IBM Security MaaS360 with Watson

Protect your endpoints with enterprise-grade threat management

Highlights
Leverage AI and security analytics powered by Watson

Defend enterprise data with robust security policies

Advance your threat detection and remediation

Integrate SIEM, SOAR and IAM support

In the current "work-from-anywhere" world, organizations seek to centrally manage endpoints and security, create frictionless experiences for their end users, reduce cyberthreats, and keep ownership costs low. Companies are challenged with multiple endpoint security tools and dashboards that can limit the ability of security analysts and IT administrators to be effective in mitigating and dealing with threats. For example, IBM's annual Cost of a Data Breach report, which features research from the Ponemon Institute, states that the global average total cost of a data breach among organizations surveyed increased 2.6% from USD 4.24 million in 2021 to USD 4.35 million in 2022. This is the highest it has been in the history of this report, with 83% of organizations studied having had more than one data breach.[1]

IBM Security® MaaS360® with Watson® is a unified endpoint management (UEM) solution which has evolved its built-in threat management capabilities from a small set of detections to include a new centralized policy and wider set of detections and responses for threats like email and SMS phishing, as well as insider threats. It is designed to help organizations merge efficiency and effectiveness by managing endpoints including mobile devices, laptops, desktops, wearables, and ruggedized devices, while also helping to protect them with augmented threat management capabilities. These threat management capabilities are built-in the product to help companies achieve the total cost of ownership levels they desire.

Evolved threat detection and remediation

According to IDC's U.S. Enterprise Workspace Management and Security Survey for 2021, mobile email phishing and SMS phishing were identified by U.S. IT and security administrators as the top two most frequently experienced mobile security threats[2].

IBM Security MaaS360 with Watson has expanded its threat management capabilities with a set of detections and responses to include mobile insider threat use cases, higher value insider threats, and zero trust detections. MaaS360 with Watson consolidates the policy and response definition in a centralized policy, enhances the risk dashboard into a full function security analytics dashboard, and provides API based integration opportunities. All this is brought together with risk-based conditional access to automate responses to threats.

In addition to protection against malware, jailbroken and rooted devices, and insecure wifi, MaaS360 with Watson also provides detection for SMS and email phishing, excess application permissions for Android devices, privilege management for Windows and MacOS users, and device configuration-based threats for Android devices. If your organization already has sophisticated threat management software, MaaS360 with Watson can integrate with most existing third party vendors.

Set up robust security policies or choose predefined ones to defend enterprise data

IBM Security MaaS360 with Watson has an updated central endpoint security policy which can control detections and responses for multiple types of threats. MaaS360 with Watson includes policies for use cases such as signature-based jailbroken and rooted device detection, IBM X-Force® exchange phishing detection (Email and SMS), excessive app permission detection, malware and insecure wifi detection, and Windows and MacOS user and process privilege detection.

Besides the common types of cyberthreats, an IT administrator has other priorities to take care of, such as managing the return of corporate devices or assisting employees who lose their devices. For these cases, an administrator can establish an on-demand location, allowing them to reclaim lost or stolen devices and detect geographic anomalies for user devices that may have been compromised. Administrators also benefit from encryption support and can enable automated actions, from basic alerts to the selective wipe of corporate resources, until issues are corrected.

Leverage AI and security analytics powered by Watson

Security analytics and dashboards are an important part of modern UEM solutions. IBM Security MaaS360 with Watson provides AI-powered analytics and insights, using both structured and unstructured data as well as applied behavioral analytics in order to provide insights and automated action recommendations.

The Policy Recommendation Engine uses customer analytics to recommend individual changes to policies that may better suit the organization. The security dashboards have been enhanced in order to fit with the evolved threat management capabilities. Detections appear on the Security Dashboard in the Security Incidents section. These security incidents are also available via the Security API and are used to calculate a risk score based on risk rules. Granular reporting, including device activity, application and data usage to installed software, is also provided.

MaaS360 with Watson also applies automatizations so that IT administrators can schedule emails to send reports on specific parameters on a daily, weekly or monthly basis to keep up-to-date on important organizational statistics.

Integrate SIEM, SOAR and IAM support

Security Information Event Management (SIEM) and Security Operations, Automation and Response (SOAR) technologies have become part of robust security postures of organizations around the world. MaaS360 with Watson has extended its integrations with these technologies and 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 where all detected incidents are available to view via a pre-packaged log source that is easily configured.

Identity and access management (IAM) is extremely useful for companies that want to protect their corporate information by granting granular access to the right resources, while maintaining compliance with company and industry standards.

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 policies can be configured to help prevent risky users and devices from interacting with sensitive data or other corporate resources. Maas360 also integrates with IBM Security Verify to offer both workforce identity and client identity features, or with existing standards-based identity provider to support conditional access capabilities. Maas360 with Watson includes multifactor authentication that can be enforced on specific SaaS applications and supports multiple second factors.

Conclusion

MaaS360 with Watson offers automation, modern endpoint management, and built-in threat management capabilities which help protect against cyberthreats such as phishing, man-in-the-middle attacks, and other common vulnerabilities. Organizations don’t need to purchase expensive add-ons and are able to integrate MaaS360 with their existing security applications to help keep their total cost of ownership at a level they want.

Why IBM?

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

Notes

[1] The Cost of a Data Breach Report 2022, IBM, July 2022

[2] U.S. Enterprise Workspace Management and Security Survey, 2021: Endpoint Device Management Highlights and Trends, IDC, August 2021

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
October 2022

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.