



AIRMAGNET® Enterprise

Sécurité, performances et conformité des réseaux sans fil

Les technologies sans fil représentent des enjeux essentiels pour l'entreprise. Bien que le WiFi offre l'opportunité de bénéficier de réseaux plus flexibles et plus abordables, il introduit également de nouveaux risques et de nouvelles menaces qui ne sont pas pris en compte par les moyens de surveillance et de sécurité traditionnels. AirMagnet Enterprise assure un contrôle complet de ces risques, tout en permettant de bloquer un grand nombre de réseaux sans fil et d'identifier les problèmes de manière proactive et en temps réel. AirMagnet Enterprise détecte chaque menace et met en oeuvre une action automatique accompagnée de plusieurs niveaux d'élimination des menaces. Chaque réseau sans fil est surveillé en permanence de façon à assurer des performances et une disponibilité optimales, et une suite d'outils actifs permet aux administrateurs réseaux de régler les éventuels problèmes à distance. Une base de données professionnelle documente chaque évènement et effectue un audit automatique du réseau en termes de conformité aux politiques en vigueur. Le résultat final est un réseau sans fil aussi sécurisé, fiable et conforme que n'importe quel réseau câblé.

Une prévention automatisée des intrusions

AirMagnet Enterprise crée un bouclier au sein de vos réseaux sans fil, qui permet de rechercher et neutraliser automatiquement les menaces dès leur apparition.

Une détection des menaces à toute épreuve

Les réseaux sans fil exposent les entreprises à un nouveau type de menaces en termes de sécurité, où le point d'accès rogue ne représente que la partie immergée de l'iceberg. AirMagnet traque en permanence plus de 135 types de menaces pour les réseaux sans fil, et sur plus de 200 canaux WiFi, via des systèmes de détection de défaillance professionnels et entièrement indépendants. L'intelligence de chaque équipement de détection est ensuite corrélée de manière centralisée puis analysée en termes d'anomalies masquées liées à la sécurité et aux performances. La solution détecte et empêche tous les types de menaces liées au WiFi, y compris les rogues, les vulnérabilités de configurations, les outils d'attaque, les attaques DoS, les problèmes de 802.11n, etc.

Des défenses automatisées et proactives

AirMagnet Enterprise permet de stopper de manière active toute menace pouvant mettre votre réseau en danger. Chaque menace peut être automatiquement traquée jusqu'à la source et stoppée à l'aide de techniques d'élimination sans fil et filaires permettant d'assurer une protection complète du réseau.



Une suppression des menaces sans fil

Le blocage sans fil permet aux gestionnaires de réseaux de stopper immédiatement les menaces à la source. N'importe quel client, point d'accès, ad hoc ou système pirate peut être ciblé et bloqué de manière sélective sans affecter pour autant le bon fonctionnement du réseau.



Suppression des menaces filaires

AirMagnet Enterprise permet également de traquer automatiquement une menace jusqu'à un emplacement situé sur le réseau câblé et de couper le port de commutation associé, protégeant ainsi le réseau câblé de plus grande taille contre les menaces provenant du réseau sans fil. Contrairement à certaines autres solutions de surveillance, l'ensemble de la recherche et du blocage des menaces est effectué exclusivement au sein de la solution AirMagnet, assurant ainsi une défense complète et indépendante du réseau.

Autopsie complète des menaces

Le système AirMagnet permet d'archiver le trafic source de n'importe quel événement en vue d'une analyse détaillée des menaces.

Cela offre ainsi au personnel chargé de la sécurité une base de données contenant une preuve matérielle des menaces et des intrusions les plus importantes.

Localisation des menaces

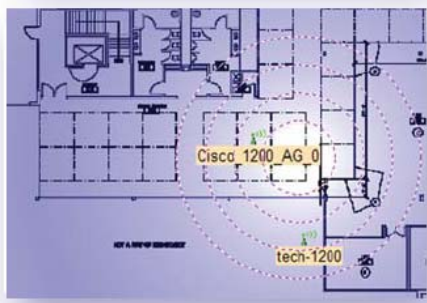
AirMagnet indique l'emplacement de l'ensemble des menaces sur une « carte » du réseau.

Le personnel chargé de la sécurité peut ainsi vérifier si une menace est présente à l'intérieur ou à l'extérieur des installations, et prendre les mesures nécessaires.

Réponse automatisée

Toutes les actions de AirMagnet peuvent être liées à une politique et déclenchées automatiquement, garantissant ainsi que les réseaux sont protégés 24 heures sur 24, même lorsque le personnel n'est pas disponible.

	Switch IP	10.1.1.252
	Switch Port Id	21 [Fa0/21]
	Wireless Info	00:0D:0B:1A:14:03
	Status	Blocked
Time	Rogue History Description	User-Sensor
10/08 09:38:33	Traced	AirMagnet System-qa2012
10/08 05:41:14	Traced	AirMagnet System-SM6
10/08 01:41:15	Traced	AirMagnet System-SM6
10/07 21:40:23	Traced	AirMagnet System-SM6
10/07 19:37:05	Wireless blocked	AirMagnet System-tv2016



Blocage et localisation de n'importe quel équipement

Un contrôle complet des rogues

Les rogues constituent une menace importante pour tous les réseaux sans fil, alors AirMagnet offre l'approche la plus rigoureuse du marché en terme de détection, désactivation, et de documentation de tous les rogues et cela en continu.



Détection automatique

AirMagnet audite chaque dispositif en permanence, sur la base de votre politique (adresse MAC, SSID, distributeur du matériel, canal, et mode 802.11). Les ACL peuvent être facilement synchronisées à partir d'autres systèmes tel WLSE de Cisco.

Détection à un endroit précis

AirMagnet identifie de manière proactive les rogues qui se trouvent à l'intérieur de n'importe quelle zone sécurisée, permettant alors de mettre en oeuvre de réelles protections sur les réseaux sans fil.

Recherche des rogues à la source

Les rogues sont automatiquement recherchés à l'aide de plusieurs procédés, de façon à les identifier et les stopper rapidement.

Désactivation des rogues

La solution AirMagnet désactive les rogues des réseaux sans fil et câblés, les isolant complètement de votre réseau. Toutes les réponses peuvent être automatisées de façon à assurer une protection permanente contre les rogues.

Documentation

AirMagnet documente avec précision chaque rogue, y compris son emplacement, son statut de blocage, les informations relatives au commutateur et au port, etc. Des rapports détaillés et exportables peuvent être générés au sein du module de création de rapports de AirMagnet.

Une surveillance proactive des performances

En plus d'assurer une sécurité optimale, le système Enterprise comprend des fonctionnalités évoluées d'analyse de performance et de dépannage.

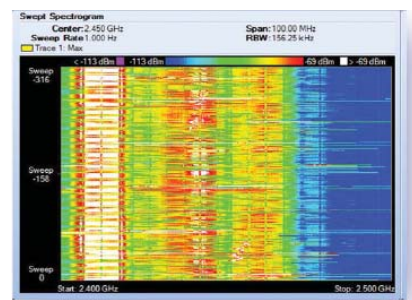
Maintien des performances optimales

AirMagnet surveille les problèmes réels liés aux performances, y compris la surcharge de ressources, les problèmes de bande passante, et les problèmes RF. La solution audite également chaque équipement sans fil en ce qui concerne des dizaines de problèmes de configuration pouvant affecter les performances du réseau. AirMagnet permet également une analyse sophistiquée des compromis en termes de performances sur les réseaux mixtes (802.11a/b/g), ainsi qu'une analyse des problèmes liés au 802.11e et à la voix.

Analyse du trafic

AirMagnet analyse les flux de trafic entre tous les dispositifs du réseau, et surveille la métrique de l'ensemble des paquets et des trames critiques. Les utilisateurs peuvent consulter en temps réel toutes les informations

relatives à toute communication, et la base de connaissances AirWise alerte les utilisateurs sur les communications présentant des problèmes de performances.



Analyseur de spectre

Analyse de spectre

Les détecteurs de l'analyseur de spectre AirMagnet permettent d'effectuer une analyse du réseau sans fil et une analyse spectrale depuis n'importe quelle position. Ils identifient et nomment automatiquement les sources d'interférence (Bluetooth, four à micro-ondes, etc.) et peuvent ensuite générer des alertes. Les utilisateurs du système peuvent alors étudier à distance tous les graphiques de spectres en temps réel.

De réels outils de dépannage

Lorsqu'un problème de performances est détecté, seul AirMagnet offre une suite d'outils de dépannage sans fil permettant aux gestionnaires réseaux d'étudier et de résoudre le problème à distance. Un outil de diagnostic des connexions permet d'identifier la cause de n'importe quel problème de connectivité 802.11 ou 802.1x. Les utilisateurs du système peuvent tester à distance des serveurs DHCP et peuvent également tester n'importe quelle liaison du réseau sans fil à distance. Chaque sonde comprend également l'analyseur de réseaux sans fil le plus abouti, permettant d'examiner en profondeur le fonctionnement interne du réseau. Les utilisateurs peuvent bénéficier de n'importe quel niveau de détail avec un décodage de paquet natif. Ils peuvent également enregistrer leurs sessions de dépannage AirMagnet afin de les réutiliser ultérieurement, ou peuvent également enregistrer leurs sessions sous plusieurs formats différents.

Une résolution plus rapide des problèmes

L'interface utilisateur de AirMagnet identifie rapidement le coupable, la nature, le moment, l'endroit et la cause de chaque problème au sein du réseau sans fil. Les équipements les plus problématiques du réseau sont immédiatement exposés via une page de corrélation dédiée qui dresse la liste des équipements menaçants sur la base du nombre et de la gravité des alarmes et des violations. Cela permet de faire la distinction entre les équipements qui sont la cause première d'un problème et les équipements qui sont simplement affectés par ce problème. Les utilisateurs peuvent également suivre les tendances au sein de leurs réseaux à n'importe quel moment, n'importe quel endroit ou selon n'importe quelle politique, à l'aide d'une page de graphiques facilement personnalisable.

Un expert sans fil intégré

AirMagnet Enterprise comprend un système expert de connaissances et de bonnes pratiques liées au sans fil. Chaque politique et chaque alarme est expliquée en détail, y compris les raisons de son importance et les étapes pouvant être mises en oeuvre afin de résoudre le problème. Cela permet de réduire considérablement la formation du personnel technique, et assure un accès rapide aux informations permettant de prendre les meilleures décisions possibles pour le réseau.

Conformité totale aux politiques

AirMagnet Enterprise permet d'aider les utilisateurs à créer, à documenter et à appliquer les politiques sans fil sur la base des besoins liés à leurs activités.

Le système comprend une bibliothèque de profils de politiques préconfigurés adaptées aux besoins spécifiques de l'industrie (gouvernement, santé, vente au détail, logistique, etc.), ainsi que des réglementations telles HIPAA et GLBA. Les politiques peuvent être appliquées à n'importe quel niveau du réseau, à des villes, des immeubles, des étages, des équipements ciblés, ou même à des réseaux locaux virtuels au sein d'un seul équipement.

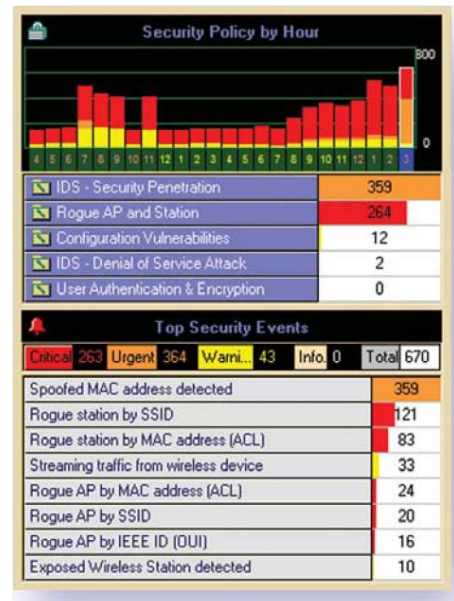
Des rapports de conformité

AirMagnet Enterprise comprend des rapports de conformité détaillés couvrant une grande variété de réglementations comprenant Sarbanes-Oxley, HIPAA, DoD 8100.2, PCI-DSS, FISMA et GLBA. Ces rapports sont liés à chaque section des normes respectives, et offrent une évaluation de chaque équipement et de chaque politique, tout en documentant les éventuelles actions correctives nécessaires.

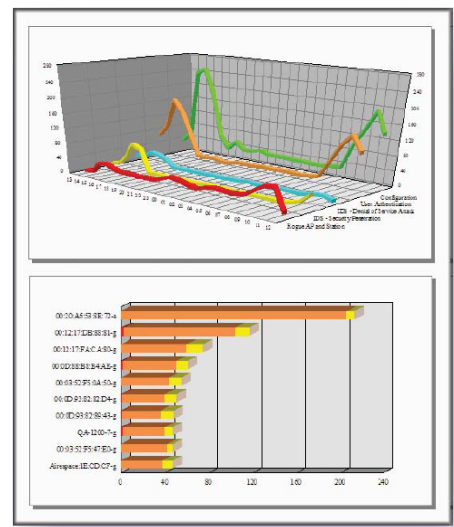
La solution comprend également une bibliothèque de plus de 50 rapports pré-établis couvrant l'ensemble des aspects liés à la sécurité et aux performances des réseaux sans fil. Les rapports peuvent être exportés sous plusieurs formats : PDF, HTML, XML, Ms Word, MS Excel, format txt, etc.

Notification et signalisation

AirMagnet Enterprise fournit des informations ciblées et précises aux ingénieurs réseaux et aux systèmes de supervision, via un système de notification complet. Les notifications comprennent les formats SNMP versions 1, 2 et 3, SysLog, EventLog, la messagerie électronique, le pager, la messagerie instantanée, les SMS, l'impression, etc. Le support RDEP permet à AirMagnet d'être intégré de manière uniforme à d'autres systèmes IDS câblés. Toutes les notifications peuvent être configurées sur la base de seuils d'événements et des alertes individuelles peuvent être envoyées à des destinataires spécifiques. En cas d'aggravation des problèmes, les notifications et les réponses peuvent être automatiquement signalées de manière progressive selon la gravité du problème.



Un suivi facilité des politiques liées au réseau



Une création intégrée de rapports de conformité et de rapports liés aux politiques

L'Architecture SmartEdge

AirMagnet Enterprise repose sur une architecture entièrement révolutionnaire qui offre une variabilité dimensionnelle et une flexibilité jusqu'ici inégalées. Le système se compose de trois éléments – « AirMagnet SmartEdge Sensors », déployé au sein du réseau afin d'analyser vos réseaux sans fil, un serveur « Enterprise » centralisé, qui met en corrélation les événements et s'intègre à d'autres systèmes, et les consoles « Enterprise », qui assurent l'interface utilisateur avec le système.

Des sondes flexibles et intelligentes

Toutes les sondes AirMagnet possèdent des antennes amovibles, et peuvent être personnalisées par l'utilisateur. Des sondes « renforcées » et résistantes aux intempéries permettent de surveiller des environnements extérieurs et hostiles. Les sondes AirMagnet sont également les seules sondes à tolérance de pannes du marché, permettant une analyse Wi-Fi complète, même en cas de coupure du réseau sans fil.

Un déploiement rapide et flexible

« AirMagnet SmartEdge Sensors » supporte le PoE 802.af, et offre une option de zéro configuration « plug-and-play » en vue d'un déploiement simple et rapide. L'option économiseur de câble AirMagnet permet à un commutateur PoE d'alimenter une sonde AirMagnet et un point d'accès actif avec un seul câble Cat5e, éliminant ainsi la nécessité d'un câble supplémentaire.

Une variabilité dimensionnelle et la possibilité d'un serveur de secours

Un seul serveur AirMagnet Enterprise peut supporter des milliers de sondes à distance et peut s'adapter à n'importe quelle taille à l'aide du matériel adéquat. N'importe quel nombre de serveurs peut être surveillé à l'aide d'une seule console AirMagnet, et le système comprend une licence de serveur redondant permettant de bénéficier d'un serveur de secours. Les mises à niveau du système peuvent être planifiées et contrôlées afin de protéger n'importe quelle liaison de réseau sans fil à distance.

L'analyse locale unique de AirMagnet permet de réduire considérablement la bande passante nécessaire entre la sonde et le serveur. Une sonde AirMagnet n'envoie généralement que quelques paquets par seconde (environ 5% de ce qui est constaté avec d'autres sondes).

L'intégration avec AirMagnet Laptop

Les utilisateurs de AirMagnet Enterprise peuvent également recevoir de manière sécurisée des données provenant d'utilisateurs de AirMagnet Laptop sur le terrain. Un AirMagnet Laptop peut être temporairement transformé en sonde distante destinée à être utilisée au sein de la console Enterprise. De la même manière, les utilisateurs situés sur le terrain peuvent télécharger des politiques et des ACL à un emplacement spécifique depuis le serveur Enterprise.

Une intégration en termes de gestion de réseau

AirMagnet s'intègre facilement aux systèmes de gestion de réseaux de niveau plus élevé, via SNMP (y compris la version 3). Les utilisateurs peuvent également synchroniser leurs ACL avec le WLSE de Cisco, et intégrer les alarmes AirMagnet aux systèmes IDS câblés traditionnels, à l'aide du protocole RDEP supporté.

Une gestion de bases de données

AirMagnet Enterprise comprend une licence non restrictive de Microsoft SQL, et supporte également d'autres bases de données telles qu'Oracle 10 et Access (non incluses).

Les utilisateurs peuvent gérer leur base de données directement depuis l'interface utilisateur AirMagnet, et peuvent en outre sauvegarder, restaurer et purger des données de manière sélective.

A propos de AirMagnet

Créée en 2001, AirMagnet, Inc. fournit des systèmes logiciels de sécurité et de gestion de réseaux sans fil à plus de 5000 entreprises à travers le monde.

Pour commander des produits AirMagnet, ou pour obtenir davantage d'informations, contactez :

Avirnet

10 avenue du Québec
91944 COURTABOEUF Cedex

Tél. 33 (0)1 60 92 42 08

www.avirnet.com

