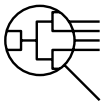
IBM Security MaaS360 with Watson

Protect your endpoints with enterprise-grade threat management

Receive AI and security analytics powered by Watson

Create robust security policies to help protect enterprise data



Advance your threat detection and remediation

Integrate SIEM and SOAR support for identity and access management

Distributed workforce models have quickly risen in popularity, leaving organizations to manage and protect multiple types of devices while increasing their cybersecurity challenges. Modern threats include phishing, mutating software, advanced persistent threats (APT), insider threats and vulnerabilities around cloud-based computing services.

Enhanced with automation and informed by AI, a cyber threat management system can help counter today's advanced attacks from cybercriminals by implementing a zero trust framework that assumes a complex network's security is always at risk to external and internal threats.

IBM Security® MaaS360® with Watson® is a SaaS unified endpoint management (UEM) solution with security built in to its core. This allows your IT team to monitor and protect endpoints, apps and content across all your organization's platforms.

IBM Security MaaS360 with Watson expands detection, prevention and response capabilities for endpoint security using a zero trust approach. AI security analytics powered by IBM Watson® enables responses based on the risk posture of users and devices. This enables IT teams to leverage a zero trust strategy and XDR use cases through integrations with the IBM Security stack.

Receive AI and security analytics powered by Watson
IBM Security MaaS360 with Watson provides Advisor Insights from the console home screen so your IT staff can see near real-time alerts to potential security risks and vulnerabilities. The Policy Recommendation Engine uses customer analytics to recommend individual changes to policies that may suit the organization. IBM MaaS360 with Watson has a Security Dashboard that allows for:

- Security incidents to be reviewed as they appear on the Security Dashboard or Security API
- Incidents to be used to calculate a Risk Score based on Risk Rules
- User-based risk management that utilizes AI to assess multiple risk factors, spanning from device attributes to user behavior
- Construction of comprehensive risk profiles to assess the potential adverse impact a user may have on the organization, using specific risk levels to categorize users
- Granular reporting, including device activity, application and data usage to installed software
- Automated email scheduling to send reports on specific parameters on a daily, weekly or monthly basis to keep up-to-date on important organizational statistics

Create robust security policies to help protect enterprise data
IBM Security MaaS360 with Watson has a new central endpoint security policy management feature to help address detection and response for multiple types of threats. An administrator can trigger remote actions to cover a wide array of situations, including:

- Security Policy creation, management and deployment to help address the most common types of threats
- Automated actions for blocking or wiping devices not currently running the accepted OS or app version
- The ability to lock devices, regardless of operating system, down to the login screen
- An on-demand location action which allows administrator's attempting to reclaim a lost or stolen device to detect geographic anomalies for user devices that may have been compromised
- Support for major VPN vendors and wifi configuration, with easy set-up of profiles that is distributed quickly via the device security policy
- The IBM MaaS360 Mobile Enterprise Gateway module delivers to file shares such as Windows File Share or SharePoint
- The MaaS360 VPN, which can be deployed as always-on, on-demand or per app
- Encryption support, enabling automated actions from basic alerts to the selective wipe of corporate resources until issues are corrected

Advance your threat detection and remediation
IBM Security MaaS360 with Watson enables enterprise-grade threat defense to detect threats and automate remediation across users, devices, apps, data and networks. Threat management is now a standalone service within MaaS360 that includes endpoint security and advanced user risk management. The MaaS360 threat management capabilities have evolved to include additional high value detections and a consolidated policy and response framework to aid with the following:

- SMS and email phishing
- IBM Security Trusteer® signature-based jailbreak and root detection
- Excessive app permission detection for Android devices
- IBM Security Trusteer malware and insecure wifi detection
- Windows and mac user process privilege detection
- Device configuration-based threats for Android devices
- Integration with an organizations' already existing threat defense app

Integrate SIEM and SOAR support for identity and access management
IBM Security MaaS360 with Watson has extended its integrations with SIEM and SOAR. MaaS360 has created a new API that provides incident events and data generated by MaaS360 to third party systems. MaaS360 integrates seamlessly with IBM® QRadar® to offer an end-to-end security experience. IBM MaaS360 incidents are available via a pre-packaged log source that is easily configured.

The integration between MaaS360 and QRadar technologies allows for:

- Realtime event processing for the Security Dashboard and Security API
- Realtime user and device risk evaluation based on event feeds
- Updated QRadar device support module and application integration
- SOAR runbooks and action integration
- Mobile threat incidents from MaaS360 to be merged with BAU security monitoring and processes
- IBM MaaS360 user data that can become part of User Behavior Analytics
- MaaS360 User Risk scoring which can be included in the data provided to QRadar and UBA via the Security API
- IBM MaaS360 for QRadar application integration, which is powered by the IBM X-Force® App Exchange and provides a visual overview of your MaaS360 devices, with views and drill down information for incidents discovered by MaaS360
- SOC analysts to view MaaS360 threat events in QRadar and act on them
- The SOAR system to update User Risk metrics, take automated actions and track cases, and escalate cases as needed based on follow-ups from SOC analysts

In addition to malware within applications, additional risks can threaten the security of organizations' users, devices and data. From man-in-the-middle attacks that prey on poorly configured home and public wifi systems, to increasingly convincing phishing emails, users are constantly vulnerable to a growing landscape of threats. Maas360 has a unified landing page for enterprise SSO and can provision any corporate application for use with the identity launchpad or unified app catalog. Risk-based conditional access (CA) policies can be configured so that risky users and devices don't interact with sensitive data or other corporate resources. Maas360 can also integrate with any existing standards-based identity provider to support conditional access capabilities. MFA can be enforced on specific SaaS applications and supports multiple second factors, including:

- Email and SMS one-time passcode (OTP)
- FIDO token support
- FIDO 2 and WebAuthn support for passwordless access
- IBM Verify Authenticator app, which includes support for a time-based OTP, push authentication via TouchID or FaceID, and passwordless QR code login

Conclusion

IBM Security MaaS360 with Watson has advanced security features for endpoints, applications and content, covering major operating systems and device types. MaaS360 features AI and security analytics, data loss protection, mobile threat management, and identity and access management, enabling users to establish policies and compliance rules while helping companies establish a zero trust framework.

For more information

To learn more about IBM Security MaaS360 with Watson, please contact your IBM representative or IBM Business Partner, or visit ibm.com/products/unified-endpoint-management.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
September 2022