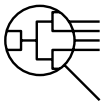
IBM Security MaaS360 with Watson

使用企业级威胁管理保护端点

接收由 Watson 支持的 AI 和安全分析

创建稳健的安全策略，助力保护企业数据



提高威胁检测和补救能力

集成 SIEM 和 SOAR 对身份和访问管理的支持

分布式劳动力模型已迅速普及，使企业能够管理和保护多种类型的设备，同时面临的网络安全挑战也相应增加。现代威胁包括网络钓鱼、变异软件、高级持续性威胁 (APT)、内部威胁和基于云计算服务的漏洞。

通过自动化和人工智能的增强，网络威胁管理系统可以通过实施零信任框架来帮助应对当今来自网络犯罪分子的高级攻击，该框架假设复杂网络的安全始终面临外部和内部威胁的风险。

IBM Security® MaaS360® with Watson® 是一款基于软件即服务 (SaaS) 的统一端点管理 (UEM) 解决方案，以安全为核心。借助该解决方案，IT 团队可以监控和保护组织所有平台上运行的端点、应用程序和内容。

IBM Security MaaS360 with Watson 使用零信任方法扩展了检测、预防和响应功能以确保端点安全。IBM Watson® 提供的 AI 安全分析支持基于用户和设备的风险态势做出响应。这使 IT 团队能够通过与 IBM Security 堆栈的集成来利用零信任策略和 XDR 用例。

接收由 Watson 支持的 AI 和安全分析

IBM Security MaaS360 With Watson 提供来自控制台主屏幕的 Advisor Insights 功能，确保 IT 人员可以查看与潜在安全风险和漏洞相关的实时警报。Policy Recommendation Engine 利用客户分析，推荐可能适合企业的个体策略调整方案。IBM MaaS360 with Watson 提供安全仪表板，可实现：

- 当安全事件出现在安全仪表板或安全 API 上时进行复核
- 用于根据风险规则计算风险分数的事件
- 利用 AI 评估多种风险因素的基于用户的风险管理，从设备属性到用户行为
- 构建全面的风险概况，以评估用户可能对组织产生的潜在不利影响，使用特定的风险等级对用户进行分类
- 细粒度报告，包括设备活动、应用程序和已安装软件的数据使用情况
- 自动定时发送邮件，每日、每周或每月发送有关特定参数的报告，以保持重要组织统计数据的最新状态

创建强大的安全策略以帮助保护企业数据

IBM Security MaaS360 with Watson 拥有全新的中央端点安全策略管理功能，有助于检测和响应多种类型的威胁。管理员可以触发远程操作，以应对各种情况，包括：

- 创建、管理和部署安全策略，以帮助解决最常见的威胁类型
- 用于阻止或擦除当前未运行接受的操作系统或应用程序版本的设备的自动操作
- 无论是什么操作系统，都可以锁定设备，直到登录屏幕
- 按需定位操作允许管理员试图找回丢失或被盗的设备，以检测可能已被入侵的用户设备的地理位置异常情况
- 支持主要 VPN 供应商和 Wi-Fi 配置，轻松设置配置文件，可通过设备安全策略快速分发
- IBM MaaS360 Mobile Enterprise Gateway 模块支持文件共享，例如 Windows File Share 或 SharePoint
- MaaS360 VPN 可随时按需或按应用程序部署
- 加密支持，支持从基本警报到选择性擦除公司资源的自动操作，直到解决问题

提高威胁检测和补救能力

IBM Security MaaS360 with Watson 支持企业级威胁防御，可跨用户、设备、应用程序、数据和网络检测威胁并自动执行补救措施。威胁管理目前是 MaaS360 内的一项独立服务，包括端点安全和高级用户风险管理。MaaS360 威胁管理功能已发展到包括额外的高价值检测以及整合的策略和响应框架，以帮助解决以下问题：

- SMS 和电子邮件网络钓鱼
- IBM Security Trusteer® 基于特征符的越狱和 root 检测
- Android 设备应用程序权限过度检测
- IBM Security Trusteer 恶意软件和不安全的 Wi-Fi 检测
- Windows 和 Mac 用户进程特权检测
- Android 设备基于设备配置的威胁
- 与组织现有的威胁防御应用程序集成

集成 SIEM 和 SOAR 对身份和访问管理的支持

IBM Security MaaS360 with Watson 扩展了与 SIEM 和 SOAR 的集成。MaaS360 创建了一个新的API，将 MaaS360 生成的事件和数据提供给第三方系统。MaaS360 与 IBM® QRadar® 无缝集成，以提供端到端安全体验。可通过易于配置的预打包日志源获取 IBM MaaS360 事件。

MaaS360 与 Qradar 技术集成实现以下功能：

- 安全仪表板和安全 API 的实时事件处理
- 基于事件源的实时用户和设备风险评估
- 已更新的 QRadar 设备支持模块和应用整合
- SOAR 运行手册和操作集成
- MaaS360 移动威胁事件与 BAU 安全监视和进程合并
- IBM MaaS360 用户数据可成为用户行为分析的一部分
- 可将 MaaS360 用户风险评分可包含在通过安全 API 提供给 Qradar 和 UBA 的数据中
- IBM MaaS360 for Qradar 应用整合由 IBM X-Force® App Exchange 提供支持，提供 MaaS360 设备的可视化概览，以及 MaaS360 发现的事件的视图和深入信息
- SOC 分析人员查看 Qradar 中的 MaaS360 威胁事件并采取行动
- SOAR 系统更新用户风险指标，采取自动化操作并跟踪案例，并根据 SOC 分析人员的跟进情况按需上报案例

除了应用程序中的恶意软件外，其他风险可能会威胁组织用户、设备和数据的安全。从针对配置不佳的家庭和公共 Wi-Fi 系统的中间人攻击，到越来越令人信服的网络钓鱼电子邮件，用户不断受到越来越多的威胁。Maas360 拥有统一的企业 SSO 登录页面，可为任何企业应用程序提供身份启动台或统一的应用程序目录。可配置基于风险的有条件访问权 (CA) 策略，避免风险用户和设备与敏感数据或其他企业资源交互。Maas360 也可以与基于现有标准的身份提供者集成，以支持有条件访问权功能。MFA 可在特定 SaaS 应用程序上强制实施，并支持多个次要因素，包括：

- 电子邮件和 SMS 一次性通行码 (OTP)
- FIDO 标记支持
- FIDO 2 和 WebAuthn 支持无通行码访问
- IBM Verify Authenticator 应用程序包括支持基于时间的一次性通行码 (OTP)、通过 TouchID 或 FaceID 推送认证、以及无密码二维码登录

结论

IBM Security MaaS360 with Watson 具有针对端点、应用程序和内容的高级安全功能，适用于主要操作系统和设备类型。MaaS360 具有 AI 和安全分析、数据丢失保护、移动威胁管理以及身份和访问管理功能，使用户能够在帮助公司建立零信任框架的同时制定策略和合规性规则。

详细信息

要了解 IBM Security MaaS360 with Watson 的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或者访问 ibm.com/cn-zh/products/unified-endpoint-management。

国际商业机器（中国）有限公司
了解更多信息，欢迎访问我们
的中文官网：**https://www.ibm.com/cn-zh**

美国出品
2022 年 9 月