Antivirus vs EDR

décembre 20, 2021
by SentinelOne

Pendant des décennies, les entreprises ont investi dans des antivirus dans l'espoir de résoudre leurs problèmes de sécurité. Mais la sophistication et la prévalence des malwares n'ayant cessé d'augmenter ces dix dernières années, les limites des antivirus traditionnels sont devenues évidentes. Certains fournisseurs ont donc proposé une alternative moderne pour les remplacer : l'EDR (Endpoint Detection and Response).

Mais, en quoi les solutions EDR diffèrent-t-elles des antivirus traditionnels ? Comment et pourquoi sont-elles plus efficaces face aux menaces d'aujourd'hui ?

Caractéristiques d'une solution antivirus

À l'époque où les malwares pouvaient être facilement comptabilisés sur une simple feuille excel, les antivirus next-gen permettaient aux entreprises de détecter et d'éradiquer les virus présents sur les endpoints, et de prendre des mesures pour les empêcher de nuire. La méthode d'un antivirus consiste à analyser le disque dur à la recherche de la signature du virus présent dans la base de données du logiciel, si celui-ci est à jour et s'il connaît ce malware.

Aujourd'hui, il existe de nombreuses raisons pour lesquelles les solutions antivirus ne peuvent pas faire face aux menaces actuelles. Tout d'abord, le nombre de logiciels malveillants détectés quotidiennement est supérieur à celui qu'une équipe de sécurité est capable de gérer.

Deuxièmement, la détection par la signature peut souvent être contournée par les hackers, sans qu'ils n'aient à réécrire leur malware. En effet, les signatures ne se concentrent que sur quelques caractéristiques, les cybercriminels ont donc appris à créer des logiciels malveillants, dits polymorphes, dont la signature change à chaque réplication. Les hachages de fichiers, par exemple, sont parmi les caractéristiques les plus faciles à modifier, mais les chaînes internes peuvent également être *randomisées*, indiscernables et cryptées différemment à chaque nouvelle version du logiciel malveillant.

Troisièmement, les hackers motivés par l'argent, tels que les opérateurs de ransomware, ont dépassé les simples attaques de malwares basés sur des fichiers. Les attaques en mémoire ou fileless, les ransomwares à commande humaine tel que Hive ou les attaques à « double extorsion » comme Maze, Ryuk etc…peuvent conduire à une compromission et à une perte de la propriété intellectuelle par exfiltration de données sans jamais déclencher une détection basée sur une signature antivirus.

Face à l'augmentation des menaces et au manque d'efficacité des antivirus, certains fournisseurs ont donc essayé de les compléter par d'autres services tels que le contrôle de firewall, le cryptage de données, des listes d'autorisation et de blocage des processus et autres outils. Connues sous le nom générique de « EPP » (ou Endpoint Protection Platforms), ces solutions restent, néanmoins, fondées sur une approche par signature.

Caractéristiques d'une solution EDR

Alors que toutes les solutions antivirus se concentrent sur les fichiers, potentiellement malveillants, présents dans le système, un outil EDR s'appuie sur la collecte et l'analyse des données à partir d'un endpoint pour détecter en temps réel les fichiers anormaux. Comme son nom l'indique, l'EDR a été inventé pour détecter une infection et lancer une réponse. Plus le système est rapide et sans intervention humaine, plus il est efficace.

Une solution EDR efficace intègre également des capacités de blocage des fichiers malveillants, mais il est important qu'elle reconnaisse que toutes les attaques modernes ne sont pas basées sur des fichiers. En outre, les EDR proactifs offrent aux équipes de sécurité une réponse automatisée et une visibilité approfondie des modifications de fichiers, des créations de processus et des connexions réseau qui ont eu lieu sur le endpoint que l'on ne trouve pas dans les antivirus.

Le système EDR est bien mieux conçu pour faire face aux cybercriminels d'aujourd'hui. En se concentrant sur la détection d'une activité inhabituelle et en fournissant une réponse, l'EDR ne se limite pas à la détection des menaces connues, basées sur des fichiers. Une solution EDR peut rechercher des schémas d'activité anormaux, inhabituels et indésirables et émettre une alerte afin qu'un analyste de sécurité enquête.

De plus, comme les outils EDR fonctionnent en collectant un large éventail de données provenant de tous les terminaux protégés, ils offrent aux équipes de sécurité la possibilité de visualiser ces données dans une interface pratique et centralisée. Les équipes informatiques peuvent intégrer ces données à d'autres outils pour une analyse plus approfondie et contribuer ainsi à faire évoluer la stratégie de sécurité de l'entreprise tout en définissant la nature des futures attaques potentielles. Les données complètes fournies par un système EDR peuvent également permettre une recherche et une analyse rétrospectives des menaces.

L'un des plus grands avantages d'un EDR avancé est sa capacité à contextualiser les données issues de chaque endpoint et à atténuer la menace sans intervention humaine. Cependant, tous les EDR ne sont pas capables de le faire, car beaucoup d'entre eux transmettent les données EDR au cloud pour une analyse à distance (et donc différée).

Et l'Active EDR, c'est quoi ?

Les solutions EDR offrent aux équipes de sécurité une visibilité optimisée sur tous les terminaux du réseau de leur entreprise. Malgré cela, nombre d'entre elles n'ont pas l'impact escompté, car leur gestion exige beaucoup de ressources humaines.

Plutôt que de bénéficier d'une meilleure sécurité et d'un allègement de la charge de travail de leurs équipes sécurité, de nombreuses entreprises, ayant investi dans l'EDR, sont contraintes de réaffecter des ressources d'une tâche de sécurité à une autre. Elles disposent de moyens limités pour mettre en corrélation et hiérarchiser une multitude d'alertes, tout en éprouvant des difficultés pour identifier rapidement et efficacement les dispositifs infectés.

En exploitant la puissance de l'apprentissage automatique et de l'intelligence artificielle, l'Active EDR peut décharger l'équipe SOC et atténuer de manière autonome les événements sur les endpoints sans dépendre des ressources cloud.

Au-delà de l'EDR, le XDR pour une visibilité et une intégration optimales

Si la solution Active EDR est la prochaine étape pour les entreprises qui n'ont pas encore dépassé le stade de l'antivirus, celles qui ont besoin d'une visibilité et d'une intégration optimales sur l'ensemble de leur parc, doivent envisager la solution Extended Detection and Response, ou XDR.

Le XDR est le successeur intelligent de l'EDR. Il intègre tous les contrôles de visibilité et de sécurité dans une vision holistique de l'environnement d'une entreprise. Avec un pool unique de données brutes comprenant des informations provenant de l'ensemble de l'écosystème, le XDR permet une détection et une réponse aux menaces plus rapides, plus approfondies et plus efficaces que l'EDR, en collectant et en rassemblant des données provenant d'un plus grand nombre de sources.

Les hackers ont depuis longtemps dépassé le stade de l'antivirus et de l'EPP et les entreprises doivent considérer que ces solutions ne sont plus à la hauteur des menaces d'aujourd'hui. Un simple coup d'œil aux médias démontre que de nombreuses grandes entreprises, ayant pourtant investi dans des contrôles de sécurité, sont prises au dépourvu par des attaques modernes telles que les ransomwares. Il incombe aux éditeurs de solutions de sécurité, de veiller à ce que leurs logiciels soient adaptés non seulement aux attaques d'hier, mais aussi à celles d'aujourd'hui et de demain.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Cybersécurité : à quoi doit-on s'attendre en 2022 ?
- Cybersécurité : les huit contre-vérités que les RSSI entendent trop souvent
- Guerre en Ukraine : impact des cyberattaques et conseils aux RSSI
- Dix idées reçues sur la sécurité de macOS qui font courir des risques aux entreprises