

McAfee Vulnerability Manager

Surveillance hautes performances, en temps réel et continue des actifs

Principaux avantages distinctifs

- Evolutivité, précision et flexibilité inégalées
- Evaluation en temps réel des nouveaux équipements dès leur apparition sur le réseau, inventaire complet des logiciels et du matériel, mappage des utilisateurs aux actifs et création automatique de la topologie réseau
- Combinaison de la découverte et de la surveillance actives et passives des actifs du réseau pour identifier les équipements virtualisés, mobiles et non visibles
- Analyses ciblées sur la base d'audits approfondis des équipements, dont les résultats alimentent une base de données des actifs faisant autorité
- Evaluation des vulnérabilités entièrement automatisée grâce au marquage dynamique des systèmes
- Solution mise à jour avec les vulnérabilités et les menaces les plus récentes via McAfee Global Threat Intelligence™
- Sécurité basée sur les informations d'identification des utilisateurs avec privilèges grâce à l'intégration de Cyber-Ark
- Analyse des réseaux IPv4 et IPv6
- Génération de rapports entièrement flexible — analyse unique des actifs et génération de rapports connexes à tout moment
- Workflows de gestion des risques automatisés pouvant inclure des applications McAfee, développées en interne ou d'éditeurs tiers

Protégez votre entreprise grâce à la solution la plus souple, éprouvée et évolutive du secteur, pour une gestion des vulnérabilités en temps réel et extrêmement simple. McAfee Vulnerability Manager, avec sa fonctionnalité McAfee Asset Manager, offre une évolutivité et des performances inégalées, et examine de façon active ou passive l'ensemble des composants du réseau. Si un équipement ou un actif possède une adresse IP ou utilise votre réseau, McAfee Vulnerability Manager peut l'identifier et l'évaluer automatiquement et en temps réel, et ainsi déterminer l'état de conformité de l'ensemble des ressources du réseau.

McAfee Vulnerability Manager est la référence du secteur en matière de gestion des vulnérabilités. En effet, la solution prend en compte les réalités de l'entreprise en examinant tous les types de configurations réseau et des actifs. Elle peut effectuer une analyse passive, continue ou active des éléments et au moment choisis par vous et vous permet d'automatiser la découverte, l'évaluation et la correction de tous vos actifs, ainsi que la génération de rapports sur ceux-ci. Vous pouvez ainsi déceler les équipements non visibles de votre réseau de même que les smartphones, les tablettes et les ordinateurs portables qui se connectent et se déconnectent entre deux analyses planifiées. Vous serez surpris de constater tous les éléments passés inaperçus ou qui n'avaient pas été analysés, au risque de compromettre la conformité de votre entreprise. Des milliers d'entreprises font confiance à la solution McAfee Vulnerability Manager pour détecter et hiérarchiser les vulnérabilités, que le déploiement compte quelques centaines de postes ou 4 millions d'adresses IP à analyser en continu.

Facilité de mise en œuvre

Grâce à McAfee, vous pouvez mettre en œuvre une procédure d'analyse fiable. McAfee Vulnerability Manager s'installe facilement sur votre matériel physique ou virtualisé, ou peut être déployé au moyen d'appliances McAfee à la sécurité renforcée. En quelques minutes, vous serez prêt à lancer votre première analyse.

Le chargement et la maintenance de l'inventaire d'actifs sont tout aussi simples. Grâce au module McAfee Asset Manager, la base de données des actifs est mise à jour immédiatement dès que de nouveaux équipements sont mis en ligne, et vous offre ainsi une visibilité en temps réel sur les équipements connectés au réseau. En outre, étant donné que McAfee Vulnerability Manager s'intègre étroitement avec des outils de gestion d'actifs d'entreprise, tels que LDAP, Microsoft Active Directory et la plate-forme de gestion McAfee® ePolicy Orchestrator® (McAfee ePO™), vous ne devez gérer qu'un seul référentiel central contenant toutes vos données d'actifs.

Visibilité sur l'ensemble des actifs

Le module en option McAfee Asset Manager augmente la visibilité grâce à une découverte et une surveillance des actifs passives exécutées en continu. Rapidement déployé sur un port SPAN, ce système surveille le trafic pour détecter et mapper tous les éléments du réseau, y compris les équipements non fiables, les hôtes VMware oubliés ainsi que les terminaux mobiles. Il peut ainsi dresser une liste des équipements, des modèles et des communications, ces informations vous permettant d'apprécier les risques et de les réduire. Les informations sur les équipements sont automatiquement envoyées à McAfee Vulnerability Manager en vue d'une évaluation immédiate. McAfee Asset Manager peut par ailleurs procéder à un inventaire complet des logiciels et des composants matériels de chaque actif détecté.

Analyses personnalisées en fonction de vos besoins

McAfee Vulnerability Manager vous offre diverses options pour vous aider à établir des références et à démontrer votre conformité aux réglementations du secteur. Pour définir plus rapidement vos stratégies, analysez un système « de référence » pour établir une ligne de base, utilisez les modèles de conformité fournis ou chargez des stratégies qui mettent en œuvre la norme SCAP (Security Content Automation Protocol).

McAfee Vulnerability Manager analyse tous les actifs du réseau, même les actifs problématiques dans les environnements d'infrastructure critiques et isolés. Par exemple, si votre entreprise possède des réseaux sans connexion externe, vous pouvez déployer un analyseur pour ordinateur portable ou un analyseur virtuel pour détecter et analyser les actifs de ces réseaux. Vous avez ensuite la possibilité de conserver les résultats de l'analyse dans l'environnement fermé ou, le cas échéant, de les cumuler pour les communiquer à un système centralisé.

La plupart des systèmes d'exploitation exigent une authentification des actifs avant d'autoriser l'accès à des informations de configuration sensibles, mais, pour certaines équipes de sécurité,

Couverture d'analyse

- Analyse de plus de 450 versions de systèmes d'exploitation, y compris Microsoft Windows, UNIX, Cisco, Android, Linux, Apple Macintosh, Apple iOS et VMware
- Analyse approfondie des applications web (vulnérabilités liées aux catégories OWASP Top 10 et CWE Top 25)
- Recherche des vulnérabilités et des logiciels malveillants pour les logiciels Adobe, AOL, Apple, Microsoft (Office, IIS, Exchange), Blue Coat, CA, Cisco, Citrix, Facebook, Google, HP, IBM (Lotus Notes et WebSphere), Novell, Oracle, Real Networks, RIM (BlackBerry Enterprise Server), SAP, Oracle Java, Symantec et VMware
- Analyse des principales bases de données dont DB2, MySQL, Oracle, Microsoft SQL Server et Sybase

Normes et certifications

- La solution inclut des modèles pour ASCII 33, BÂLE II, BILL 198 (CSOX), BSI IT (GR), COBIT, FDCC, FISMA, GLBA, HIPAA, ISO 27002, JSOX, MITS, PCI, SOX, NIST SP 800-68, SANS Top 20, SCAP, OVAL, et bien d'autres.
- Elle prend en charge différentes normes, dont les audits certifiés CIS, les normes COBIT, CPE, CVE, CVSS, DISA STIG, FDCC/SCAP, ISO 17799/ISO 27002/FINRA, ITIL, NIST-SP800, NSA, OVAL et SANS Top 20.
- Certification « Common Criteria »
- Chiffrement conforme à la norme FIPS 140-2

Spécifications techniques

Pour consulter les spécifications produit ainsi que les configurations matérielles et logicielles requises, visitez le site www.mcafee.com/fr.

les informations d'identification nécessaires sont difficilement accessibles. Grâce à l'intégration de la suite Privileged Identity Management de Cyber-Ark, la découverte et l'analyse des actifs basées sur les informations d'identification sont non seulement hautement sécurisées, mais elles s'effectuent également de façon très simple et performante.

Détermination du risque en quelques minutes

Lorsque McAfee Asset Manager identifie un nouveau système sur le réseau, il transmet des informations détaillées à son sujet à McAfee Vulnerability Manager, qui peut alors lancer une analyse ciblée. En l'espace de quelques minutes, vous connaissez le statut de ce système et le risque qu'il présente pour votre environnement.

Marquage des actifs pour plus d'efficacité

Vous pouvez également avoir recours à des stratégies de marquage pour placer automatiquement de nouveaux équipements dans des groupes d'analyse sur la base du profil de chaque équipement et du risque qu'il représente. L'analyse pertinente peut ensuite être lancée immédiatement ou dans le cadre de l'analyse périodique suivante, en fonction des stratégies que vous définissez.

Détection des vulnérabilités et des logiciels malveillants

Alors que d'autres produits se contentent d'examiner superficiellement les configurations et les ports ouverts, McAfee Vulnerability Manager effectue une analyse en profondeur. La solution procède à des évaluations au niveau du système et des applications, qui incluent les bannières de base de données, les paramètres de stratégie, les clés de Registre, les autorisations associées aux lecteurs et aux fichiers ainsi que les services en cours d'exécution. Elle est capable de tester plus de 450 versions de système d'exploitation, afin de détecter le plus large éventail de vulnérabilités. Les inspections effectuées interceptent également le contenu malveillant, notamment les chevaux de Troie, les virus et autres logiciels malveillants (*malware*).

Vous pouvez compléter les contrôles prédéfinis et les mises à jour de protection contre les menaces « jour zéro » en écrivant des scripts et des contrôles personnalisés afin de tester des applications héritées et propriétaires. McAfee Vulnerability Manager évalue également le contenu tiers conforme aux normes XCCDF, OVAL et SCAP.

Examen amélioré des applications web

McAfee Vulnerability Manager permet aux administrateurs de gérer les applications web de la même façon que les actifs réseau habituels. Ces applications web peuvent être regroupées, être affectées d'un niveau de priorité, d'un propriétaire et d'une personnalité. Grâce à des fonctionnalités entièrement automatisées, McAfee Vulnerability Manager effectue une analyse approfondie des applications web et passe au peigne fin tout l'éventail des vulnérabilités web.

Mise à jour continue

Partout dans le monde, des millions de sondes communiquent à des centaines de chercheurs de McAfee Labs les dernières évolutions du paysage des menaces. McAfee Global Threat Intelligence fournit à McAfee Vulnerability Manager, directement et en temps réel, les évaluations des risques et les avis sur les menaces afin de vous protéger des menaces émergentes.

Gestion, évolutivité et intégration à la carte

McAfee vous offre la possibilité de concevoir vos propres analyses et rapports et de personnaliser la gestion de la façon qui vous convient le mieux. Vous pouvez surveiller simplement les ressources en local à l'aide d'un analyseur ou suivre la progression des analyses effectuées par des centaines de moteurs d'analyse distants à partir d'une console unique. Notre architecture multiniveau s'adapte à la taille et aux besoins de chaque organisation.

Grâce à une interface de programmation d'applications (API) ouverte, McAfee Vulnerability Manager peut être intégré avec la plupart des applications.

Réponse en fonction du risque

La vue unique directement exploitable des vulnérabilités permet une réduction des coûts de gestion des patches et d'audit. Par exemple, le jour de la distribution mensuelle des correctifs par les éditeurs, vous pouvez rapidement déterminer les systèmes concernés par une nouvelle vulnérabilité Microsoft Windows ou Adobe. Inutile d'analyser de façon répétée l'ensemble du réseau : en quelques minutes, McAfee Vulnerability Manager hiérarchise les risques potentiels posés par les nouvelles menaces sur la base des données de configuration existantes et des scores de risque.

Grâce à ces informations, vous pouvez sélectionner des actifs en fonction de leur importance et les soumettre instantanément à une analyse ciblée, par un simple clic avec le bouton droit de la souris.

Mise en conformité pour une confiance accrue

Bénéficiez de preuves concluantes (par exemple, des informations telles que les résultats d'analyse théoriques et réels, les systèmes exclus de l'analyse ou encore les échecs d'analyse) pour démontrer l'absence de vulnérabilités de certains systèmes : une exigence de plus en plus courante dans le cadre des audits. Associant surveillance active et passive, tests d'intrusion et analyse avec et sans authentification, McAfee Vulnerability Manager vous permet d'identifier les vulnérabilités et les infractions aux stratégies avec le plus haut degré de précision. La gestion complète des vulnérabilités n'a jamais été aussi simple.

