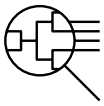
IBM Security MaaS360 with Watson

Proteja sus endpoints con una gestión de amenazas de nivel empresarial

Obtenga IA y análisis de seguridad basados en Watson

Cree políticas de seguridad sólidas para ayudar a proteger los datos empresariales



Propicie la detección y corrección de amenazas

Integre SIEM y SOAR en la gestión de identidad y acceso

Los modelos de personal geográficamente disperso han ganado popularidad rápidamente, lo que hace que las organizaciones tengan que gestionar y proteger varios tipos de dispositivos, al tiempo que sus retos de ciberseguridad aumentan. Las amenazas modernas incluyen el phishing, la mutación del software, las amenazas persistentes avanzadas (APT), las amenazas internas y las vulnerabilidades en torno a los servicios informáticos basados en cloud.

Un sistema de gestión de amenazas mejorado con automatización e informado por IA puede ayudar a combatir los avanzados ataques actuales de los ciberdelincuentes mediante la implementación de un marco de zero trust que da por hecho que la seguridad de una red compleja siempre está expuesta a amenazas externas e internas.

IBM Security® MaaS360® with Watson® es una solución SaaS de gestión unificada de endpoints (UEM) con la seguridad integrada en su núcleo. Eso permite al equipo de TI supervisar y proteger endpoints, aplicaciones y contenido en todas las plataformas de una organización.

IBM Security MaaS360 with Watson amplía las prestaciones de detección, prevención y respuesta aplicadas a la seguridad de endpoints con un enfoque de zero trust. El análisis de seguridad de IA basado en IBM® Watson ofrece respuestas basadas en la posición de riesgo de los usuarios y dispositivos. Esto permite a los equipos de TI aplicar una estrategia de zero trust y casos de uso de XDR mediante integraciones con la pila de IBM Security.

Obtenga IA y análisis de seguridad basados en Watson
IBM Security MaaS360 with Watson incluye información de Advisor en la pantalla de inicio de la consola, de modo que el personal de TI pueda ver alertas de posibles riesgos de seguridad y vulnerabilidades prácticamente en tiempo real. El motor de recomendación de políticas emplea análisis de clientes para recomendar cambios individuales en políticas que podrían ser apropiados para la organización. IBM MaaS360 with Watson tiene un panel de seguridad que permite:

- Revisar incidentes a medida que aparecen en el panel o en la API de seguridad
- Utilizar los incidentes para calcular una puntuación de riesgo basada en reglas de riesgo
- Gestionar el riesgo en función del usuario recurriendo a la IA para evaluar varios factores de riesgo, desde los atributos del dispositivo hasta el comportamiento del usuario
- Elaborar exhaustivos perfiles de riesgo para evaluar el posible impacto adverso de un usuario sobre la organización, utilizando niveles de riesgo específicos para categorizar a los usuarios
- Elaborar informes detallados en los que se incluya desde la actividad del dispositivo o el uso de aplicaciones y datos hasta el software instalado
- Programar automáticamente el envío por correo electrónico de informes sobre parámetros específicos cada día, semana o mes, a fin de estar al corriente de estadísticas importantes de la organización

Cree políticas de seguridad sólidas para proteger los datos empresariales
IBM Security MaaS360 with Watson incorpora una nueva función centralizada de gestión de políticas de seguridad de endpoints que mejora la detección de varios tipos de amenazas y la respuesta a ellas. Los administradores pueden activar medidas remotas para cubrir una amplia gama de situaciones, como:

- Creación, gestión e implementación de políticas de seguridad que ayuden a hacer frente a los tipos de amenazas más comunes
- Acciones automatizadas para bloquear o borrar dispositivos que no tengan la versión aceptada de un sistema operativo o aplicación
- Capacidad de bloquear dispositivos, independientemente del sistema operativo, incluida la pantalla de inicio de sesión
- Una acción de ubicación bajo demanda que, cuando un administrador intente recuperar un dispositivo perdido o robado, le permita detectar anomalías geográficas en los dispositivos de usuario que puedan estar comprometidos
- Compatibilidad con los principales proveedores de VPN y configuraciones de wifi, mediante una configuración de perfiles sencilla que se distribuye rápidamente a través de la política de seguridad de dispositivos
- El módulo IBM MaaS360 Mobile Enterprise Gateway es compatible con servicios de uso compartido como Windows File Share o SharePoint
- MaaS360 VPN, que se puede implementar de forma permanente, bajo demanda o por aplicación
- Soporte de cifrado que permite acciones automatizadas, como alertas básicas o el borrado selectivo de recursos corporativos hasta que se corrigen los problemas

Propicie la detección y corrección de amenazas
IBM Security MaaS360 with Watson ofrece una defensa de nivel empresarial para detectar amenazas y automatizar la corrección en usuarios, dispositivos, aplicaciones, datos y redes. La gestión de amenazas ahora es un servicio independiente dentro de MaaS360 que incluye seguridad de endpoints y gestión avanzada del riesgo de los usuarios. Las prestaciones de gestión de amenazas de MaaS360 han evolucionado para incluir detecciones adicionales de alto valor, así como una política consolidada y un marco de respuesta para ayudar con lo siguiente:

- Phishing por SMS y correo electrónico
- Detección de jailbreak y root basada en firmas de IBM® Security Trusteer
- Detección de permisos de aplicación excesivos en dispositivos Android
- Detección de malware y redes wifi no seguras de IBM Security Trusteer
- Detección de privilegios en procesos de usuario de Windows y Mac
- Amenazas basadas en la configuración de dispositivos Android
- Integración con la aplicación de defensa frente a amenazas ya existente en una organización

Integre SIEM y SOAR en la gestión de identidad y acceso
IBM Security MaaS360 with Watson ha ampliado sus integraciones con SIEM y SOAR. MaaS360 ha creado una nueva API que proporciona eventos y datos de incidentes generados por MaaS360 a sistemas de terceros. MaaS360 se integra sin problemas con IBM® QRadar para ofrecer una experiencia de seguridad integral. Los incidentes de IBM MaaS360 están disponibles a través de un origen de registro preempaquetado que se configura fácilmente.

La integración entre las tecnologías MaaS360 y QRadar permite:

- Procesamiento de eventos en tiempo real en el panel y la API de seguridad
- Evaluación del riesgo de usuarios y dispositivos en tiempo real basada en fuentes de eventos
- Módulo actualizado de soporte de dispositivos QRadar e integración de aplicaciones
- Runbooks SOAR e integración de acciones
- Combinación de incidentes de amenazas móviles de MaaS360 con la monitorización y los procesos de seguridad BAU
- Integración de datos de usuario de IBM MaaS360 en los análisis de comportamiento de usuario
- Inclusión de la puntuación de riesgo de usuario de MaaS360 en los datos proporcionados a QRadar y UBA a través de la API de seguridad
- Integración de aplicaciones de IBM MaaS360 para QRadar basada en IBM® X-Force App Exchange que brinda una visión general de los dispositivos MaaS360, con vistas e información detallada de los incidentes detectados por MaaS360
- Consulta de eventos de amenazas de MaaS360 en QRadar y resolución de estos por parte de los analistas SOC
- Sistema SOAR para actualizar las métricas de riesgo de usuario, tomar medidas automatizadas y realizar un seguimiento de los casos, escalándolos según sea necesario en función de los comentarios aportados por los analistas SOC

Además de malware dentro de aplicaciones, existen otros riesgos que pueden amenazar la seguridad de los usuarios, dispositivos y datos de organizaciones. Los usuarios están constantemente expuestos a un panorama de amenazas cada vez mayor, desde ataques de intermediario (man-in-the-middle) que se aprovechan de redes wifi públicas y domésticas mal configuradas hasta correos electrónicos de phishing muy convincentes. Maas360 cuenta con una página de destino unificada para el SSO empresarial y puede ofrecer cualquier aplicación corporativa para su uso con el launchpad de identidades o el catálogo unificado de aplicaciones. Se pueden configurar políticas de acceso condicional (CA) en función del riesgo, de manera que los usuarios y dispositivos de riesgo no interaccionen con datos confidenciales u otros recursos corporativos. Maas360 también se puede integrar con cualquier proveedor de identidad existente basado en estándares para admitir prestaciones de acceso condicional. Es posible aplicar MFA en aplicaciones SaaS específicas para admitir varios segundos factores, entre ellos:

- Contraseña de un solo uso (OTP) por correo electrónico y SMS
- Compatibilidad con tokens FIDO
- Compatibilidad con FIDO 2 y WebAuthn para acceso sin contraseña
- Aplicación IBM Verify Authenticator, que incluye compatibilidad con una OTP temporal, autenticación push mediante Touch ID o Face ID e inicio de sesión mediante código QR sin contraseña

Conclusión

IBM Security MaaS360 with Watson ofrece prestaciones de seguridad avanzadas para endpoints, aplicaciones y contenido, y funciona en los principales sistemas operativos y tipos de dispositivos. MaaS360 cuenta con IA y análisis de seguridad, protección frente a pérdida de datos, gestión de amenazas móviles y gestión de identidad y acceso, lo que permite a los usuarios establecer políticas y normas de cumplimiento a la vez que ayuda a las empresas a definir un marco de zero trust.

Más información

Para obtener más información sobre IBM Security MaaS360 with Watson, póngase en contacto con su representante o su socio comercial de IBM, o visite ibm.com/es-es/products/unified-endpoint-management.

IBM España, S.A.
Santa Hortensia, 26-28
28002 Madrid

Producido en los
Estados Unidos de América
Septiembre de 2022