Une sécurité renforcée, avec moins de ressources.

Cylance renforce la protection des terminaux sans entraver les performances du PC ni engendrer de coûts supplémentaires

CYLANCE™

Introduction

Lorsque vous réfléchissez au nombre de gros titres régulièrement publiés à propos de violations majeures de données (malgré les dépenses en hausse pour des technologies de sécurité dans les entreprises), cette conclusion s'impose d'elle-même : quelque chose ne fonctionne pas.

Les solutions classiques visant à protéger les ressources informatiques ne sont plus efficaces dans l'environnement actuel des menaces de plus en plus complexes. Un grand nombre de fournisseurs vantent les mérites d'un ensemble de technologies disparates pour bénéficier d'une meilleure protection, chaque technologie permettant de stopper certaines menaces. Mais ces produits ne permettent aucune évolutivité et la protection offerte est de moins en moins efficace. Pour identifier et neutraliser les attaques des logiciels malveillants les plus récents, le fait d'utiliser plusieurs de ces produits classiques ne suffit pas.

Le déploiement d'un nombre de plus en plus élevé de technologies de sécurité induit des coûts bien plus importants en termes de ressources et d'infrastructure, notamment en ce qui concerne les serveurs, la bande passante, les dispositifs, etc. Qui plus est, bon nombre de ces produits exercent une incidence négative sur les performances du système et des applications, ce qui peut aboutir à une baisse de la productivité pour les utilisateurs finaux et l'organisation dans son ensemble. Les outils de sécurité d'ancienne génération peuvent demander bien plus de temps et d'argent aux organisations que ce qu'elles s'imaginent.

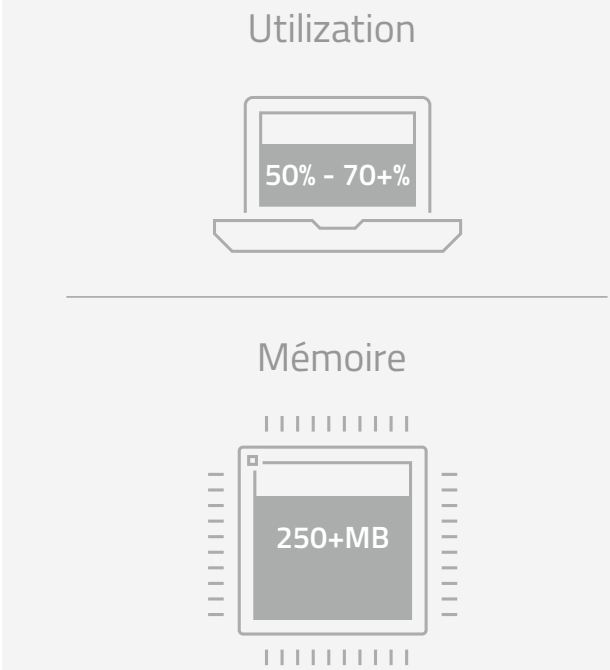
Il est temps d'adopter une nouvelle approche de sécurité qui comble toutes les lacunes des anciennes méthodes. Les entreprises peuvent déployer des solutions de sécurité qui reposent sur de nouvelles capacités d'intelligence artificielle et d'apprentissage automatique. Ces méthodes avancées sont conçues pour neutraliser les attaques les plus récentes, sans entraver les performances ni accroître les coûts. Le présent livre blanc décrit certains des principaux inconvénients des méthodes classiques de sécurité pour les terminaux, et s'intéresse à la façon dont les organisations de toutes tailles et de n'importe quel secteur d'activités peuvent tirer profit des progrès réalisés dans les technologies de sécurité pour protéger leurs systèmes et leurs données contre les menaces de la manière la plus rentable possible.

La sécurité traditionnelle nuit aux performances et accroît les coûts

Les solutions de sécurité classiques présentent deux inconvénients majeurs : elles entravent les performances et constituent une source de coûts supplémentaires.

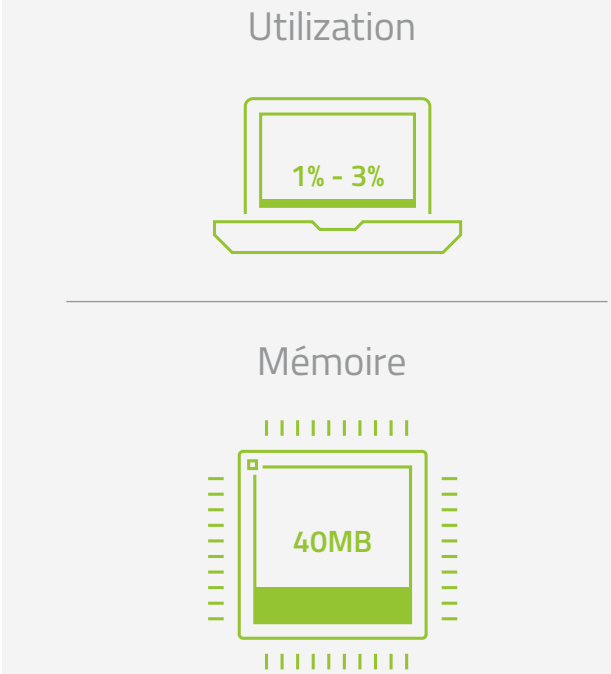
En se dotant d'outils de sécurité classiques, les sociétés doivent tenir à jour de vastes bases de données de signatures de logiciels malveillants connus ou d'applications approuvées. Elles doivent également déployer constamment du matériel et des logiciels supplémentaires, en composant avec une intégration limitée, voire inexistante ; télécharger de nouveaux

Sécurité traditionnelle des terminaux (STT)



STT – Utilisation UC : 50 à + de 70% ; mémoire : + de 250 Mo

Sécurité des terminaux de nouvelle génération (Cylance)



STNG (Cylance) – Utilisation UC : 1 à 3% ; mémoire : 40 Mo

Grande légèreté et faible impact

fichiers de signatures pour tenir à jour les bases de données de signatures ; et réaliser des analyses quotidiennes et des analyses de la mémoire, des courriels, etc. en temps réel.

Tout cela exige de nombreux cycles d'UC et dégrade l'utilisation des dispositifs clients. En moyenne, les produits de sécurité classiques pour les terminaux utilisent entre 50% et plus de 70% de cycles d'UC lors d'analyses intensives. Cela aboutit à des réclamations constantes de la part des utilisateurs finaux dans de nombreuses organisations, qui souhaitent savoir pourquoi leur système est d'une telle lenteur ou pourquoi 15 minutes de démarrage sont nécessaires chaque matin. Par ailleurs, cela augmente également les coûts et réduit la productivité, puisque les utilisateurs passent plus d'appels au centre d'assistance lorsque des problèmes surviennent.

L'impact négatif sur les performances va directement à l'encontre de ce que souhaitent actuellement les entreprises, à savoir des performances améliorées pour les systèmes et les applications, permettant aux employés de réaliser des tâches plus rapidement et efficacement. Si les systèmes sont lents, cette lenteur se répercute sur la réponse apportée aux besoins des clients, sur le développement d'un nouveau produit ou service, ou encore sur le lancement d'une campagne marketing.

L'impact sur le résultat net et les opérations commerciales peut être considérable. Les solutions de sécurité doivent neutraliser les attaques de manière efficace, mais sans entraver les performances afin de ne pas décevoir les employés et les clients.

Les récentes études menées dans le secteur démontrent l'impact important que peuvent avoir les technologies de sécurité sur l'expérience utilisateur. À titre d'exemple, Dimensional Research a réalisé une enquête en ligne en 2015 à la demande de Dell auprès de 460 professionnels de l'informatique et 301 utilisateurs professionnels aux États-Unis, au Royaume-Uni et en Allemagne. 91% des professionnels interrogés ont déclaré que les mesures de sécurité classiques mises en place par leur employeur avaient un impact négatif sur leur productivité. Une large majorité (92%) des professionnels interrogés ont déclaré subir des répercussions négatives lorsqu'ils doivent appliquer des mesures de sécurité supplémentaires pour travailler à distance. En examinant les changements apportés aux politiques de sécurité de l'entreprise au cours des 18 derniers mois, plus de la moitié des professionnels interrogés ont déclaré que l'impact négatif de la sécurité sur leur travail quotidien a augmenté.

L'impact négatif sur les performances et l'expérience utilisateur peut avoir d'autres conséquences fâcheuses pour les organisations. Par exemple, près de 70% des professionnels de l'informatique interrogés par Dimensional Research ont déclaré que les solutions de contournement adoptées par les employés pour éviter les mesures de sécurité imposées par le service informatique constituent le plus grand risque pour l'entreprise. Si le problème des performances est particulièrement complexe pour les entreprises, c'est que bien souvent, les décisionnaires ne tiennent pas compte de l'impact sur les systèmes et les ressources lorsqu'ils évaluent des produits de sécurité.

Outre les problèmes de performances, le coût plus élevé (issu à la fois des dépenses de temps et d'argent pour utiliser ces produits et des violations de sécurité qui peuvent résulter d'une sécurité inappropriée) constitue un autre problème lié aux produits de sécurité basés sur des signatures.

À titre d'exemple, dans la mesure où les produits basés sur des signatures sont inefficaces contre les logiciels malveillants, les entreprises choisissent bien souvent de déployer d'autres technologies de sécurité coûteuses, notamment des solutions de détection et de réponse pour les terminaux. Au lieu de se focaliser sur la neutralisation des programmes malveillants avant qu'ils ne s'exécutent sur les systèmes, ces solutions recherchent des indicateurs d'infection laissés par une partie d'un programme malveillant exécuté, et nécessitent des employés hautement qualifiés et très bien rémunérés.

Dans de nombreux cas, cette étape intervient lorsque les logiciels malveillants se sont déjà propagés de système en système dans l'organisation, ce qui peut être extrêmement préjudiciable pour cette dernière. Par ailleurs, les solutions qui recueillent et stockent la plupart des événements du système pour les activités de détection et de réponse peuvent finir par recueillir plus d'informations que les renseignements nécessaires, ce qui aboutit à des coûts plus élevés liés aux ressources.

Si l'on s'intéresse au temps et au coût, des analyses minutieuses réalisées sur des terminaux par des logiciels anti-programmes malveillants reposant sur des signatures sont synonymes de retards dans le travail pour les utilisateurs et de productivité moindre. Lorsque vous multipliez 10 minutes

d'analyses deux fois par jour par le nombre d'utilisateurs sur un réseau, vous obtenez rapidement un nombre à plusieurs chiffres qui peut avoir un impact financier sur la société.

D'autres coûts sont induits par le grand nombre de logiciels malveillants qui pénètrent dans l'entreprise. Ces coûts comprennent la résolution des problèmes liés aux programmes malveillants, la réinstallation de l'image sur les machines, la baisse de productivité des utilisateurs finaux, les compétences supplémentaires en sécurité informatique nécessaires et les coûts juridiques (si des dommages et intérêts découlent d'une attaque).

Les produits basés sur des signatures nécessitent également une maintenance, liée principalement à la diffusion des signatures. Ces activités de maintenance sont généralement réalisées tous les jours, mais elles peuvent également intervenir toutes les heures. Les systèmes isolés physiquement nécessitent une maintenance accrue, puisqu'ils ne peuvent pas récupérer des mises à jour depuis la passerelle Internet du fournisseur du produit. Les administrateurs peuvent avoir besoin de récupérer manuellement chaque mise à jour, de la placer sur un support amovible, de vérifier si le support ne comporte aucun logiciel malveillant, puis de transférer physiquement ce support à un système sur le réseau physiquement isolé pour poursuivre la diffusion.

Les fournisseurs de produits de sécurité classiques forcent les clients à déployer de plus en plus de couches de technologies sur les terminaux pour essayer d'améliorer l'efficacité de la protection. Ces technologies supplémentaires, comme les systèmes de prévention des intrusions hôtes et les recherches de fichiers sur la base de leur réputation, sont source d'installations, de matériel et de frais de gestion supplémentaires. Dans de nombreux cas, les utilisateurs peuvent voir quatre à six processus de sécurité différents pour les terminaux utilisés au sein de l'entreprise.

Incapacité à protéger

Non seulement les produits de sécurité basés sur des signatures exercent un impact sur les performances et augmentent les coûts, mais ils échouent à leur mission principale : protéger les organisations du contenu malveillant. Aucun fournisseur de produits de sécurité classiques pour les terminaux n'est en mesure d'empêcher l'exécution des programmes malveillants. Par définition, les antivirus basés sur des signatures ont toujours un patient zéro, puisque le programme malveillant doit être identifié avant que la signature ne puisse être écrite. De nombreuses nouvelles menaces évoluées sont des attaques de type « zero-day », qui utilisent différentes techniques dont il faut également empêcher l'exécution.

C'est l'un des inconvénients de la surveillance post-exécution. La plupart du temps, une série de comportements constitue un comportement malveillant. Il peut toutefois être trop tard pour bloquer le logiciel malveillant si la détermination n'est pas effectuée à temps, et plus important encore, à chaque fois. Pour certaines solutions, plusieurs minutes, voire plusieurs jours ou semaines sont nécessaires pour réaliser de telles déterminations.

Le recours à des méthodes de sécurité basées sur des signatures présente un inconvénient majeur : en fonction du niveau de risque, les organisations peuvent attendre jusqu'à 72 heures qu'un fichier de signatures soit créé. La création d'un fichier de signatures se fait en plusieurs étapes. Plus on attend avant d'appliquer une protection efficace, une protection efficace, plus le nombre de terminaux infectés augmente, ce qui coûte plus d'argent.

Dans son Étude sur le coût des violations de données en 2016, le Ponemon Institute a révélé que le coût total moyen d'une violation de données pour les 383 sociétés participant aux

recherches effectuées s'élève à 4 millions de dollars (USD). Le coût moyen payé pour chaque document perdu ou volé et renfermant des informations sensibles et confidentielles est de 158 USD.

Pour terminer, il existe des coûts indirects qui découlent des attaques parvenant à contourner les outils basés sur des signatures. Cela comprend le préjudice causé à la réputation de la marque, le coût méconnu des informations de l'entreprise ou des secrets d'État perdus ou volés, etc.

Les menaces informatiques ont évolué pour devenir plus sophistiquées au fil des années, et elles peuvent facilement muter pour prendre de nouvelles formes méconnaissables. À ce jour, quasiment tous les programmes malveillants sont polymorphes, ce qui signifie qu'ils sont extrêmement personnalisés et ciblés. Les techniques traditionnelles d'analyse de logiciels malveillants, comme les fichiers de signatures, l'heuristique ou le recoupement de la réputation, sont facilement mises en déroute par les programmes malveillants ayant muté. Par ailleurs, comme les logiciels malveillants examinent leur environnement pour savoir si des techniques d'analyse dynamique sont utilisées (comme la mise en bac à sable), ces techniques sont facilement mises à mal.

Même si le paysage de la cybersécurité se caractérise par des changements constants, les composants de base de la détection des programmes malveillants sont restés identiques pendant plus de trente ans.

Des technologies antivirus vieilles de plusieurs dizaines d'années et basées sur des signatures ne sont pas efficaces contre les raz-de-marée actuels d'attaques sophistiquées comprenant des variantes infinies de logiciels malveillants. À titre d'exemple, les pirates informatiques peuvent facilement et efficacement déguiser (ou « faire muter ») les programmes malveillants en utilisant des packs logiciels répandus. Ces logiciels modifient les caractéristiques du programme malveillant et changent les empreintes numériques, ce qui facilite la pénétration en évitant les antivirus reposant sur des signatures. Cette opération est aussi simple que de changer la plaque d'immatriculation d'une voiture volée. En réalité, les analyses indiquent que 99% des empreintes des logiciels malveillants ne sont vues que pendant 58 secondes ou moins, et la plupart des programmes malveillants n'ont été vus qu'une seule fois, ce qui vous donne une idée de la vitesse à laquelle les pirates informatiques modifient leur code pour éviter d'être détectés.

Avec la myriade d'attaques réussies ayant fait les gros titres ces dernières années, il est évident que les approches classiques semblent inefficaces. Et la situation ne risque pas de s'arranger pour les méthodes de sécurité classiques. Ces produits ne pourront pas être améliorés, puisqu'ils utilisent encore une technologie réactive. Ils se fient à une base de code vieille de plusieurs dizaines d'années pour offrir une protection réactive, ce qui augmente la probabilité de dégâts issus des attaques. En outre, ils exigent de la part des clients qu'ils achètent et réunissent plusieurs technologies, ce qui augmente les coûts opérationnels et de matériel dédié.

Pour terminer, les fournisseurs traditionnels vendent des technologies de sécurité complémentaires qui gonflent encore plus la sécurité sur le terminal avec d'autres agents, des logiciels à exécuter et des interfaces de gestion à utiliser, ce qui tire les coûts vers le haut. Pour couronner le tout, les logiciels sont de plus en plus instables, puisque de nombreuses couches sont ajoutées aux bases de code existantes, ce qui provoque défaillances et dysfonctionnements des logiciels.

Une approche plus pertinente envers la sécurité

Une approche nouvelle et moderne envers la sécurité, qui offre une alternative aux anciens outils basés sur des signatures, est aujourd'hui disponible. Cette technologie se focalise sur une prédiction et une prévention proactives, plutôt que sur une réaction après coup. Grâce à l'intelligence artificielle et l'apprentissage automatique, cette technologie identifie et bloque immédiatement les logiciels malveillants et les menaces « zero-day » afin d'empêcher leur exécution, ce qui permet aux organisations de se protéger contre ces attaques sans avoir besoin de signatures. Des modèles mathématiques et d'apprentissage automatique en temps réel empêchent les menaces d'endommager les systèmes.

Dans la mesure où cette solution est intégrée à chaque terminal et empêche de manière préventive les programmes malveillants de s'exécuter sur ces terminaux, les entreprises peuvent se défendre plus efficacement contre les attaques les plus récentes.

À la différence des méthodes classiques qui sont réactives et échouent bien souvent à neutraliser les logiciels malveillants, cette approche est préventive. Par conséquent, elle est en mesure de neutraliser 99% des programmes malveillants qui attaquent les terminaux, contre une moyenne de 60 à 70% pour les produits anti-logiciels malveillants classiques basés sur des signatures.

Outre le fait d'offrir un niveau de sécurité bien meilleur, cette approche répond de manière efficace aux problèmes de performances liés aux solutions classiques. Dans la mesure où elle n'implique pas le recours à des signatures et utilise moins de technologies, elle consomme peu de ressources, notamment en termes d'UC et de mémoire. Une architecture de protection devrait être silencieuse pour les utilisateurs et simple à déployer et à gérer pour les administrateurs.

Comme nous l'avons évoqué précédemment, le fait que les technologies de sécurité classiques doivent se fier à de vastes bases de données de signatures de logiciels malveillants connus ou d'applications approuvées constitue l'une de leurs principales faiblesses. Les solutions modernes peuvent prendre des décisions en temps réel sur un terminal en comparant les caractéristiques d'un objet à des modèles d'intelligence artificielle qui sont mis à jour quelques fois par

an. Cela signifie qu'il n'est plus nécessaire de télécharger en permanence de nouveaux fichiers de signatures.

La solution de sécurité plus récente est moins encombrante, puisqu'elle n'a pas besoin d'examiner en détail un terminal pour essayer de trouver des programmes malveillants comme le font les produits classiques basés sur des signatures. Par conséquent, sa présence sur le système d'exploitation et les applications est transparente, tant pour l'utilisateur final que pour le terminal.

Ces solutions permettent également aux entreprises d'éviter les coûts élevés induits par l'utilisation des méthodes classiques de détection de programmes malveillants. En disposant de défenses plus efficaces contre les programmes malveillants, les entreprises n'ont pas besoin de déployer des outils de détection et de réponse pour les terminaux qui nécessitent des employés hautement qualifiés. Elles remplacent les méthodes désuètes capables d'identifier un logiciel malveillant uniquement lorsqu'il a été exécuté et qu'il a potentiellement porté préjudice à l'entreprise.

Les analyses approfondies réalisées sur les terminaux par des logiciels reposant sur des signatures sont éliminées, tout comme les longs retards de travail pour les utilisateurs finaux. Pour les entreprises comptant des milliers d'utilisateurs sur un réseau, cela peut aboutir à un montant considérable en termes de prévention des coûts. Est également éliminée la maintenance coûteuse nécessaire pour les produits basés sur des signatures.

La robustesse accrue de l'approche de sécurité rendue possible par les solutions modernes peut aider les organisations à se prémunir contre les attaques. Des millions de dollars de pertes de données, de frais juridiques, de pénalités réglementaires et d'autres coûts sont ainsi évités. Qui plus est, les coûts immatériels liés au préjudice porté à la marque (résultant d'un incident de sécurité) sont écartés.

Pour finir, le personnel de sécurité et informatique a tout le loisir de se focaliser sur des missions plus stratégiques et innovantes. Cela est rendu possible grâce aux économies de temps réalisées du fait de l'absence d'outils basés sur des signatures.

Résumé et conclusion

Les entreprises qui se fient à des produits de sécurité basés sur des signatures n'ont rien fait de mal. Elles n'avaient simplement pas d'autre choix, puisqu'aucune solution viable n'était disponible. Il n'en reste pas moins que ces produits n'offrent pas une protection appropriée contre les menaces informatiques actuelles, et qu'elles deviennent de moins en moins efficaces chaque jour.

Tandis que les pirates informatiques sont passés à des attaques plus sophistiquées, les anciennes méthodes visant à sécuriser les informations n'ont pas évolué avec le temps. La mutation des programmes malveillants permet aux pirates informatiques d'utiliser le même vecteur d'attaque et les mêmes logiciels malveillants dans une nouvelle attaque indétectable. Ainsi, une solution antivirus plus intelligente est nécessaire pour empêcher l'exécution des programmes malveillants jusqu'à présent inconnus et stopper le raz-de-marée de menaces « zero-day ».

Qui plus est, ces solutions d'ancienne génération exercent une incidence négative sur les performances des applications et des systèmes opérationnels clés, et tirent les coûts de sécurité à la hausse en raison des multiples couches de défenses nécessaires.

Mais il existe à présent une alternative. Il s'agit de solutions de sécurité préventive qui empêchent les attaques, identifient les menaces avant qu'elles ne se matérialisent, et offrent un nouveau niveau de sécurité, de performances et d'économies. Elles sont en mesure de faire face aux pirates informatiques et aux créateurs de logiciels malveillants, et de neutraliser leurs attaques avant qu'elles n'aient un impact réel.

Cette approche moderne envers la sécurité est mise en œuvre dans trois domaines essentiels : fournir une protection maximale pour les données et les systèmes ; fournir cette protection sans sacrifier les performances ; et fournir des économies et d'autres avantages stratégiques, comme permettre au personnel informatique et de sécurité de travailler sur des projets à long terme plutôt que de répondre en permanence aux urgences du quotidien.

Plutôt que de s'en remettre à la parole d'un fournisseur, Cylance recommande aux cadres informatiques et de sécurité d'évaluer les produits de sécurité classiques en les comparant dans un environnement « réel ». Cylance propose des examens du bien-fondé de la conception, ce qui simplifie l'évaluation de ses technologies par rapport aux technologies de sécurité actuelles d'une autre société. Pour accéder aux outils de test de la société, rendez-vous sur www.cylance.com.

+33-1-70395287
sales@cylance.com
www.cylance.com
Second Floor, 89/90 South Mall, Cork City, Ireland T12 RPP0