EPP et EDR – une protection complète en parfaite symbiose

Les solutions traditionnelles de protection des endpoints (EPP) ne suffisent pas pour se défendre contre les cybermenaces complexes. Seule une combinaison de mécanismes classiques de protection des endpoints avec des technologies modernes de détection et de réponse (EDR) offre le niveau de protection nécessaire.

Pratiquement toutes les entreprises sont confrontées à des cybermenaces de plus en plus difficiles. Chaque jour, des centaines de milliers de nouveaux virus, chevaux de Troie et autres codes malveillants sont découverts. En outre, les méthodes d'attaque deviennent de plus en plus sophistiquées et complexes, comme les attaques «zero-day» qui exploitent la fenêtre temporelle entre l'apparition d'un nouveau virus et le développement d'un antidote, ou les attaques ciblées sur des employés spécifiques et les Advanced persistent Threats qui infiltrent le réseau de l'entreprise et causent des dommages à long terme. Ces menaces avancées peuvent, par exemple, chiffrer des documents importants pour extorquer une rançon, ou accéder à des données confidentielles à des fins d'espionnage industriel.

L'antivirus ne suffit plus

Les solutions traditionnelles de protection des endpoints qui reposent sur la prévention, les fichiers de signature et les algorithmes heuristiques offrent une bonne protection contre les logiciels malveillants connus. Toutefois, elles ne peuvent offrir qu'une protection limitée contre les nouvelles attaques sophistiquées, car elles ne surveillent pas en permanence les processus et les applications fonctionnant sur le réseau. Certaines équipes de sécurité informatique utilisent donc des solutions de protection supplémentaires, notamment des plateformes dites EDR (Endpoint Detection and Response). Celles-ci détectent également des menaces inconnues jusqu'alors et fournissent des informations importantes sur la manière de les contrer. Mais lorsque différents produits de différents fabricants sont utilisés, la vue d'ensemble fait défaut et l'effort administratif augmente considérablement.

Une protection complète grâce à la combinaison d'EPP et EDR

«Panda Adaptive Defense 360» (AD360) est la réponse révolutionnaire de WatchGuard à ce problème. Il s'agit de la première et unique solution permettant de combiner une plateforme de protection des endpoints (EPP – Endpoint-Protection-Platform) hautement efficace avec les technologies EDR de nouvelle génération. Le service EDR de l'AD360 garantit que seuls les processus fiables sont exécutés. Le modèle de sécurité repose sur trois piliers: Premièrement, toutes les applications sur les ordinateurs et les serveurs de l'entreprise et toutes les activités sur les terminaux sont constamment surveillées selon l'approche Zero-Trust. Deuxièmement, la classification est effectuée en temps réel grâce à une combinaison innovante de technologies d'IA telles que les Big Data, le Machine Learning et le Deep Learning. AD360 bloque automatiquement tout processus reconnu comme malveillant sans que l'équipe informatique n'ait à intervenir. Troisièmement, les applications qui ne peuvent pas être automatiquement classées sont bloquées et analysées par les techniciens spécialisés de PandaLabs en recherche de menaces.

Allège la charge des équipes informatique, attractif pour les partenaires

De cette manière, AD360 automatise de nombreux processus de sécurité informatique qui devaient auparavant être effectués manuellement et réduit considérablement la charge de travail du personnel informatique. La plateforme EPP de WatchGuard fait partie de la solution globale, qui propose une sécurité simple et centralisée, des mesures de récupération, une surveillance et des rapports en temps réel, une protection basée sur les profils, un contrôle central des appareils et un filtrage web. En combinaison avec la fonctionnalité EDR, il en résulte la meilleure protection possible contre les logiciels malveillants, basée sur les dernières technologies en matière de prévention, de détection, de forensic et de désinfection, tout cela consolidé dans une solution globale.

Adaptive Defense 360 est une solution basée sur le cloud qui combine divers services gérés et est idéale pour les PME ayant un minimum de ressources informatiques en interne. La solution est également intégrée à la plateforme Aether de Panda. Cela permet aux entreprises de gérer de manière centralisée leurs clients AD360 à partir d'un tableau de bord unifié. Aether est également capable de gérer plusieurs clients. Cela permet aux partenaires de WatchGuard d'acheter des pools de licences, qu'ils peuvent ensuite attribuer individuellement à différents clients et ainsi proposer AD360 comme solution de cyberprotection innovante.

Adaptive Defense 360: les points clés

- Combinaison de EPP et EDR avec une gestion centralisée
- Analyse et réponse plus rapides aux problèmes de cybersécurité
- Classification automatique de tous les processus et applications en cours
- Détection et résolution automatique des activités malveillantes
- Surveillance continue et visualisation centralisée des endpoints
- Solution de gestion multi-clients – idéale pour les PME et les revendeurs

BOLL
IT Security Distribution

BOLL Engineering SA

En Budron H15
1052 Le Mont-sur-Lausanne vente@boll.ch
Tél. 021 533 01 60 www.boll.ch