Mil' Services

Informatique

Notre solution de supervision système

Monitoring / Sécurité / Backup

La solution RG System embarque sur une interface unique toutes les fonctionnalités de Remote Monitoring & Management dont vous avez besoin ! Alerting, ticketing, accès à distance, audit de parc, automatisation etc. Nous avons toutes les cartes en main pour être performant dans la supervision et la gestion du parc de nos clients !

L'interface SaaS RG System nous offre une vision à 360° de l'état de santé des machines supervisées. Procéder à des audits logiciels et matériels devient un jeu d'enfant ! Nous sommes en mesure d'intervenir rapidement et à distance si un incident est détecté grâce à des alertes mails et/ou SMS reçues en 24/7. Ces alertes sont alors transformées en tickets d'incident afin de permettre à nos équipes de suivre efficacement la résolution du problème. Et parce que nous avons besoin de communiquer sur la qualité de votre travail auprès de nos clients. Des rapports d'activité personnalisables peuvent être envoyés directement par mail aux destinataires choisis !

Le contrôle à distance un point central de votre offre de maintenance

Un incident est détecté, nous avons que très peu de temps pour intervenir et éviter la rupture d'activité. Avec RG System, nous assurons une maintenance rapide et efficace grâce aux outils de prise de main à distance mis à disposition directement depuis l'interface web. Notre fonctionnalité propriétaire Native Remote Control ou LogMeIn Pro.

Automatisez la résolution d'incident et focalisez-vous sur des actions à plus forte valeur ajoutée

Basée sur la technologie propriétaire ReactEngine™ développée par les équipes RG System, la fonctionnalité Automatisation nous permet de paramétrer des actions curatives suite à la détection d'un ou plusieurs incidents, et ainsi permettre leur résolution automatique.

Mieux vaut patcher que guérir

L'arborescence multi-tenante RG System vous permet, en un seul clic, de déployer des mises à jours Windows et des applications tierces sur toutes les machines des parcs gérés. Vous gagnez ainsi un temps précieux dans la protection de vos clients, notamment en ces temps troubles où ransomwares et cryptolockers font partie de notre quotidien. C'est vraiment aussi simple que cela !

Bitdefender

Avec Bitdefender Cloud Security avec une seule console nous pouvons fournir à toutes les couches de sécurité des terminaux de nos clients la meilleure protection contre les attaques de sécurité avancées et ciblées. Cloud Security inclut Antivirus et Antimalware, Anti Exploit, Advanced Machine Learning, Content Control et Device Control. En outre, ce service cloud peut être étendu avec des services de sécurité supplémentaires facultatifs.

Local & Cloud Signature and Machine Learning

Local & Cloud signature est utilisée pour identifier les menaces, tandis que les algorithmes avancés d'apprentissage automatique permettent de prédire et d'identifier les menaces inconnues avant leur exécution.

Pare-feu avec Détection d'Intrusions

Protégez les terminaux contre les attaques potentielles à l'intérieur et à l'extérieur du réseau avec un pare-feu bidirectionnel et une Détection des Intrusions.

Anti-Exploit

Les exploits sont souvent impliqués dans de grandes attaques de ransomware, car ils détournent des applications légales pour compromettre le système. Advanced Anti-Exploit détecte les exploits inconnus sur la base de fichiers ou sans fichiers (uniquement en mémoire) en mettant l'accent sur les techniques d'attaque et de l'utilisation des techniques comportementales, au lieu des signatures des exploits déjà connus.

Suivi des processus

Le Process Inspector surveille en permanence les processus d'exploitation pour détecter les signes de comportement malveillant. Sur la base de ces signes, le Process Inspector peut bloquer les attaques qui ont échappé à d'autres couches de protection.

Gestion et analyse des risques encourus par les endpoints (console)

Bitdefender Endpoint Risk Analytics présente un score de risque basé sur les paramètres des appareils de notre client en ce qui concerne la sécurité du navigateur, du réseau, des informations d'authentification, et du système d'exploitation tout en tenant compte des vulnérabilités des applications.

Nous disposons ainsi d'une visibilité continue sur la posture de sécurité de leurs clients et peuvent comparer les risques selon les entreprises ou sur la durée pour montrer les améliorations ou assurer la conformité réglementaire.

Pour limiter les risques et réduire la surface d'attaque, il est possible de procéder à une analyse descendante pour détecter les problèmes de configuration et les corriger. Environ 90 % des corrections peuvent être appliquées automatiquement et, si vous utilisez Bitdefender Patch Management, nous pouvons également appliquer les patchs manquants depuis la même fenêtre, en toute simplicité.

Prévention contre les menaces avancées ATS

Une prévention automatisée efficace contre les attaques avancées est essentielle pour éviter les violations et limiter l'examen manuel des incidents.

Les technologies suivantes, disponibles dans l'extension Bitdefender Advanced Threat Security (ATS), ont été conçues spécialement pour détecter les menaces les plus discrètes et les bloquer avant qu'elles ne puissent être nuisibles :

- Le Machine Learning personnalisable d'HyperDetect bloque les attaques avancées dès la préexécution avec un ensemble d'algorithmes avancés de ML que vous pouvez configurer pour être plus agressif en mode « bloquer » ou « rapport uniquement ».

- Fileless Attack Defense analyse le code de commande en mémoire et bloque rapidement les attaques sans fichier ou par script s'appuyant sur des outils tels que PowerShell ou l'invite de commande.

- Sandbox Analyzer détone automatiquement ou manuellement les fichiers ou scripts suspects pour fournir un verdict et une visibilité totale sur le contexte de la menace et les modifications qu'un élément tente d'apporter.

Solution de détection et de réponse dédiée aux endpoints (EDR)

Même les meilleurs niveaux de durcissement et de prévention n'empêchent pas les attaquants et les menaces internes d'accéder aux infrastructures des fournisseurs de services ou des clients. Il devient donc essentiel de détecter et d'arrêter tout comportement dangereux avant qu'il ne se transforme en coûteuse violation de données, et de bénéficier d'une visualisation complète de l'attaque pour détecter les lacunes de sécurité, ou présenter l'impact d'un incident dans les audits de conformité.

Avec ses technologies intégrées de Machine Learning et d'analyse comportementale perfectionnées depuis 2009, Bitdefender EDR fournit plus de détections exploitables que n'importe quelle autre solution comme le prouvent les tests MITRE 2020. Nous minimisons notre charge opérationnelle avec plus d'informations contextuelles, des technologies supplémentaires pour filtrer les fausses alertes, des incidents classés par ordre de priorité, une investigation guidée et des mesures de réponse.

Pour les entreprises dont la sécurité actuelle des endpoints ne fournit pas la réponse et la visibilité nécessaires face aux attaques avancées, l'ajout de Bitdefender EDR est une manière rapide et efficace de renforcer la sécurité. Il est recommandé de compléter l'EDR avec les systèmes de durcissement et AV Next-Gen de Bitdefender pour bloquer automatiquement la plupart des menaces avant leur exécution, limiter les risques de violations de données et simplifier l'administration de la sécurité.

Acronis

sauvegarde et récupération de données

SOLUTIONS PETITES, MOYENNES ET GRANDES ENTREPRISES

Acronis Backup 12.5 offre la protection des données la plus simple et la plus rapide au monde. Backup 12.5 est la solution la plus complète pour protéger les données avec la sauvegarde la meilleure et la plus rapide. Une sauvegarde d'Acronis est 26% plus rapide que celle des concurrents les plus proches. Que les données soient maintenant sur site, stockées dans un cloud privé ou public ou sur des appareils mobiles.

Acronis Backup 12.5 offre diverses fonctionnalités innovantes qui permettent d'automatiser la protection des données. Cette solution assure moins d'actions manuelles, vous permettant de travailler plus efficacement. Gérez et surveillez toutes les activités depuis un appareil avec la console web Acronis. Cet outil de surveillance montre toutes les activités dans une vue générale.

Acronis Backup 12.5 permet à votre organisation de fonctionner en cas de problèmes ou de catastrophe grave. Backup 12.5 protège les données de manière proactive pour éviter les temps d'arrêt et restaure les données en quelques secondes. Acronis Backup 12.5 sauvegarde les données aussi souvent que vous le souhaitez, sans affecter les performances.

Acronis Backup 12.5 est disponible pour divers systèmes, serveurs, périphériques, applications et solutions cloud.