policies in an effort to limit the movement of corporate data to places that data does not belong—either via malicious action or user error.

MaaS360 container application

The first option in MaaS360 is its native application as a container. In this case, the UEM app becomes a productivity suite, delivering mail, calendar, contacts, and other enterprise applications and resources to an encrypted sandbox built to restrict the copying, exporting, or even downloading of sensitive data, all without breaking the user experience; all applications within this container are designed to mimic the look and feel of the device OS's mail, calendar, and contacts applications, making transitioning simple for all users.

This containment can also extend to applications outside of the container. Through mobile app management (MAM) settings such as those within MaaS360's Workplace Persona container policies, certain enterprise applications can be configured to require authentication or to limit the ability of a user to migrate data outside of the application.

Data loss prevention

OS developer methods

iOS User Enrollment

This method, introduced in iOS 13, allows a device to split ownership between a personal Apple ID and a corporate Apple ID. This means that not only is data secured but user privacy is upheld by giving IT the ability to only view the corporate data.

While envisioned for BYOD usage, it isn't difficult to see its effectiveness for organizationally- owned devices as well since data accessed on the corporate side can be limited from interacting with the personal side of the device. That corporate data can also be easily removed once a device is lost, stolen, or unenrolled as it creates a separate volume specific to those files.Any corporate Windows 10 devices can make use of the DLP capabilities available through Windows Information Protection. As mentioned above, this feature allows organizations to designate specific apps and data on a user's device as sensitive.

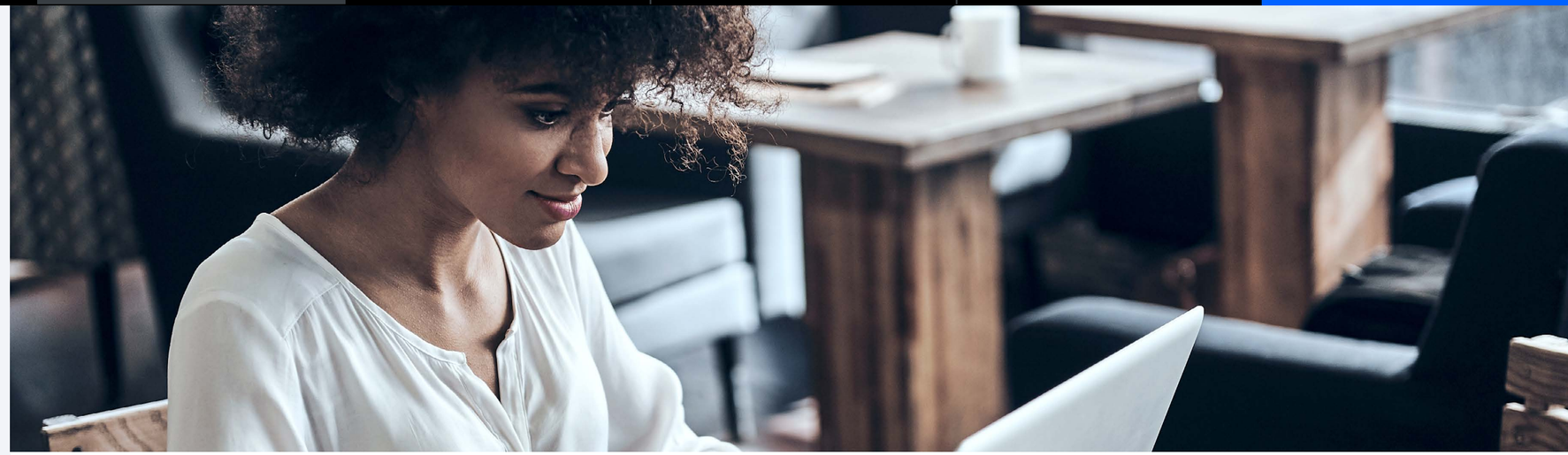
Data loss prevention

OS developer methods

Android Enterprise

Android Enterprise Profile Owner (PO) mode establishes a separate work profile on the Android operating system devoted to the corporate applications a user needs to access on a personal device. These applications are denoted with a briefcase icon and can be configured to not share data with their personal counterparts.

Device Owner (DO) mode can either distribute its own work profile for corporate owned, personally-enabled (COPE) deployments or fully manage the applications on the entire device. This gives administrators control over any installed service or application to preserve DLP and give more granular control over the operating system.



Data loss prevention

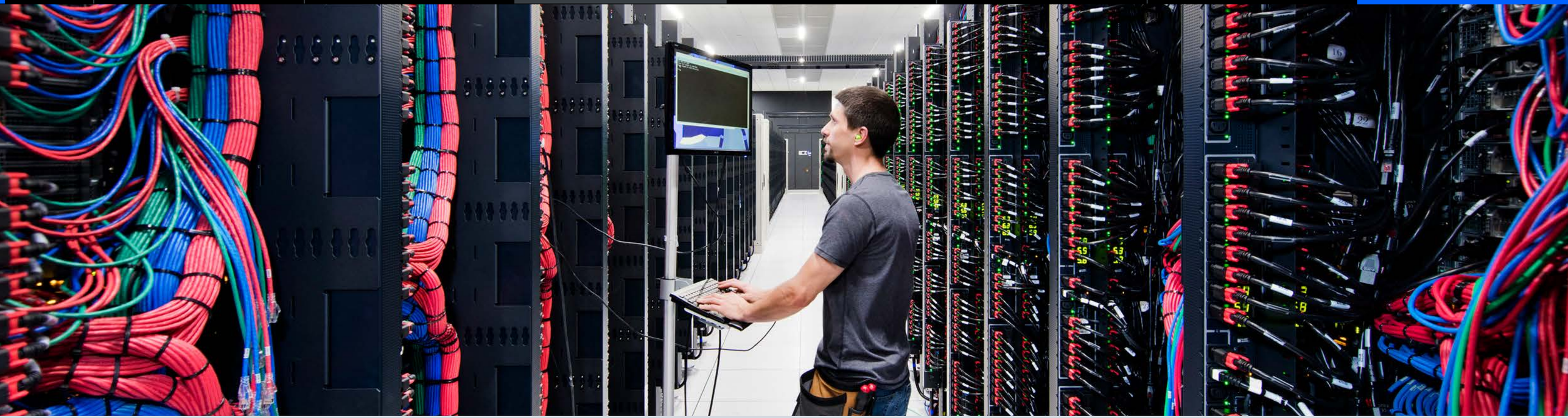
OS developer methods

Windows 10

Any corporate Windows 10 devices can make use of the DLP capabilities available through Windows Information Protection. As mentioned above, this feature allows organizations to designate specific apps and data on a user's device as sensitive. These items will then be encrypted and must first be decrypted each time a user goes to interact or view them. This is a feature available to all corporate-owned Windows 10 devices

In the case of BYOD, however, these devices often run the Windows 10 Home operating system, which does not allow for WIP or most API-based policies. Regardless, MaaS360 can still support certain necessary security functions on these devices in an effort to establish DLP through good data and operating system hygiene, including:

- Reporting on the service status, versions, and AV definitions of installed anti-virus, anti spyware, and similar software
- Granular patch and update management as well as the ability to distribute any applications, files, or scripts
- Automated out-of-compliance rules and actions for devices missing patches or running an older version of Windows 10, among other possible parameters



Interested in learning more about establishing DLP policy or supporting BYOD devices with MaaS360? Request a demo today.

Start a trial

Policies and compliance rules

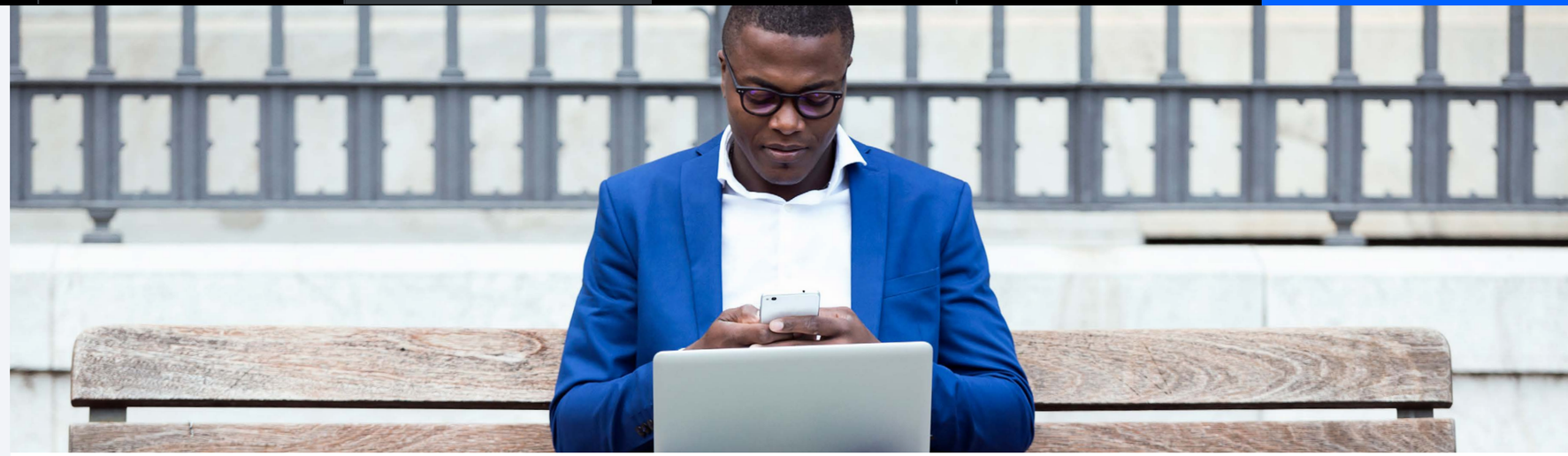
Basic device actions

At its core, a UEM solution enables expected mobile device management (MDM) capabilities. The most common capabilities are remote actions that an administrator can trigger to cover a wide array of situations. While there are dozens of actions within MaaS360, the most heavily used are listed here:

Lock
MaaS360 allows for any device, regardless of operating system, to be locked down to the login screen. In the event of a lost or stolen phone, tablet, or laptop, this is the first line of defense to ensure data cannot be accessed.

Locate
While MaaS360, through its reporting engine, can give the full picture of where devices have checked-in over a period of hours, days, or weeks, the on-demand location action is another tool for administrator's attempting to reclaim a lost or stolen device—or, in the case of a potential attack, detect geographic anomalies for user devices that may have been compromised.

Wipe/Selective Wipe
This is the clean-up hitter of actions. In reality, wipe and selective wipe are two separate actions, but the concept of device wiping itself is usually a last resort. The wipe command is a full factory reset on the device where the action is executed. On a corporate device that has been confirmed stolen or has been compromised, this is typically the route taken. For a personal device, however, the idea of wiping all data is a hard pill to swallow for users, precipitating the need for a selective wipe. In this case, MaaS360 will only remove the data that has been distributed through the platform—corporate applications, access to email, calendar, or contacts, and access to intranet or fileshares.



Policies and compliance rules

Network and VPN configuration

One of the first steps to good security hygiene when allowing users to access corporate resources from personal or corporate devices is the configuration of secure networks and VPN profiles. With support for all major VPN vendors and any Wi-Fi configuration, MaaS360 allows for profiles to be setup easily and distributed quickly via device security policy.

If your organization does not currently have a VPN or does not want to use its VPN for mobile access, MaaS360 have two options:

- The Mobile Enterprise Gateway is a relay configured to the MaaS360 container application delivering secure access to fileshares such as WFS or Sharepoint
- MaaS360 VPN is a native VPN that can be deployed as always-on, on-demand, or per app, to address the need for a secure connection across all applications and sites, a certain range of sites and applications, or specific applications, respectively

Policies and compliance rules

Compliance actions

Encryption support

While many devices can have their encryption levels configured via device policy—BitLocker for Windows or full device encryption for an Android Enterprise DO user, for instance—there are cases where the level of encryption can be changed by the user. In those scenarios, MaaS360 provides compliance actions meant to alert users about their encryption status. The automated actions can be as simple as a basic alert message to as impactful as a selective wipe of corporate resources until the issue is corrected.

Jailbreak and root detection

Similarly to encryption, a device found to have been jailbroken or rooted by a user—that is, compromised in such a way that the user has root access and can sideload applications and bypass the app store—can be immediately blocked from the corporate network or, in the case of a corporate device, factory reset to have that device put back into compliance.

App and OS compliance

As most organizations require a minimum OS version on an employee device for that employee to continue to have access to resources, MaaS360 provides the ability to take automated action in blocking or wiping devices not currently running the accepted version.

Geofencing

Via MaaS360 geofencing policy, compliance rules can be configured to block access to or selectively wipe sensitive data from a user's device. This is typically common in secure work environments, such as a hospital or financial institution, wherein the user may not need access once they have left for the day.

Interested in learning more about compliance rules and security policies through MaaS360? Request a demo today.

Start a trial

Threat detection and remediation

Mobile Threat Management (MTM) should be the baseline

Via an integration with IBM Trusteer, MaaS360 delivers real-time malware detection, recognizing known malware signatures present in installed applications. Users found to have these malicious applications will have access to corporate resources restricted, and the administrator will be notified of the issue.

Additionally, Trusteer can be configured to limit access to unsecured Wi-Fi connections to ensure users are always initiating sessions on a secure network.

Threat detection and remediation

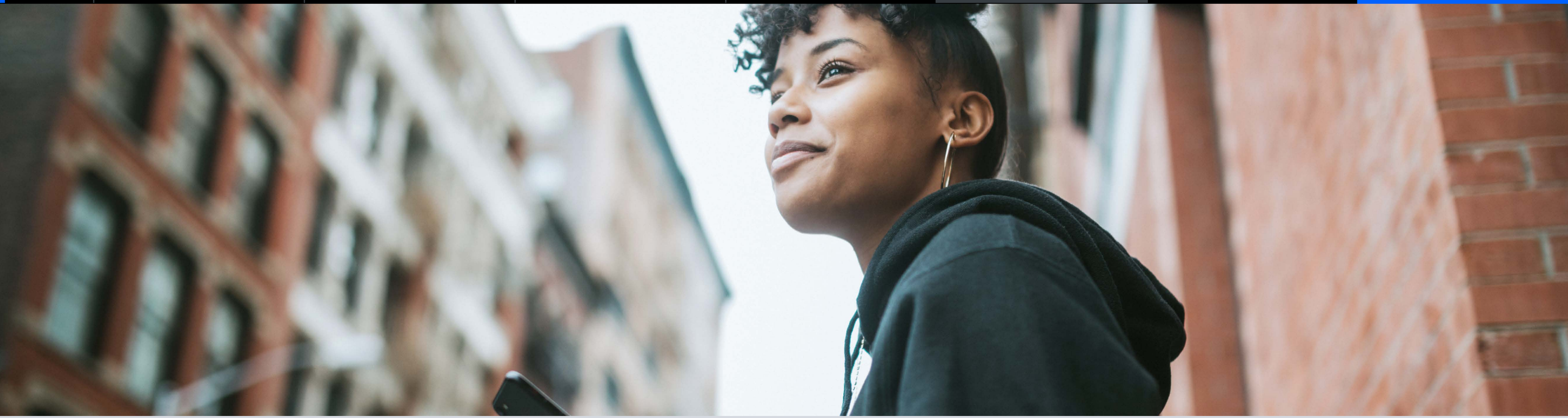
Mobile Threat Defense (MTD) is the full defense package

Beyond the detection of malware within applications, additional risks still threaten the security of your users, devices, and data. Whether man-in-the-middle attacks preying on poorly configured home and public Wi-Fi or increasingly convincing phishing emails, users are constantly vulnerable to a growing landscape of threats.

Via leading MTD vendor, Wandera, MaaS360 delivers proactive threat identification and remediation. Through Wandera's MI:RIAM AI platform, administrators gain access to real-time threat intelligence, from a continuously updated database of known malicious applications and phishing sites—which a user can automatically be blocked from accessing—to network defense aimed at stopping man-in-the-middle attacks and cryptojacking.

If your organization already has a threat defense app it prefers users install on their devices, MaaS360 can accommodate that as well. Most major security vendors provide their applications through the IBM Security App Exchange, giving additional UEM functionality for enterprise use.

Regardless of the threat detection or defense option you choose for your deployment, the MaaS360 compliance rule framework can be configured to remediate threats through the UEM console—whether those threats were detected natively or through an integration.



Interested in learning more about MaaS360’s available threat management capabilities and integrations? Request a demo today.

Start a trial

Identity and access management

Beyond the detection of malware within applications, additional risks still threaten the security of your users, devices, and data. Whether man-in-the-middle attacks preying on poorly configured home and public Wi-Fi or increasingly convincing phishing emails, users are constantly vulnerable to a growing landscape of threats.

SSO

Tying into an organization's existing directory service, MaaS360 provides a unified landing page for enterprise sign-on. Any corporate application can be provisioned for use via the Identity launchpad and delivered individually through MaaS360 or via the MaaS360 unified app catalog.

MFA

For devices enrolled in MaaS360, MFA can be enforced on specific SaaS applications. This MFA can support multiple second factors:

- Email and SMS one-time passcode (OTP)
- FIDO Token support
- FIDO 2/WebAuthn support for passwordless access
- Via the IBM Verify Authenticator app:
  - Time-based OTP
  - Push authentication via TouchID or FaceID
  - Passwordless QR code login

Conditional Access

Used in conjunction with automated compliance rules, risk-based Conditional Access (CA) policies can be configured to ensure risky users and devices are not interacting with sensitive data or other corporate resources.

Integration with existing tools

Beyond these native workflows, MaaS360 can also integrate with any existing standards-based IdP to support MaaS360 conditional access capabilities.

Interested in learning more about how MaaS360 establishes effective IAM policies? Request a demo today.

Start a trial