eBOOK

eBook : EDR vs. AV : ce qu'il faut savoir

Introduction

La sécurité multicouche est le modèle le plus efficace pour protéger les réseaux et les utilisateurs des menaces actuelles et futures. Elle met en avant deux types de solutions pour la sécurité des points de terminaison : les antivirus (AV) et les outils EDR (Endpoint Detection and Response). Les deux offrent des avantages. Comment donc faire votre choix ? Les outils EDR vont-ils remplacer les antivirus traditionnels ? Pour en savoir plus, nous vous invitons à poursuivre la lecture de cet eBook.

L'un ou l'autre—mais pas les deux

Un antivirus et un outil EDR se disputent l'utilisation des ressources, ce qui peut entraîner des problèmes si les deux sont exécutés en même temps. Pour cette raison, nous recommandons de ne pas utiliser à la fois un antivirus et un outil EDR sur un point de terminaison. Il est préférable de choisir l'un ou l'autre pour chaque terminal.

Lors de ce choix, il est important de prendre en compte plusieurs facteurs, tels que le type d'entreprise à protéger, les utilisateurs concernés et le coût. Certains clients peuvent avoir besoin de l'un ou de l'autre pour l'ensemble de leur base d'utilisateurs. D'autres peuvent stratégiquement déployer un outil EDR pour certains utilisateurs et utiliser un antivirus pour les autres. C'est pourquoi SolarWinds MSP propose les deux.

Antivirus : une protection solide à un prix abordable

Un antivirus protège vos clients contre les logiciels malveillants. SolarWinds® RMM vous permet de gérer la protection antivirus de vos clients de manière centralisée, à partir d'un seul tableau de bord, en parallèle d'autres couches de sécurité. Vous gérez les mises à jour automatiques du programme et des définitions de virus pour vos clients—sans nécessiter aucune intervention de la part des utilisateurs. Lorsqu'un virus ou un logiciel malveillant est détecté, il est immédiatement placé en quarantaine. Les antivirus sont une protection courante depuis de nombreuses années. La plupart des utilisateurs connaissent leur rôle, ce qui facilite leur vente.

Les bases de signatures (ou définitions de virus) doivent néanmoins être mises à jour régulièrement. C'est là qu'est le problème. La qualité de protection offerte par le programme dépend essentiellement de la réactivité du fournisseur. De nouvelles menaces apparaissent quotidiennement. Pour éviter qu'elles ne soient découvertes une fois les dommages causés, il est essentiel de disposer des mises à jour en temps opportun.

Le champ d'action des antivirus est par ailleurs limité aux virus et aux logiciels malveillants. Les terminaux sont néanmoins exposés à des menaces qui vont au-delà des virus. C'est le cas des attaques sans fichiers, de plus en plus fréquentes et indétectables par les antivirus. Les cybercriminels ont également recours à des techniques d'évasion pour contourner les antivirus. Par exemple, ils utilisent des packers pour chiffrer les logiciels malveillants et les rendre difficiles à intercepter, ou ils développent des logiciels malveillants capables de modifier leur signature à une cadence définie afin de ne pas être détectés par les bases de signatures existantes. En fin de compte, les antivirus sont un palmarès de menaces que les cybercriminels s'efforcent de dépasser depuis des années. Cela ne veut en aucun cas dire que les antivirus sont impuissants (de nombreux fournisseurs offrent toujours une excellente couverture englobant de nombreuses menaces), mais des lacunes sont à prendre en compte.

Malgré les problèmes évoqués, pourquoi choisir de déployer un antivirus managé ? Tout d'abord, les antivirus fournissent une protection contre les cybermenaces. Ils restent donc utiles pour les utilisateurs finaux. De plus, le fait que vous gériez la protection antivirus de vos clients leur évite d'avoir à s'en soucier eux-mêmes. La principale raison de choisir un antivirus managé reste probablement le coût. Le prix par utilisateur d'un antivirus managé est inférieur à celui d'un outil EDR. Les clients soucieux de leurs dépenses sélectionneront donc l'antivirus. Notez cependant que vos marges sur la vente d'antivirus peuvent diminuer. Par ailleurs, comme nous le verrons dans la section suivante, l'investissement initial dans une solution EDR peut valoir la peine par rapport aux coûts d'une attaque ou d'une violation de données.

Parmi les autres avantages de l'antivirus managé dans SolarWinds RMM :

- **Une seule source de gestion :** le MSP est l'interlocuteur unique du client pour le déploiement, la gestion, la mise à jour des définitions et les rapports sur les menaces. Il développe avec son client une relation de confiance, ce qui peut lui permettre de générer des revenus supplémentaires dans d'autres domaines.
- **Sécurité « verrouillée » :** des stratégies empêchent toute intervention de l'utilisateur final. Impossible de forcer l'installation d'une mise à jour ou de désinstaller le programme sans disposer des droits d'accès appropriés. Cela évite les menaces internes (utilisateurs qui tentent d'installer des logiciels malveillants), les suppressions accidentelles ou les manipulations inappropriées du logiciel antivirus.
- **Supervision facile :** vous programmez les analyses, mettez à jour le logiciel et déployez les mises à jour des définitions. Là encore, aucune intervention des clients/utilisateurs finaux n'est nécessaire.

Ces avantages s'appliquent également à un outil EDR, mais le prix d'un antivirus reste inférieur.

EDR : la sécurité des points de terminaison élevée au rang supérieur

L'EDR est une fonctionnalité multidimensionnelle qui porte les capacités de l'antivirus à un niveau supérieur—pour une plus grande sécurité et (surtout) une plus grande tranquillité d'esprit. Comme pour l'antivirus, les MSP gèrent l'EDR sans nécessiter aucune intervention de l'utilisateur final. Face aux nouvelles menaces qui apparaissent quotidiennement, la gestion d'un grand nombre de terminaux peut être plus difficile avec un antivirus ou d'autres solutions ponctuelles. C'est là que l'EDR prend tout son sens.

Une solution EDR se concentre sur la protection des terminaux et détecte des menaces qui vont au-delà des logiciels malveillants. Au lieu d'analyser uniquement les fichiers, l'EDR fait appel à un logiciel de supervision, des agents sur les terminaux, un apprentissage automatique intégré et une intelligence artificielle avancée (IA) pour identifier les comportements suspects et les traiter avant qu'ils ne soient reconnus comme dangereux.

Même si un antivirus excelle dans la détection des logiciels malveillants, les cybercriminels peuvent attaquer les points de terminaison sans utiliser de fichiers. Par exemple, si un pirate informatique trouve un port RDP ouvert, il peut utiliser cette vulnérabilité pour créer un utilisateur avec des droits d'administration sur une machine, rester caché et apporter des modifications sur le point de terminaison sans que le MSP ou l'administrateur informatique ne s'en aperçoivent (jusqu'à ce qu'il soit trop tard). Un antivirus traditionnel n'est pas conçu pour bloquer ce type d'attaque. Imaginons que plusieurs fichiers soient modifiés en même temps sur un point de terminaison (ce qui n'est pas habituel). Les solutions EDR peuvent signaler ce comportement, alerter l'administrateur et lui permettre d'agir. Au-delà de cela, une solution EDR contribue à lutter contre les menaces émergentes, qui n'ont pas encore été découvertes par la communauté de la sécurité informatique au sens large. Un logiciel antivirus basé sur des signatures laisse un vide dans ce domaine, contrairement à l'approche sans signatures d'une solution EDR.

Lorsque vous utilisez SolarWinds® Endpoint Detection and Response (EDR), le traitement est effectué en local sur le point de terminaison (contrairement à d'autres fournisseurs EDR qui nécessitent des ressources et des téléchargements longs sur le Cloud pour l'analyse et le traitement des menaces). Vous pouvez détecter les menaces plus rapidement, et bénéficier de restaurations automatisées.

Gérer les dommages causés par une menace ne suffit pas—vous devez vous demander comment et pourquoi le point de terminaison a été touché. Une solution EDR excelle dans ce domaine, car elle assure une analyse active des causes profondes. SolarWinds EDR fournit un véritable contexte via un « scénario visuel ». Vous pouvez voir quel processus a engendré l'attaque, mais

aussi comment il s'est reproduit et propagé. Vous obtenez des réponses sur la façon dont la menace est construite, ainsi que des informations exploitables sur lesquelles vous appuyer pour améliorer la sécurité de vos clients.

Le scénario se déroule en temps réel lorsqu'une attaque se produit, mais EDR vous offre toutes les défenses nécessaires. Ses options incluent l'élimination, la mise en quarantaine et la correction (restauration)—en fonction de la configuration appliquée sur l'agent pour chaque utilisateur final. Considérez l'agent EDR comme votre analyste SOC (Security Operations Center) personnel. Vous pouvez littéralement réparer les dommages causés, et rendre les ransomwares inutilisables.

Tel que nous l'indiquions précédemment, le prix par utilisateur d'un antivirus est moins élevé. Si cela semble vrai à première vue, il ne faut pas oublier qu'une protection moins puissante peut avoir de lourdes conséquences. Les attaques de ransomwares représentent bien plus que de simples nuisances—vous devez prendre en compte la perte de productivité, le coût de restauration des points de terminaison, l'atteinte à la réputation liée aux temps d'arrêt, et les amendes qui peuvent découler du non-respect des lois sur la confidentialité des données. Ces coûts peuvent largement dépasser l'investissement initial. Face à des menaces de plus en plus dangereuses et coûteuses, l'EDR deviendra probablement la norme.

Pour résumer, les solutions EDR offrent les mêmes avantages que les antivirus, avec en plus :

- **Une détection proactive :** alors que les solutions antivirus nécessitent des mises à jour de signatures et des analyses planifiées, les solutions EDR utilisent l'intelligence artificielle (IA) et l'apprentissage automatique pour détecter les menaces potentielles, et évitent ainsi les lacunes en matière de protection.
- **Une protection plus large :** en plus de détecter les virus et les logiciels malveillants, une solution EDR offre une protection contre le trafic suspect et les attaques sans fichiers.
- **Une analyse approfondie des causes :** SolarWinds EDR propose un scénario visuel pour tous les comportements suspects. Cela vous donne un meilleur aperçu de l'attaque et vous permet d'adapter les processus et les contrôles de sécurité afin d'éviter que le problème ne se reproduise.
- **Une correction rapide :** vous pouvez corriger les menaces en un instant. Par exemple, s'il s'agit d'un ransomware, vous pouvez restaurer un point de terminaison à son dernier état fonctionnel directement à partir de la solution EDR.

SolarWinds RMM et la fonctionnalité EDR intégrée

SolarWinds RMM propose un antivirus managé et la fonctionnalité SolarWinds EDR à partir du même tableau de bord Web. SolarWinds EDR utilise l'intelligence artificielle et l'apprentissage automatique pour détecter les menaces, et corrige ces menaces en fonction des stratégies définies. Cet outil permet également de restaurer un point de terminaison à son dernier état fonctionnel connu après une attaque, ce qui permet à vos clients d'économiser beaucoup de temps et d'argent et d'éviter de nombreux problèmes en cas de ransomwares.

Avec l'intégration de la fonctionnalité SolarWinds EDR dans RMM, vous pouvez désormais offrir à vos clients une détection améliorée des menaces, une supervision et une correction rapide à partir de la même interface que celle utilisée pour superviser et gérer le reste de leur infrastructure informatique. D'autres couches de sécurité intégrées, telles que la gestion des mises à jour, la protection de la messagerie, la protection Web et la sauvegarde, vous permettent de renforcer la protection de vos clients sans surmener vos équipes.

Pour en savoir plus sur l'intégration de SolarWinds EDR dans SolarWinds RMM, consultez cette page : https://www.solarwindsmsp.com/fr/produits/remote-management/endpoint-detection-and-response

À PROPOS DE SOLARWINDS

SolarWinds (NYSE:SWI) est un acteur majeur dans l'offre de logiciels de gestion d'infrastructures informatiques performants et abordables. Nos produits permettent aux organisations du monde entier, quels que soient leur type, leur taille et la complexité de leurs infrastructures, de superviser et de gérer les performances de leurs environnements sur site, dans le Cloud ou hybrides. Nous travaillons en permanence avec tous les types de spécialistes des technologies — professionnels des opérations informatiques, professionnels DevOps, fournisseurs de services gérés (MSP) — afin de comprendre les défis auxquels ils font face pour maintenir la disponibilité et les performances de leurs systèmes à un niveau élevé. Les informations tirées de ces échanges, via notre communauté en ligne THWACK par exemple, nous permettent de concevoir des produits répondant à des problématiques de gestion informatique bien comprises, de la manière attendue par les spécialistes du secteur. En plaçant l'utilisateur au centre de son activité et en visant l'excellence dans la gestion des performances informatiques hybrides de bout en bout, SolarWinds est devenu un leader mondial des logiciels de gestion de réseau et des solutions MSP. Pour en savoir plus, consultez le site solarwinds.com/fr.

solarwinds

Pour plus d'informations, veuillez contacter SolarWinds à l'adresse sales@solarwinds.com.
Pour trouver un revendeur proche de chez vous, visitez le site : http://www.solarwinds.com/partners/reseller_locator.aspx