

Protection Avancée contre les Menaces (ATD) Assurée dans le Cloud

Les fonctionnalités brevetées FireSphere bloquent les infections évasives afin de réduire la perte de données

Le développement du cloud computing associé au défi que représente la protection de votre entreprise face aux APT, menaces évasives et perte de données rencontrées aujourd'hui font de la protection avancée contre les menaces une des principales préoccupations dans chaque secteur d'activité. Ainsi que de nombreux cas importants d'atteinte à la protection des données l'illustrent, il est impossible de bloquer la totalité des malwares. Cependant, tandis que la plupart des solutions de sécurité axées sur le cloud affirment assurer une protection APT, elles ne le font que par l'intermédiaire des sièges sociaux. Elles ne peuvent inclure les utilisateurs mobiles et à distance sans faire transiter les données et créer de latence, ou laisser les utilisateurs mobiles non protégés. Seule la protection APT iboss FireSphere™ assure les fonctionnalités ATD directement vers le cloud, sécurisant tous vos utilisateurs à distance et itinérants sans la nécessité de faire transiter les données. Sans matériel ni logiciel à déployer et entretenir, la solution ATD iboss Cloud ATD permet de réduire les dépenses générales tout en améliorant la protection contre les menaces avancées et la perte de données.

L'avantage iboss

Assure la protection avancée contre les menaces dans l'ensemble de votre organisation, sur tout appareil, à tout endroit et à tout moment

- ✓ Inclut une sandbox d'analyse comportementale permettant de détecter et bloquer les malwares polymorphes avant qu'ils ne pénètrent le périmètre du réseau
- ✓ Combine une protection inégalée contre les malwares sans signature ainsi qu'une détection des infections sur tous les sites et pour tous les utilisateurs en quelques minutes, sans transit des données
- ✓ Différentes options de cloud proposées, privées ou publiques, apportant une certaine flexibilité aux entreprises qui sont limitées par la conformité aux réglementations ou qui préfèrent une solution sur site
- ✓ Fait appel au global sourcing des menaces transmises dans le cloud afin de livrer des informations scientifiques sur les malwares au moyen du Centre de Commandement exclusif CISO et des Informations sur les Menaces dans le Cloud
- ✓ Détecte les malwares préalablement inconnus ou non classés se trouvant dans votre réseau avec la surveillance brevetée d'anomalie des données, augmentant ainsi la capacité de votre entreprise à détecter les programmes malveillants les plus dangereux
- ✓ Réduit la perte des données au cours d'une attaque, tout en raccourcissant le délai de réponse aux incidents avec exfiltration des données et technologie de confinement, apportant ainsi une visibilité sur tous les vecteurs de menace
- ✓ Réduit les journaux d'événements brouillés en regroupant les événements en incidents pour obtenir davantage de renseignements exploitables, raccourcissant ainsi le délai de réponse aux incidents avec le Centre de Commandement CISO intégré
- ✓ Scanne et sécurise tous les ports et protocoles, augmentant ainsi votre capacité à détecter et bloquer les menaces évasives pour les ports telles que qui tire parti du réseau TOR
- ✓ Fournit davantage d'options pour gérer le trafic SSL que toute autre solution, augmentant ainsi la capacité de votre entreprise à détecter les menaces dans l'ensemble du trafic crypté, même en ce qui concerne le BYOD et l'accès Wifi aux visiteurs

iboss ATD Sécurise la totalité des emplacements et appareils en quelques minutes, sans faire transiter les données, réduisant les dépenses CAPEX et OPEX

- ✓ Sécurisez une grande société répartie en quelques minutes sans avoir à faire transiter de données
- ✓ Évitez les équipements matériels coûteux et gourmands en ressources, lesquels requièrent un entretien constant et des mises à niveau régulières pour rester actualisés
- ✓ Élargissez ou réduisez votre plan selon les besoins de votre entreprise, payez uniquement pour les services dont vous avez besoin
- ✓ Abaissez le coût total de propriété (TCO) et conservez vos ressources informatiques actuelles, sans aucun matériel ou logiciel à acheter, gérer ou entretenir
- ✓ Combinez votre besoin de contrôle local avec la flexibilité et l'évolutivité d'une solution de sécurité informatique externalisée avec l'option iboss Private Cloud



La plateforme iboss Cloud se déploie instantanément pour apporter la dernière technologie brevetée directement vers le cloud, y compris nos fonctionnalités exclusives de protection avancée contre les menaces. iboss présente des options pour le Cloud Public et Privé, vous offrant ainsi une flexibilité maximum pour satisfaire aux exigences de votre entreprise:

Public Cloud – Une conteneurisation unique garantit que vos données ne sont jamais mélangées avec les données d'une autre entreprise.

Private Cloud – Déployez des détecteurs locaux pour certaines fonctions, tout en redirigeant les bureaux à distance et les utilisateurs itinérants directement vers le cloud, sans faire transiter les données et sans latence.

Descriptions des Fonctionnalités

Sandbox d'Analyse Comportementale Distribuée

La Sandbox d'Analyse Comportementale iboss analyse les fichiers suspects en les exécutant dans un environnement isolé pour observer leurs comportements. Elle utilise une combinaison de règles et de méthodes heuristiques afin de déterminer si un fichier s'avère une menace ou non et fournit des informations spécifiques concernant les comportements et le contexte de cette menace. Inclut les fonctionnalités suivantes:

- ✓ **La consigne automatique** des fichiers suspects
- ✓ **Le déploiement partagé dans le cloud** permet un équilibrage à chargement automatique afin que plusieurs instances puissent s'exécuter sur **un seul réseau, sans latence**
- ✓ **La configuration sur mesure** vous permet de configurer vos propres machines virtuelles (VM) personnalisées et d'observer les comportements d'un fichier dans des environnements multiples tels que Windows XP, Windows7, etc.
- ✓ **L'intégration de rapports** avec la Console des Menaces et des Événements iboss permet l'analyse détaillée le signalement instantané
- ✓ **La consigne manuelle** d'un fichier dans la sandbox pour analyse

La Surveillance des Anomalies de Réseau

iboss FireSphere tire parti de la visibilité totale des flux Web dans l'ensemble des canaux de données, tant entrants que sortants, pour surveiller le trafic en continu, détecter les anomalies et bloquer les transferts de données suspects afin de réduire la perte des données. Inclut les fonctionnalités suivantes:

- ✓ **La visibilité totale des flux Web et l'indexage dynamique** pour un accès aux historiques des registres de données et la création de bases de référence du trafic normal
- ✓ **La surveillance continue** dans une large gamme de paramètres dont le décompte des connexions, la destination, le débit entrant et sortant et les déviations du trafic afin d'identifier un comportement inhabituel pouvant indiquer que le réseau est compromis
- ✓ **Le confinement automatique des transferts de données et le signalement** lorsqu'un problème est découvert, vous laissant ainsi le temps d'investiguer et de remédier avant l'apparition d'une perte des données

Le Centre de Commandement CISO

FireSphere élimine les interférences et les faux positifs en transmettant des messages d'alerte indiquant quelles machines ont besoin de mesures correctives et pourquoi. Inclut les fonctionnalités suivantes:

- ✓ Met en corrélation les informations d'alertes vers le nom de l'utilisateur ou de la machine du répertoire, accompagné d'un instantané d'un historique de l'ensemble des infections
- ✓ Élimine les interférences et réduit les faux positifs avec une analyse scientifique approfondie et en temps réel
- ✓ Établit les priorités relatives à la gravité des menaces en regroupant les données de millions de paramètres globaux et en dirigeant les générateurs de malwares
- ✓ Détecte les malwares évasifs déjà présents sur le réseau en surveillant et en cartographiant les rappels d'infection
- ✓ Vaccine contre les futures attaques en identifiant les alias IP et les fichiers malveillants hébergés

Informations sur les Menaces dans le Cloud

Les Informations sur les Menaces dans le Cloud analysent la façon globale d'agir d'une menace et les schémas qu'elle affiche, ce qui peut permettre de déterminer son comportement futur et vous donner le contexte complet dont vous avez besoin pour remédier rapidement aux problèmes sans devoir faire face aux interférences et faux positifs générés par les autres solutions.

Pour plus d'informations:

iboss Cloud Platform Data Sheet

iboss Secure Web Gateway Platform Data Sheet

À Propos d'iboss Cybersecurity

iboss Cybersecurity protège les réseaux complexes et répartis, répandus de nos jours, contre les APT et les menaces ciblées qui entraînent une perte des données avec la Plateforme Web Gateway Sécurisée nouvelle génération iboss, en tirant parti d'une architecture cloud innovante et de technologies brevetées de protection avancée contre les menaces. Pour plus d'informations, veuillez visiter notre site: www.iboss.com.