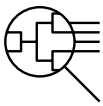
IBM Security MaaS360 with Watson

Protégez vos terminaux avec une gestion des menaces de niveau entreprise

Recevez des analyses de sécurité et d'IA alimentées par Watson.

Créez des politiques de sécurité robustes pour mieux protéger les données de votre entreprise.



Améliorez la détection et la résolution des menaces.

Intégrez un support SIEM et SOAR pour gérer les identités et les accès.

Les modèles de main-d'œuvre répartie deviennent de plus en plus populaires. En conséquence, les entreprises sont obligées de gérer et protéger de nombreux appareils tout en faisant face à de nouveaux défis en matière de cybersécurité. Les menaces modernes comprennent le hameçonnage, les logiciels malveillants en mutation, les menaces persistantes évoluées (APT), les menaces internes et les vulnérabilités sur les services informatiques basés sur le cloud.

Grâce à l'automatisation et l'IA, les systèmes de gestion des cybermenaces sont capables de contrer des attaques critiques en adoptant une approche Zero Trust qui part du principe que la sécurité d'un réseau complexe est constamment en danger. Qu'il s'agisse de menaces externes ou internes.

IBM Security® MaaS360® with Watson® est une solution SaaS de gestion unifiée des terminaux (UEM) qui fait passer la sécurité avant tout le reste. Elle permet à votre équipe informatique de surveiller et de protéger les terminaux, les applications et le contenu sur toutes les plateformes de votre entreprise.

IBM Security MaaS360 with Watson améliore les capacités de détection, de prévention et de réponse grâce à une approche Zero Trust de la sécurité des terminaux. Les analyses de sécurité IBM Watson® alimentées par IA proposent des réponses fondées sur le degré d'exposition au risque des utilisateurs et des appareils. Ce processus permet aux équipes informatiques de tirer parti de la stratégie Zero Trust et des cas d'utilisation XDR grâce à des intégrations avec la pile IBM Security.

Recevez des analyses de sécurité et d'IA alimentées par Watson
IBM Security MaaS360 with Watson propose Advisor Insights à partir de l'écran d'accueil de la console afin que votre équipe informatique puisse visualiser les alertes en temps réel sur les risques et les vulnérabilités de sécurité potentiels. Le moteur de recommandation de politiques utilise les analyses des clients pour recommander des changements individuels aux politiques qui pourraient mieux convenir à l'organisation. IBM MaaS360 with Watson est équipé d'un tableau de bord de sécurité qui permet :

- d'examiner les incidents de sécurité lorsqu'ils s'affichent sur le tableau de bord ou l'API ;
- de tirer parti des incidents pour calculer un score du risque basé sur des règles de risque ;
- à la gestion des risques basée sur l'utilisateur d'établir des facteurs d'évaluation des risques allant des attributs de périphérique au comportement utilisateur ;
- d'évaluer l'impact négatif potentiel d'un utilisateur sur l'entreprise grâce à la construction des profils de risque complets, en utilisant des niveaux de risques spécifiques pour classer les utilisateurs ;
- d'obtenir un modèle de reporting granulaire, y compris l'activité de l'appareil, les applications et l'utilisation des données sur un logiciel installé ;
- la programmation automatique des e-mails pour envoyer des rapports sur des paramètres spécifiques de manière quotidienne, hebdomadaire ou mensuelle afin d'être au courant des statistiques organisationnelles.

Créez des politiques de sécurité robustes pour mieux protéger les données de votre entreprise
IBM Security MaaS360 with Watson dévoile de nouvelles fonctionnalités centrales relatives aux politiques de sécurité des terminaux. Elles permettent de faciliter la détection et la réponse aux différents types de menaces. Un administrateur peut effectuer des actions à distance pour traiter de nombreuses situations, y compris :

- La création, la gestion et le déploiement d'une politique de sécurité qui aidera à répondre aux différents types de menaces
- Des actions automatisées qui bloqueront ou élimineront les appareils qui n'utilisent pas la version approuvée du système d'exploitation ou d'application
- La possibilité de verrouiller des appareils, quel que soit leur système d'exploitation, jusqu'à l'écran de connexion
- Une action de localisation à la demande qui permet à l'administrateur qui tente de récupérer un appareil perdu ou volé de détecter les anomalies géographiques des appareils qui auraient pu être compromis
- Une prise en charge des principaux fournisseurs de VPN et de la configuration Wi-Fi, avec un paramétrage des profils facile qui est rapidement distribué via la politique de sécurité des appareils
- Le module IBM MaaS360 Mobile Enterprise Gateway qui permet d'accéder à des partages de fichier comme Windows File Share ou SharePoint
- Le MaaS360 VPN, qui peut être déployé en continu, sur demande ou par application
- Une prise en charge du chiffrement pour automatiser des actions allant des alertes basiques à la suppression sélective des ressources de l'entreprise jusqu'à la correction des problèmes

Améliorez la détection et la résolution des menaces
IBM Security MaaS360 with Watson garantit une défense des menaces de niveau entreprise afin de détecter et d'automatiser la résolution des menaces pour tous les utilisateurs, appareils, applications, données et réseaux. La gestion des risques est devenue un service autonome au sein de MaaS360, offrant une protection des terminaux et une gestion avancée des risques liés aux utilisateurs. Les capacités de gestion des menaces de MaaS360 ont évolué pour inclure des détections à forte valeur ajoutée, une politique consolidée et un cadre de réponse pour aider dans les domaines suivants :

- Le hameçonnage par SMS ou e-mail
- La détection de débridage et de racine d'IBM Security Trusteer®
- La détection des autorisations excessives dans une application pour les appareils Android
- La détection de logiciels malveillants et de Wi-Fi non sécurisé avec IBM Security Trusteer
- La détection du privilège de processus utilisateur Windows et Mac
- Les menaces basées sur la configuration de l'appareil pour Android
- L'intégration à une application de sécurité existante au sein d'une entreprise

Intégrez un support SIEM et SOAR pour gérer les identités et les accès
IBM Security MaaS360 with Watson a étendu ses intégrations avec les solutions SIEM et SOAR. MaaS360 a créé une nouvelle API qui fournit aux systèmes tiers des événements et des données d'incidents générés par MaaS360. MaaS360 s'intègre facilement à IBM® QRadar® pour offrir une sécurité de bout en bout. Les incidents IBM MaaS360 sont disponibles depuis une source de journal déjà créée qui est facilement configurable.

Cette intégration entre MaaS360 et les technologies QRadar permet :

- de traiter des événements en temps réel sur le tableau de bord et l'API de sécurité ;
- d'évaluer en temps réel les risques utilisateurs et des appareils en fonction des flux d'événements ;
- d'intégrer le module et l'application de support de périphérique mis à jour QRadar ;
- d'intégrer les dossiers d'exploitation et les actions SOAR ;
- de fusionner des incidents liés aux menaces mobiles de MaaS360 avec la surveillance et les processus de sécurité BAU ;
- de regrouper les données utilisateur d'IBM MaaS360 avec l'analyse du comportement utilisateur (User Behavior Analytics) ;
- d'inclure le scoring MaaS360 de risque utilisateur dans les données fournies par QRadar et UBA via l'API de sécurité ;
- d'intégrer l'application IBM MaaS360 for QRadar, qui est alimentée par IBM X-Force® App Exchange et offre une vision globale des appareils MaaS360 avec des informations détaillées sur les incidents découverts par MaaS360 ;
- de donner les moyens aux analystes SOC de voir les événements de menaces de MaaS360 dans QRadar et d'y répondre ;
- au système SOAR de mettre à jour les mesures de risques utilisateurs, d'agir de manière automatisée, de suivre les événements et de faire remonter les cas si nécessaire, en fonction des suivis des analystes SOC.

Les logiciels malveillants ne sont pas les seuls à menacer la sécurité des utilisateurs, des appareils ou des données d'une entreprise. Qu'il s'agisse d'attaques de l'homme du milieu qui exploitent les réseaux Wi-Fi et privés mal configurés ou de hameçonnage par e-mail de plus en plus convaincant, les utilisateurs sont en danger constant face aux menaces qui ne cessent de grandir. Maas360 dispose d'une page d'accueil unifiée pour le SSO d'entreprise et peut mettre à disposition n'importe quelle application d'entreprise à utiliser avec le tableau de bord d'identité ou le catalogue d'applications unifié. Il est possible de configurer l'accès conditionnel (CA) fondé sur le risque afin que les utilisateurs et appareils à risque n'interagissent pas avec des données sensibles ou des ressources d'entreprise. Maas360 s'intègre également avec tous les fournisseurs d'identité existants basés sur les standards pour prendre en charge les capacités d'accès conditionnel. La MFA peut être appliquée sur des applications Saas spécifiques et prendre en charge plusieurs seconds facteurs comme :

- Un code d'accès à usage unique (OTP)
- Un jeton pris en charge par FIDO
- Un accès sans mot de passe pris en charge par FIDO 2 et WebAuthn
- L'application IBM Verify Authenticator, qui comprend un code d'accès à usage unique basé sur le temps, une authentification push via TouchID ou FaceID et une connexion sans mot de passe avec code QR

Conclusion

IBM Security MaaS360 with Watson possède des fonctionnalités de sécurité avancées pour les terminaux, les applications et le contenu, qui couvre les principaux systèmes d'exploitation et types d'appareils. MaaS360 est équipé de l'IA et d'analyses de sécurité, d'une protection pour la perte de données, d'une gestion des menaces mobiles et d'une gestion des identités et des accès. Cette solution permet aux utilisateurs de mettre en place des politiques et des règles de conformité en suivant une approche Zero Trust.

Pour plus d'informations

Pour en savoir plus sur IBM Security MaaS360 with Watson, contactez votre représentant IBM ou votre partenaire commercial IBM, ou rendez-vous sur ibm.com/fr-fr/products/unified-endpoint-management.

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex

Produit aux
États-Unis d'Amérique
Septembre 2022