Protection de Terminaux de Nouvelle Génération

Guide d'achat
version 2

SentinelOne™

SentinelOne™

Protection de Terminaux de Nouvelle Génération

Introduction

Le paysage de la sécurité actuel

Au cours des vingt dernières années d'évolution du paysage informatique, deux constantes demeurent : les cyberpirates trouvent toujours le moyen de contourner les mesures de sécurité en place, et les terminaux restent leurs cibles de prédilection. Désormais, avec le cloud et les équipements mobiles, les terminaux sont devenus le nouveau périmètre de sécurité de l'entreprise. Il est donc de plus en plus critique de les verrouiller.

Les entreprises déploient de nombreux logiciels sur les terminaux pour les sécuriser : antivirus, antimalware, pare-feu pour postes de travail, détection des intrusions, gestion des vulnérabilités, filtrage Web, antispam et bien d'autres encore. Pourtant, malgré les nombreuses solutions en place, des entreprises prestigieuses subissent toujours des violations de securite. Pour preuve, les récentes attaques ciblant la grande distribution et l`hôtellerie, ou des malfaiteurs ont piraté des serveurs de paiement au moyen de malwares spécialisés pour voler les informations de carte de crédit des clients.

L'inefficacité des mesures de sécurité traditionnelles

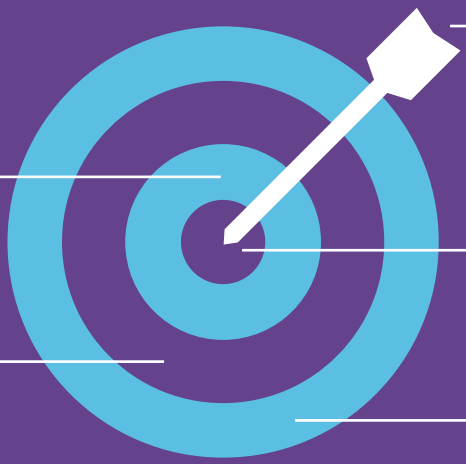
En matière cle sécurité, il existe un problèmes fondamental et récurrent : les moyens de défense se focalisent essentiellement sur des éléments connus, qu'il s'agisse de hachage, d'adresse IP, de vulnérabilité ou de comportement. Or, les pirates sont capables de mettre en oeuvre des techniques de dissimulation suffisamment ingénieuses pour contourner les outils de sécurité et compromettre le serveur ou l'ordinateur portable qu'ils ciblent. De plus, il est tres aisé d'altérer le code malveillant grâce à des outils, téléchargés ou créés sur mesure, qui permettent de contourner les mesures de sécurité. Des connaissances de base en programmation suffisent Le schéma ci-contre illustre quelques techniques de camouflage, souvent utilisées conjointement pour adapter un fichier binaire connu et lui donner une apparence totalement nouvelle, inconnue et inoffensive.

Les pirates emploient en outre différents vecteurs pour distribuer leur code malveillant et exécuter leurs attaques. Les principaux vecteurs dattaque sont énumérés a droite. Les attaques peuvent être diffusées sur un seul vecteur ou sur plusieurs, sous une forme plus sophistiquée.

Techniques de dissimulation des attaques

Packers
Conçus pour garantir que le code s'exécute uniquement sur une machine réelle (pour que le code reste dormant et évite les machines virtuelles, le débogage,etc.).

Variations/Obfuscateurs
Transforment le code malveillant connu pour qu'il apparaisse comme différent ou nouveau.



Malwares
Code exécuté sur l'ordinateur de la victim.

Ciblage
Permet au code de s'exécuter uniquement sur une machine ou un terminal ciblé et doté d'une configuration particulière.

Wrappers
Conçus pour convertir le code en nouveau fichier binaire.

Les antivirus sont-ils dépassés ?

Les antivirus existent depuis un quart de siecle et, pourtant, ils n'ont bénéficié d'aucune innovation qui leur permettrait de proteger les systèmes contre les attaques recourant à des techniques inconnues. Ils continuent à rechercher des hachages connus, et des modifications même minimes suffisent a les mettre en échec. Les antivirus négligent également le fait que certaines attaques n'utilisent aucun fichier ; elles infectent la mémoire et écrivent directement dans la RAM plutôt que dans les systèmes de fichiers.

Par ailleurs, il est bien connu que les antivirus manquent de convivialité, que leurs mises à jour consomment énormement de bande passante et que leurs analyses gourmandes en ressources monopolisent le temps processeur. Leur emploi provoque non seulement des temps d'indisponibilité, mais aussi un sentiment cle frustration chez les utilisateurs, qui sont alors tentés de désactiver le logiciel ou d'ignorer les avertissements de securité.

Le sandboxing est-il une solution?

Il y a environ cinq ans, les environnements sandbox réseau ont fait leur apparition. En substance, ils émulent l'exécution de fichiers inconnus dans une machine virtuelle sur le réseau et surveillent le comportement du fichier suspect lors de son exécution au sein de l'environnement « protégé ››, Bien que ces solutions aient amélioré le taux de détection des nouvelles menaces, elles sont loin d'être efficaces à 100 %.

Les pirates ont rapidement compris que, si leurs techniques de compression ne permettaient pas de contourner les sandbox, il leur suffisait de détecter les caractéristiques de cet environnement :un temps d'émulation limite, un manque d'interaction avec les utilisateurs et une seule image spécifique du système d'exploitation. Une fois l'environnement sandbox identifié, les pirates s'assurent que leur code malveillant ne s'exécutera pas dans lenvironnement émulé, sera marqué comme légitime et continuera sa progression vers le terminal où il sera finalement exécuté (sans que l'antivirus puisse le bloquer à ce stade).

Les antivirus de nouvelle génération basés sur les mathématiques

On parle beaucoup des antivirus autonomes de nouvelle génération intégrant des modèles mathématiques prédictifs, l'apprentissage automatique (machine learning) et l'intelligence artificielle. Que la technologie sous-jacente repose ou non sur une véritable intelligence artificielle, une telle approche présente des limites du point de vue de la sécurité. Un produit de prévention basé sur les mathématiques, quels que soient les mérites qu'on lui attribue, ne parviendra jamais à résoudre tous les défis rencontrés par votre entreprise pour protéger efficacement ses terminaux.

Dans ce nouveau paysage des menaces, il est nécessaire d'adopter une approche radicalement différente.

Vecteurs d'attaque

Malwares

Fichiers exécutables

Malwares, chevaux de Troie, vers, backdoors (portes dérobées), fichiers avec charge active

Malwares sans fichiers

Malwares agissant uniquement en mémoire, pas d'indicateurs sur les disques

Exploits

Documents

Exploits intégrés dans des documents Office, des fichiers Adobe, des macros. E-mails de spearphishing (harponnage)

Exploits de navigateur

Téléchargements, Flash, Java, Javascript, vbs, iframe/html5,plug-ins

Live/Insider Threats

Scripts

Powershell, WMI, PowerSploit, VBS

Identifiants

Récupération des identifiants, Mimikatz, tokens (jetons)

Cinq raisons d'aller au-delà des antivirus basés sur les mathématiques

1. Les malwares basés sur les fichiers ne représentent que la moitié du problème

Les attaques basées sur les fichiers PE et DLL représentent uniquement 50 a 60 % des nouveaux malwares recensés chaque semaine. Les produits qui se limitent a la prévention seront totalement inefficaces contre les menaces associant plusieurs vecteurs, surtout si elles n'utílisent pas de fichiers, par exemple :

• Memory-based malware
• Exploits
• Script-based attacks from the inside

2. Il est impossible de tout prévoir

Il est vain de penser qu'il est possible de prédire la véritable nature d'un fichier (inoffensif ou malveillant) au moyen d'une analyse statistique d'attributs prédéfinis. Puisque les attaques reposent sur les comportements humains, il est pratiquement impossible de prédire les nouvelles techniques et les nouveaux modes opératoires des cyberpirates.

3. Un taux de prévention de 99 % ne suffit pas

Lorsque ces 99 % concernent uniquement les malwares basés sur les fichiers, c'est clairement insuffisant. Même si 99 % des malwares basés sur les fichiers sont bloqués, qu'en est-il du 1 % restant ?

Si vous êtes confronté à une centaine de variantes de malwares, un taux de 99,9 % peut paraître élevé, mais l'on parle ici de millions de menaces en circulation.

Une nouvelle attaque zero-day est découverte presque chaque semaine et près d'un million de nouvelles variantes de malware sont distribuées CHAQUE SEMAINE.

UNE SEULE de ces attaques peut entraîner un grave préjudice financier et porter atteinte a la réputation de l'entreprise.

4. L'apprentissage des technologies d'intelligence artificielle prend du temps

Le déploiement initial peut demander un temps considérable puisque le produit n'utilise pas de fichiers de définition et que les équipes informatiques et de sécurité doivent apprendre au système à distinguer les éléments inoffensifs et dangereux.

C'est également à l'équipe d'administration qu'il incombe d"examiner les fichiers basés sur les hachages M5 et d'étudier les rapports de cyberveille.

Selon l'environnement et le nombre de ressources informatiques allouées au projet de sécurité, ce processus peut être extrêmement chronophage.

5. Aucune option de gestion sur site

Si votre entreprise est tenue de respecter des politiques strictes en matière de confidentialité des données et que celles-ci exigent une administration et un stockage sur site des données de l'entreprise, l'antivirus de nouvelle génération basé sur les mathématiques, malgré tout le battage qui l`entoure, n'est pas fait pour vous.

Une telle solution est toujours dépendante du cloud, sans aucune possibilité dela déployer sur un serveur de gestion sur site.

Une nouvelle approchoche de la sécurité des terminaux

Protection des terminaux de nouvelle génération

Ces dernières années, une technologie d'un nouveau genre a vu le jour, conçue pour détecter et prévenir les menaces sur les terminaux à l'aide d'une approche unique, basée sur les comportements. Plutôt que de rechercher des éléments connus ou leurs variantes par comparaison de signatures, les solutions de sécurité des terminaux de nouvelle génération analysent les caractéristiques des fichiers (pour détecter les malwares basés sur les fichiers, connus et inconnus), mais aussi le comportement du système du terminal afin d'identifier toute activité suspecte à l'exécution, La fonction EDR (Endpoint Detection and Response) surveille l'activité et permet aux administrateurs d'agir sur les incidents pour empêcher les menaces de se propager dans tout l'environnement. La protection des terminaux de nouvelle génération (NGEP, Next-Generation Endpoint Protection) va encore plus loin et applique des mesures automatisées pour bloquer et neutraliser les attaques.

Jusqu'il y a peu, les administrateurs hésitaient à utiliser les capacités de protection en raison des nombreux faux positifs que générait l'identification de comportements inhabituels mais non malveillants Skype, par exemple, ne respecte pas de nombreuses règles des applications « normales ›› en changeant dynamiquement de ports et de protocoles, alors que c'est une application légitime souvent utilisée en entreprise. La protection NGEP doit pouvoir apprendre à connaître l'environnement et les systèmes locaux afin de ne pas signaler les comportements légitimes.

La protection des terminaux de nouvelle génération en remplacement de l'antivirus

Si vous évaluez des solutions de sécurité de nouvelle génération pour les terminaux, vous pensez peut-être qu'il s'agit d'un outil supplémentaire qui va encombrer le système (et grever votre budget). Et si vous travaillez dans un secteur réglementé, il se peut que vous deviez conserver votre antivirus et installer la protection des terminaux en couche supplémentaire, afin de vous protéger contre de nouvelles attaques inconnues. De nombreux éditeurs ne prétendent d'ailleurs pas que leurs solutions remplacent un antivirus. Mais si la solution NCEP a été testée et certifiée et qu'il est attesté qu'elle répond aux critères exigés des antivirus (en ayant réussi le test de détection), vous pouvez envisager de la substituer a votre antivirus.

Pour remplacer totalement les fonctions de protection des anciennes technologies statiques de protection des terminaux, les solutions NOEP (Next Generation Endpoint Protection) doivent être suffisamment autonomes pour sécuriser les terminaux contre les menaces existantes et avancées, aux différents stades du cycle de vie de l'attaque (pré-exécution, en cours d'exécution, post-exécution).

Votre solution NCEP doit se concentrer sur quatre aspects de la protection qui, mis en oeuvre conjointement, permettent de détecter et prévenir la plupart des techniques d'attaques avancées à toutes les étapes de leur cycle de vie.

Détection des malwares avancés

Votre solution NGEP doit être capable de détecter et de bloquer les malwares inconnus et les attaques ciblées, même lorsqu'ils ne présentent pas d'indicateurs statiques de compromission. Cela implique une analyse comportementale dynamique, c'est-à-dire l'analyse et la surveillance en temps réel du comportement des processus et des applications, sur la base d'une instrumentation de bas niveau des activités et opérations du système d'exploitation - dont la mémoire, le disque, le registre, le réseau, etc. Étant donné que de nombreuses attaques détournent les processus système et applications légitimes pour masquer leurs activités, il est essentiel de parvenir a inspecter le processus d'exécution et de recréer le véritable contexte d'exécution. La technique est encore plus efficace en cas d'exécution sur l'équipement, que celui-ci soit hors ligne ou en ligne (pour le protéger même des attaques transmises par clé USB)

Limitations des risques

La détection des menaces est nécessaire, mais si elle est exécutée seule, il peut s'écouler des jours, des semaines, voire des mois avant que l'attaque ne soit neutralisée. Une limitation des risques automatisée et rapide doit être intégrée a la NGEP. Les options de limitation des risques doivent reposer sur des règles et être assez flexibles pour couvrir un large éventail de cas d'utilisation, comme la mise en quarantaine d'un fichier, l'arrêt d'un processus spécifique, la déconnexion de la machine infectée du réseau ou son arret total. Une limitation rapide des risques pendant les premières phases du cycle de vie de l'attaque minimisera les dommages et accélèrera la correction.

Correction

Pendant l'exécution, les malwares créent, modifient ou suppriment souvent les paramètres du registre et des fichiers système, et altèrent les paramètres de configuration. Ces changements ou les résidus qu'ils laissent peuvent entraîner une instabilité ou un dysfonctionnement du système. La solution NGEP doit être à même de restaurer un terminal à son état fiable, précédant l'infection par malware, tout en enregistrant les modifications apportées et les corrections implémentées.

Investigation numérique

Aucune technologie de sécurité ne prétend être efficace a 100 %. La capacité à fournir une visibilité et une analyse complète des terminaux en temps réel est donc un point essentiel. Une visibilité claire et opportune de l'activité malveillante dans tout l'environnement vous permet d'évaluer rapidement la portée d'une attaque et de prendre les mesures qui s'imposent. Cela nécessite une piste d'audit en temps réel des événements survenus sur un terminal pendant une attaque, et la capacité de rechercher des indicateurs de compromission.

Évaluation des fournisseurs de solutions NGEP

Questions d'évaluation

Maintenant que vous connaissez les critères à prendre en compte dans l'évaluation d'une solution NGEP, vous devez limiter votre choix aux meilleurs candidats de votre présélection. Demandez une version d'évaluation du logiciel. Assurez-vous qu'il sagit d'une version de production complète pour que vous puissiez observer son fonctionnement dans votre environnement et juger de ses résultats aux tests de sécurité que vous avez préparés. Dans le cadre de votre évaluation, tenez compte des points suivants ;

1. La solution EPP et EDR combinée en un seul agent doit-elle être déployée via un outil de déploiement de logiciel traditionnel et gérée / exploitée via une seule console de gestion centrale ?
2. Le logiciel offre-t-il une fonctionnalité de « multi-tenant » pour les terminaux sur site et dans le cloud ? Par exemple, si une entreprise dispose de deux équipes informatiques devant gérer différentes entités ou filiales dans différents pays, le logiciel peut-il supporter cette fonction et prendre en charge les terminaux ?
3. En ce qui concerne les terminaux (dont les terminaux mobiles s'ils sont pris en charge), quelles plates-formes et quelles versions principales de systèmes d'exploitation sont prises en charge ? Pour chacun d'entre eux, quelles sont les con gurations requises (processeur, mémoire, stockage) ?
4. Par quels moyens techniques le produit détecte-t-il et bloque-t-il les attaques de chaque vecteur - en ce compris les malwares, les exploits et les menaces internes ou actives ?
5. À quelle fréquence les mises à jour sont-elles disponibles ? Les mises à jour sont-elles envoyées au terminal ou téléchargées par une connexion initiée par le terminal lui-même ? Les mises à jour nécessitent-elles une intervention de l'utilisateur (p. ex. un redémarrage) ?
6. Les mises à jour nécessitent-elles une intervention de l'utilisateur (redémarrage, par exemple) ?
7. Le produit peut-il prévenir les menaces si le terminal est déconnecté du réseau ?
8. Dans quelle mesure le produit est-il évolutif ? Combien de clients peuvent être pris en charge par chaque console de gestion ?
9. Le serveur de gestion est-il basé sur le cloud ou physiquement sur site ?
10. Comment le produit évite-t-il les faux positifs et apprend-il les comportements inoffensifs du système ? Quel est le taux actuel de faux positifs ?
11. Quel est le taux actuel de faux positif ?
12. Une intégration avec les systèmes SIEM est-elle possible pour la gestion des incidents ?
13. Existe-t-il des règles de prévention pour se protéger des menaces en temps réel ?
14. Quelles offres de support le fournisseur de la solution de protection des terminaux propose-t-il ? Les mises à jour et mises à niveau des logiciels font-elles partie des frais de licence ?
15. Les mises à jour logicielles font-elles partie du coût de la licence ?

Pourquoi SentinelOne?

Brief historique

SentinelOne a été fondé par un groupe d'experts internationaux spécialisés en systèmes de défense et cyberveille, conscients de la nécessité de réinventer la protection des terminaux. Aujourd'hui, notre équipe d'experts s'est étoffée et reste motivée par l'innovation.

SentinelOne endpoint protection platform

Endpoint Protection Platform (EPP) de SentinelOne offre aux entreprises une protection unifiée et en temps réel des terminaux. Elle centralise la prévention, la détection et l'intervention au sein d'une même plate-forme gérée par une console unique. La solution tire parti de fonctions avancées d'apprentissage automatique (machine learning) et d'automatisation intelligente pour protéger les terminaux Windows, OS X et Linux contre les menaces transmises sur tous les principaux vecteurs : malwares avancés (basés sur les fichiers et exécutés en mémoire), exploits et attaques furtives basées sur des scripts. Elle surveille étroitement tous les processus et threads d'exécution sur le système, jusqu'au niveau du noyau. La visibilité sur les opérations du système tout entier (appels système, fonctions réseaux, E/S, registre, etc.) et la prise en compte des données d'historique offrent un aperçu complet du contexte qui permet de distinguer entre comportements normaux et malveillants. Dès qu'un comportement typiquement malveillant est identifié et marqué, il déclenche un ensemble de mesures qui neutralisent immédiatement l'attaque. Parmi ces mesures :

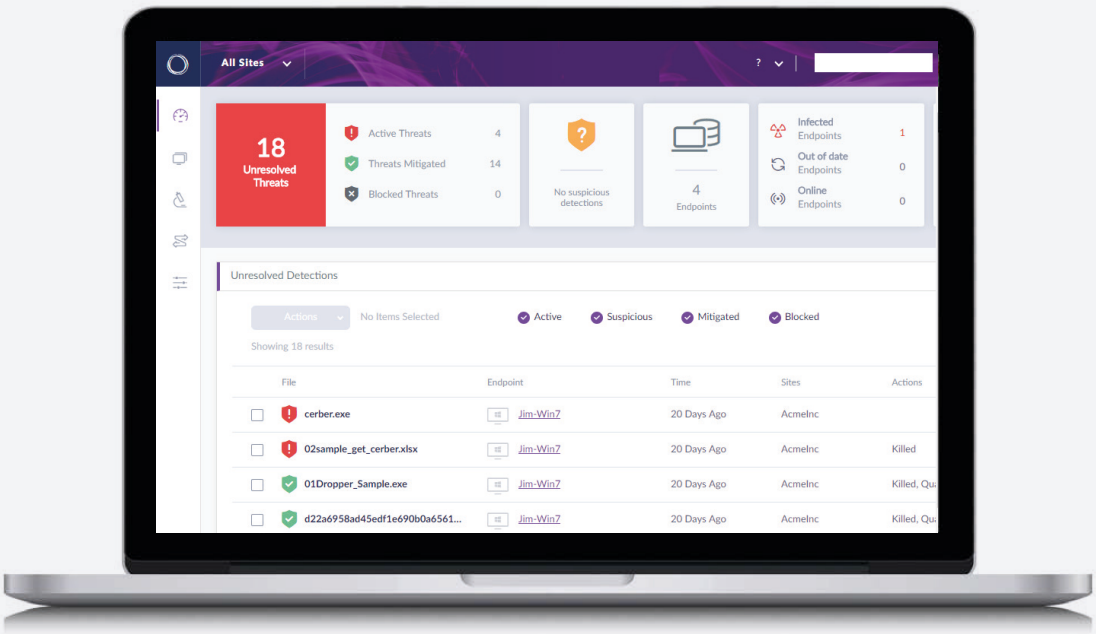
Limitation des risques — Des règles faciles à configurer permettent d'arrêter les processus suspects, de mettre en quarantaine ou de supprimer les fichiers binaires malveillants et tous les éléments associés avant d'isoler le terminal du reste du réseau.

Immunisation — Dès qu'une attaque est bloquée, les informations pertinentes sont immédiatement partagées avec les autres terminaux du réseau pour immuniser les systèmes susceptibles d'être pris pour cible dans le cadre d'une attaque coordonnée.

Correction — Les fichiers supprimés ou modifiés sont automatiquement restaurés à l'état antérieur à l'attaque.

Investigation numérique — Vous bénéficiez d'une vue à 360 degrés de l'attaque, comprenant les informations de fichier, le chemin d'accès, le nom de la machine, l'adresse IP, le domaine et d'autres données (disponibles dans SentinelOne ou via votre solution SIEM).

De plus, SentinelOne EPP est une solution unique et légère qui utilise en moyenne 1 à 2 % du temps processeur, de sorte que le terminal peut fonctionner de manière performante — qu'il s'agisse d'un ordinateur portable, d'un poste de travail, d'un appareil mobile ou d'un serveur. Comme la solution se concentre sur chaque système individuellement, aucune analyse active ni mise à jour de signature n'est nécessaire et les terminaux sont toujours protégés, qu'ils soient connectés au réseau ou non. SentinelOne EPP est pris en charge sur les principaux systèmes d'exploitation mobiles, d'ordinateur de bureau/portable et de serveur.



Solution certifiée en remplacement de l'antivirus

AV-TEST, principal institut de recherche antivirus indépendant, a décerné à SentinelOne EPP la certification Approved Corporate Endpoint Protection à la fois pour Windows et OS X, ce qui confirme son efficacité dans la détection des malwares avancés et dans le blocage des menaces connues. SentinelOne EPP est le seul fournisseur de solutions de protection des terminaux de nouvelle génération à avoir obtenu cette certification sur les deux plates-formes.

La solution SentinelOne EPP a été également certifiée conforme aux exigences PCI DSS et HIPAA par le bureau d'études indépendant Tevora. Cette certification permet désormais aux entreprises de remplacer leurs suites antivirus existantes par SentinelOne EPP tout en satisfaisant les exigences de conformité PCI DSS et HIPAA.

SentinelOne™

Pour plus d'informations sur SentinelOne, consultez notre site: sentinelone.com