IBM Security MaaS360 with Watson

Protégez vos terminaux avec une gestion des menaces de niveau entreprise

En bref

Tirez parti de l'IA et des analyses de sécurité alimentées par Watson

Protégez les données de l'entreprise avec des politiques de sécurité robustes

Améliorez la détection et la résolution des menaces

Intégrez la prise en charge des technologies SIEM, SOAR et IAM

Dans le contexte actuel de télétravail généralisé, les entreprises cherchent à centraliser la gestion des terminaux et de la sécurité, à créer des expériences fluides pour leurs utilisateurs finaux, à réduire les cybermenaces et à maintenir les coûts de propriété à un niveau bas. Les entreprises sont confrontées à une multitude d'outils et de tableaux de bord de sécurité des terminaux qui peuvent limiter la capacité des analystes de la sécurité et des administrateurs informatiques à atténuer les menaces et à y faire face efficacement. Ainsi, le rapport annuel d'IBM sur le coût d'une violation de données qui s'appuie sur des recherches de l'Institut Ponemon indique que le coût total moyen mondial d'une violation de données chez les entreprises interrogées a augmenté de 2,6 %, passant de 4,24 millions de dollars en 2021 à 4,35 millions de dollars en 2022. C'est le chiffre le plus élevé jamais atteint dans l'histoire de ce rapport, 83 % des entreprises étudiées ayant subi plus d'une atteinte à la protection des données.[1]

IBM Security® MaaS360® with Watson® est une solution de gestion unifiée des terminaux (UEM) qui a fait évoluer ses capacités intégrées de gestion des menaces, passant d'un petit ensemble de détections à une nouvelle politique centralisée et à un ensemble plus large de détections et de réponses pour des menaces telles que l'hameçonnage par e-mail et par SMS et les menaces internes. Il est conçu pour aider les entreprises à associer l'efficacité à la performance en gérant les terminaux, y compris les appareils mobiles, les ordinateurs portables, les ordinateurs de bureau, les dispositifs portables et les appareils renforcés, tout en aidant à les protéger grâce à des capacités accrues de gestion des menaces. Ces capacités de gestion des menaces sont intégrées au produit afin d'aider les entreprises à atteindre les niveaux de coût total de possession qu'elles souhaitent.

Évolution de la détection des menaces et de la résolution
Selon l'étude de l'IDC sur la gestion et la sécurité de l'espace de travail des entreprises américaines pour 2021, les administrateurs informatiques et de sécurité américains ont identifié l'hameçonnage par e-mail sur mobile et l'hameçonnage par SMS comme les deux menaces de sécurité mobile les plus fréquentes[2].

IBM Security MaaS360 with Watson a étendu ses capacités de gestion des menaces à l'aide d'un ensemble de détections et de réponses pour inclure les cas d'utilisation concernant les menaces mobiles internes , les menaces internes de grande valeur et les détections zero trust. MaaS360 with Watson consolide la définition de la politique et de la réponse au sein d'une politique centralisée, améliore le tableau de bord des risques pour en faire un tableau de bord analytique de la sécurité complet et offre des possibilités d'intégration basées sur l'API. Tout cela est associé à un accès conditionnel basé sur les risques pour automatiser les réponses aux menaces.

En plus de la protection contre les logiciels malveillants, les appareils débridés et rootés, et le Wi-Fi non sécurisé, MaaS360 with Watson assure également la détection de l'hameçonnage par SMS et par e-mail, des autorisations d'application excessives pour les appareils Android, de la gestion des privilèges pour les utilisateurs de Windows et de MacOS, et des menaces basées sur la configuration de l'appareil pour les appareils Android. Si votre entreprise dispose déjà d'un logiciel sophistiqué de gestion des menaces, MaaS360 with Watson peut s'intégrer à la plupart des produits de fournisseurs tiers existants.

Mettez en place des politiques de sécurité robustes ou choisissez des politiques prédéfinies pour défendre les données de l'entreprise
IBM Security MaaS360 with Watson dispose d'une politique de sécurité centrale actualisée pour les terminaux capable de contrôler les détections et les réponses pour plusieurs types de menaces. MaaS360 with Watson inclut des politiques pour des cas d'utilisation tels que la détection d'appareils débridés et rootés basée sur des signatures, la détection de l'hameçonnage IBM X-Force® Exchange (e-mail et SMS), la détection de permissions d'applications excessives, la détection de logiciels malveillants et de Wi-Fi non sécurisé, et la détection de privilèges d'utilisateurs et de processus Windows et MacOS.

Outre les types courants de cybermenaces, l'administrateur informatique doit s'occuper d'autres priorités, telles que la gestion de la restitution des appareils de l'entreprise ou l'assistance aux employés qui perdent leurs appareils. Dans de tels cas, un administrateur peut établir une localisation à la demande, ce qui lui permet de récupérer les appareils perdus ou volés et de détecter les anomalies géographiques pour les appareils d'utilisateurs susceptibles d'avoir été compromis. Les administrateurs bénéficient également d'une assistance au chiffrement et peuvent configurer des actions automatisées, depuis les alertes de base jusqu'à l'effacement sélectif des ressources de l'entreprise, jusqu'à ce que les problèmes soient corrigés.

Tirez parti de l'IA et des analyses de sécurité alimentées par Watson
Les analyses de sécurité et les tableaux de bord constituent une part importante des solutions UEM modernes. IBM Security MaaS360 with Watson fournit des analyses et des informations alimentées par l'IA exploitant des données structurées aussi bien que non structurées et des analyses comportementales appliquées afin de fournir des informations et des recommandations d'action automatisées.

Le moteur de recommandation de politiques utilise les analyses des clients pour recommander des modifications individuelles des politiques susceptibles de les rendre plus adaptées à l'organisation. Les tableaux de bord de sécurité ont été améliorés afin de s'adapter à l'évolution des capacités de gestion des menaces. Les détections s'affichent dans le tableau de bord de la sécurité, dans la section Incidents de sécurité. Ces incidents de sécurité, également disponibles via l'API de sécurité, servent à calculer un score de risque basé sur des règles de risque. Ils permettent également d'obtenir des rapports granulaires concernant l'activité de l'appareil, l'utilisation des applications et des données, et les logiciels installés.

MaaS360 with Watson applique également des automatisations afin que les administrateurs informatiques puissent programmer l'envoi d'e-mails avec des rapports sur des paramètres spécifiques sur une base quotidienne, hebdomadaire ou mensuelle afin de rester à jour sur les statistiques importantes de l'organisation.

Intégrez la prise en charge des technologies SIEM, SOAR et IAM
Les technologies d'information sur la sécurité et gestion des événements (SIEM), d'opérations de sécurité, et d'orchestration, automatisation et réponse en matière de sécurité (SOAR) font désormais partie des mesures de sécurité robustes des entreprises du monde entier. MaaS360 with Watson a étendu ses intégrations avec ces technologies et a créé une nouvelle API qui fournit des événements d'incidents et des données générés par MaaS360 à des systèmes tiers. MaaS360 s'intègre de manière fluide à IBM® QRadar® pour offrir une expérience de sécurité de bout en bout, dans le cadre de laquelle tous les incidents détectés sont visualisables depuis une source de fichiers journaux d'origine facile à configurer.

La gestion des identités et des accès (IAM) est extrêmement utile pour les entreprises qui souhaitent protéger leurs informations en accordant un accès granulaire aux ressources appropriées, tout en respectant les normes de l'entreprise et du secteur.

Maas360 dispose d'une page d'accueil unifiée pour le SSO d'entreprise et peut provisionner n'importe quelle application d'entreprise pour l'utiliser avec le tableau de bord d'identité ou le catalogue d'applications unifié. Il est possible de configurer des politiques d'accès conditionnel basées sur le risque pour empêcher les utilisateurs et les appareils à risque d'interagir avec des données sensibles ou d'autres ressources de l'entreprise. Maas360 s'intègre également à IBM Security Verify pour offrir des fonctions d'identification du personnel et des clients, ou à un fournisseur d'identification basé sur des normes existantes pour prendre en charge les capacités d'accès conditionnel. Maas360 with Watson inclut l'authentification multi-facteur qui peut être appliquée à des applications SaaS spécifiques et il prend en charge de nombreux facteurs secondaires.

Conclusion
MaaS360 with Watson assure l'automatisation, la gestion moderne des terminaux et des capacités intégrées de gestion des menaces qui contribuent à protéger contre les cybermenaces telles que l'hameçonnage, les attaques man-in-the-middle et d'autres vulnérabilités courantes. Les entreprises n'ont pas besoin d'acheter d'onéreux modules complémentaires. Elles peuvent intégrer MaaS360 à leurs applications de sécurité existantes afin de maintenir leur coût total de possession au niveau souhaité.

Pourquoi IBM ?
IBM Security MaaS360 with Watson possède des fonctionnalités de sécurité avancées pour les terminaux, les applications et les contenus qui couvrent les principaux systèmes d'exploitation et types de dispositifs. MaaS360 comprend l'IA et l'analyse de la sécurité, la prévention de la perte de données, la gestion des menaces mobiles et la gestion des identités et des accès, ce qui permet de mettre en place des politiques et des règles de conformité tout en aidant les entreprises à établir une approche de type Zero trust dans leur cadre de sécurité.

Pour plus d'informations,
Pour en savoir plus sur IBM Security MaaS360 with Watson, contactez votre interlocuteur IBM habituel ou un partenaire commercial IBM, ou rendez-vous sur ibm.com/fr-fr/products/maas360.

Notes

1. Rapport sur le coût d'une violation de données 2022, IBM, juillet 2022
2. U.S. Enterprise Workspace Management and Security Survey, 2021: Endpoint Device Management Highlights and Trends, IDC, août 2021

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

Produced in the
United States of America
October 2022