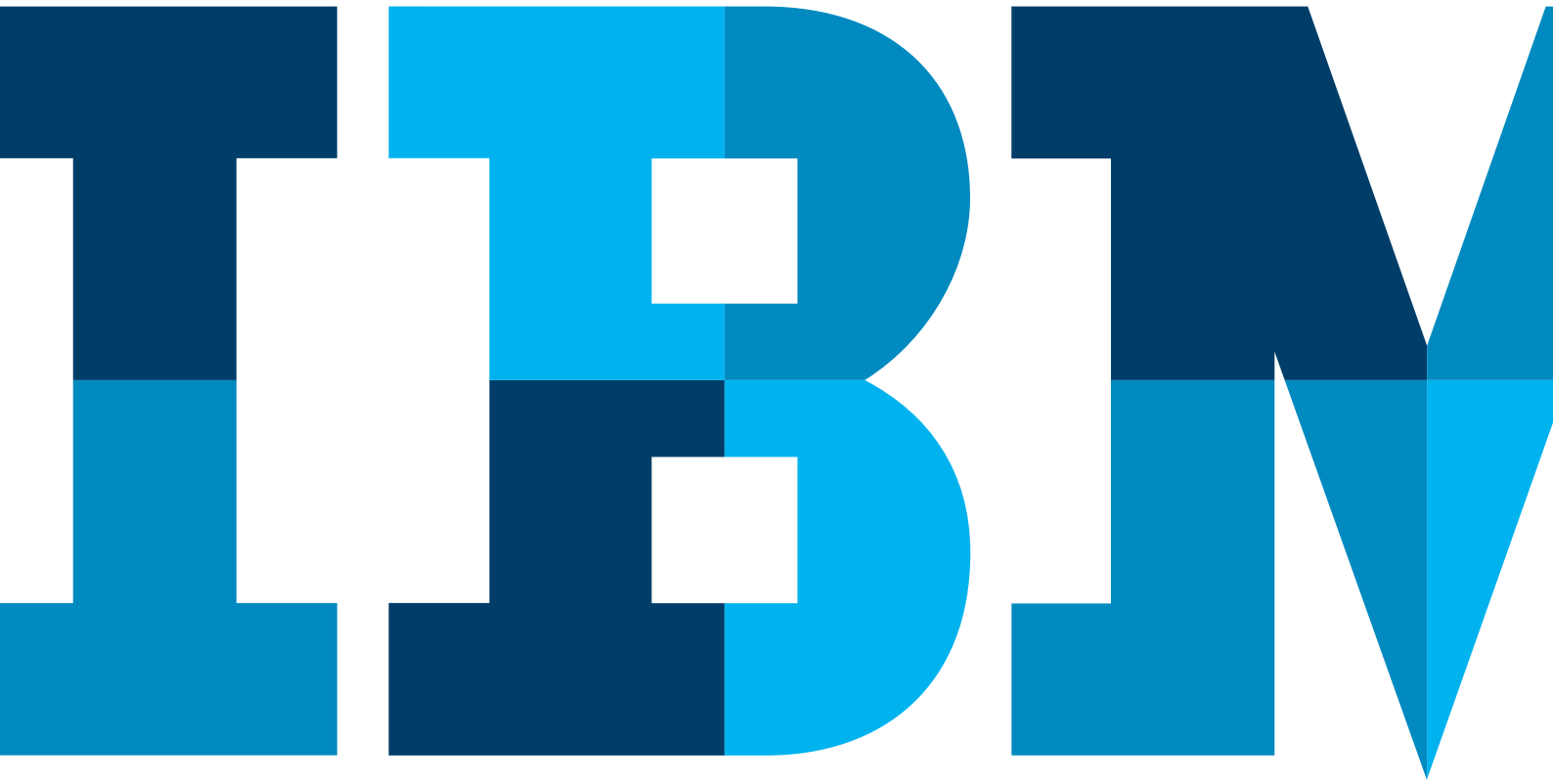
Sécurité IBM
Livre blanc

Mars 2017

L’intelligence augmentée élimine les vulnérabilités sur les terminaux et la mobilité



IBM

Sommaire

Évoluer vers un avenir mieux sécurisé

Quel que soit leur type ou leur taille, les entreprises deviennent rapidement de véritables organisations numériques, exploitant des technologies et des systèmes qui les rendent plus compétitives, agiles, efficaces et prospères. La technologie mobile en particulier joue un rôle critique, puisqu'elle apporte les avantages incontournables de l'entreprise numérique.

Cependant, un nombre rapidement croissant de menaces de cybersécurité parmi les plus virulentes ciblent les terminaux. Les pirates diffusent constamment de nouvelles attaques par hameçonnage pour obtenir les coordonnées d'accès à des PC, tablettes et smartphones. Les attaques zéro-jour et les outils capables d'identifier les systèmes vulnérables imposent la mise en œuvre de nouvelles défenses pour protéger les entreprises.

Face à l'évolution des menaces et aux exigences de la conformité, il est logique que les outils nécessaires à la gestion et à la sécurité des terminaux et de la mobilité évoluent aussi. En quelques années seulement, nous sommes passés de la gestion des dispositifs mobiles à la gestion de la mobilité, puis à la gestion unifiée des terminaux (UEM), qui fournit un plus haut niveau de fonctionnalité de gestion et des capacités de sécurité plus efficaces.

Les systèmes d'intelligence augmentée qui renforcent les capacités humaines, au lieu de répliquer toute la capacité de l'intelligence humaine, comme y aspire l'intelligence artificielle, développeront la prochaine génération de solutions de sécurité et d'informatique.

La technologie cognitive et l'intégration de l'intelligence augmentée figurent parmi les plus importantes avancées de la gestion unifiée des terminaux, comme IBM MaaS360 avec Watson. L'intégration avec Watson change la donne à plusieurs niveaux. Premièrement, elle réduit le nombre et l'ampleur des tâches manuelles et des détails de la mobilité qui accaparent le temps des administrateurs et des responsables des systèmes en découvrant les alertes et les éclairages clés pour les présenter directement sur la console MaaS360. Deuxièmement, elle accélère les changements liés aux règles et politiques de sécurité. Troisièmement, l'utilisation de la technologie cognitive autorise des raffinements supplémentaires dans les politiques et les normes, pour renforcer leur contextualisation dans les besoins spécifiques de l'entreprise, contrairement aux règles plus générales.

IBM MaaS360 With Watson™

Ce livre blanc discute de ces avantages et de ceux qu'apportent l'intelligence augmentée et les technologies cognitives.

La nécessité d'éliminer les vulnérabilités sur les points terminaux

Comme les entreprises sont confrontées à des exigences juridiques et de conformité plus rigoureuses pour bénéficier de pratiques de cybersécurité plus efficaces, les vulnérabilités des terminaux ne peuvent plus être tolérées. Cependant, comme les pirates utilisent des approches innovantes et déploient de nouveaux types de malware, cette intolérance n'est jamais facile à mettre en œuvre. D'après une étude du Ponemon Institute, le coût moyen d'une violation des données est de 4 millions USD,[1] et le coût de chaque document perdu a augmenté pour atteindre 156 USD. Ces coûts n'incluent pas les conséquences pour l'entreprise et sa réputation. Par exemple, suite à la fameuse attaque Target, l'entreprise a subi une baisse de 46 % de ses bénéfices.[2]

La dernière étude de l'Institut SANS sur la sécurité des terminaux[3] conclut que les entreprises ont besoin de systèmes de protection robustes sur les terminaux à cause de deux tendances croisées :

1. Un environnement utilisateur plus complexe favorise les erreurs des utilisateurs et laisse des portes ouvertes aux attaques.
2. Des menaces ciblées et intelligentes sont dissimulées dans des e-mails ou des sites Web légitimes pour l'utilisateur sans formation adaptée ou peu vigilant.

D'après l'étude SANS, 47 % des violations réussies sont dues à des erreurs d'utilisateur, ce qui oblige les entreprises à mettre en œuvre des protections qui ne dépendent pas des utilisateurs en première ligne de défense. En outre, elle indique que 38 % des violations abouties utilisent des techniques d'ingénierie sociales sophistiquées pour se donner une apparence inoffensive. Les malwares zéro-jour et les malware sans signature représentent un autre groupe de 36 % des violations réussies, exigeant une meilleure sécurité des terminaux.

Des logiciels exacerbent le problème avec des vulnérabilités connues qui n'ont pas été corrigées ou mises à jour par des versions périodiquement sécurisées. La recherche et l'élimination des vulnérabilités s'avèrent plus difficiles avec des outils de protection manuels ou n'offrant qu'une intelligence limitée. Ce problème s'aggravera, étant donné que le terme « terminaux » commence déjà par s'élargir en incluant un nombre croissant de nouveaux types de terminaux.

Comment les technologies cognitives et l'intelligence augmentée éliminent les vulnérabilités sur les terminaux

Dans de nombreuses situations, le problème de la sécurité des terminaux ne réside pas dans le manque de connaissances extraites des logs, des données sur les menaces, du suivi des comportements et d'autres éclairages. Il réside surtout dans le difficile développement d'une compréhension fine des séquences d'événements et des solutions applicables. Les technologies cognitives utilisent l'intelligence augmentée pour classer toutes les informations et les activités et fournir aux administrateurs informatiques et aux analystes de la sécurité des éclairages exploitables et des tableaux de bord centrés sur les terminaux.

Ces technologies améliorent la capacité de protection et de gestion des terminaux grâce à une collection de mesures stratégiques dans un grand nombre d'entreprises différentes. Elles révèlent un contexte étendu pour interpréter les données de sécurité, prendre des décisions mieux informées pour renforcer les actions, les politiques de sécurité et la gestion des terminaux. Par exemple, il est possible de développer une notation de la sécurité mobile qui permet d'évaluer la posture de la sécurité de l'entreprise par rapport à ses pairs. Cette notation permet d'établir une comparaison critique de la sécurité des terminaux, de la sécurité des connexions et d'autres aspects clés de l'environnement mobile.

Les outils UEM basés sur l'intelligence augmentée font évoluer les processus de sécurité et de gestion du changement en enrichissant le contexte des menaces, avec une personnalisation qui répond mieux aux besoins uniques et à l'infrastructure de chaque entreprise. Par conséquent, les actions sont déterminées par la prioritisation basée sur l'organisation, et non pas selon une perspective générale. Comme le nombre des vulnérabilités et des menaces augmente tous les mois, leur prioritisation précise prend une importance critique.

Les technologies cognitives permettent aux équipes informatiques et de la sécurité d'adopter une approche de la cyberdéfense beaucoup plus proactive, et de déterminer divers éléments, tels que :

1. **Que s'est-il passé ?** Les équipes peuvent plus rapidement identifier et comprendre un événement de sécurité ou un problème de gestion des terminaux. Même si de nombreuses solutions existantes peuvent identifier la plupart de ces événements, elles prennent souvent plus de temps, n'aboutissent pas toujours à un résultat ou fournissent seulement des informations partielles. Le personnel est alors obligé de consacrer plus de temps pour identifier les détails du problème et comprendre la relation entre ces informations et leur environnement. De nombreux produits existants fournissent uniquement un support réactif, au lieu de proactif, après le problème ou la violation.
2. **Que peut-il se passer ?** Avec l'intelligence augmentée, il devient possible de prévoir ce qui se passera sur les terminaux avant un événement, afin que SecOps prépare les conséquences. Cette approche change la donne. Toutes les entreprises

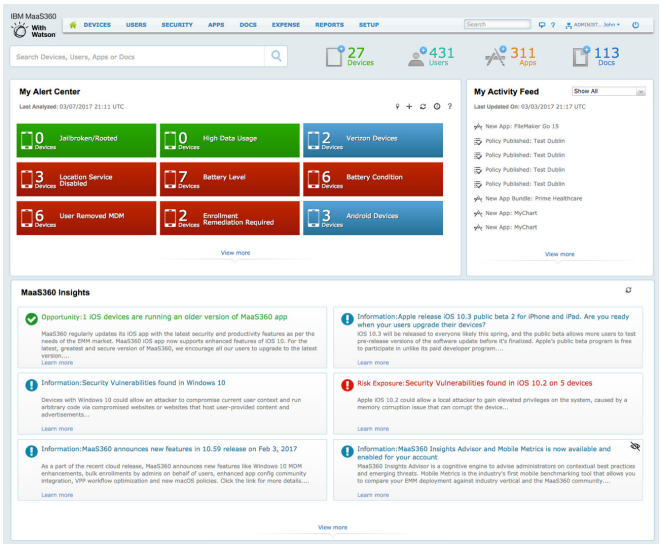
n'ont pas les mêmes vulnérabilités ou les mêmes fonctions de gestion des terminaux. Ces éléments uniques ont des conséquences importantes au regards des risques ou des problèmes futurs. Les technologies cognitives permettent aux entreprises d'établir des correspondances entre des menaces futures et leurs cyber-défenses actuelles.

3. **Ce qu'il faut faire ?** Plus les risques présents et futurs sont compris, plus il devient possible de définir efficacement des options correctives. Grâce à l'intelligence et aux technologies cognitives, les entreprises peuvent évaluer des options plus variées et développer une connaissance avancée des résultats pour chacune d'elles. En exploitant des données cohérentes descriptives de chaque permutation et en réduisant le volume des données subjectives, il est alors beaucoup plus simple de comparer des options et de choisir la meilleure alternative. Les actions peuvent alors être présentées à un administrateur, en un seul clic.

IBM® MaaS360 avec Watson fournit une approche cognitive à la solution UEM

IBM est un pionnier de l'ère cognitive avec la technologie Watson. En intégrant la technologie avec IBM MaaS360 et l'excellente intelligence de la sécurité X-Force Exchange, il est maintenant possible d'améliorer le retour sur investissement (ROI) des projets de création des terminaux et de renforcer considérablement la sécurité de ces terminaux. Les avantages de cette solution UEM de prochaine génération sont les suivants :

- Identifier et déployer des opportunités de transformation numérique
- Réduire les risques de sécurité
- Augmenter la productivité du personnel
- Renforcer l'efficacité du service informatique et SecOps
- Aider l'entreprise à prendre des décisions informées, incluant des décisions sur les dépenses.



IBM MaaS360 avec Watson réunit trois fonctions essentielles :

- Advisor qui fournit des renseignements exploitables dans le contexte de l'entreprise
- Mobile Security Index qui fournit le premier tableau de bord de sécurité mobile public du secteur
- Mobile Metrics qui fournit la première génération de données de référence de mobilité basée dans le cloud pour ce secteur d'activité.

Synthèse

Les terminaux se multiplient rapidement dans les entreprises actuelles, avec de nouveaux types, tels que les terminaux vestimentaires, et les technologies émergentes comme l'Internet des objets, sans compter les différents terminaux choisis par les utilisateurs. Il n'est donc pas surprenant que de nouvelles vulnérabilités émergent presque tous les jours. Les approches traditionnelles appliquées à la gestion des vulnérabilités sur les terminaux ne peuvent pas surmonter les nouvelles difficultés ni fournir les éclairages pertinents dont les entreprises ont besoin pour prendre des décisions optimales et informées. La réponse adaptée consiste à améliorer les outils de gestion des terminaux avec des technologies cognitives et d'intelligence augmentée. Il est maintenant possible de mettre en œuvre une approche efficace à trois étapes pour identifier ce qui se passe, projeter ce qui peut se passer et choisir la solution optimale pour résoudre le problème. Rendant ce nouveau type d'outil encore plus utile, elle peut aussi évaluer les données provenant de nombreuses entreprises et les analyser par rapport aux besoins unique de leur environnement.

Pour plus d'informations, visitez :

Pour en savoir plus sur IBM MaasS360, contactez votre interlocuteur IBM ou votre partenaire commercial IBM. Vous pouvez également consulter le site Web suivant : **ibm.com/maas360**

IBM United Kingdom Limited
PO Box 41, North Harbour
Portsmouth, Hampshire PO6 3AU
Royaume-Uni

IBM Ireland Limited
Oldbrook House
24-32 Pembroke Road
Dublin 4

IBM Ireland, entreprise déclarée en Irlande sous le numéro 16226.

Références

1 « Etude de l'Institut Ponemon sur le coût des failles de sécurité 2016 » IBM Security, 2016

2 « Target : les violations de données font chuter les bénéfices » The New York Times, 26 fév. 2014

3 « Vulnérabilités sur les terminaux : Enquête SANS sur le paysage des menaces 2016, » SANS Institute, Sept. 2016

TechTarget Custom Media

WGW03299FRFR-00