SentinelOne™

L'offre de valeur SentinelOne

Pour être efficace, la protection des postes de travail doit pouvoir détecter les comportements malveillants sur tous les vecteurs d'attaque et intervenir instantanément de manière judicieuse, par le biais d'une plate-forme unique simple à gérer.

C'est ce que vous offre SentinelOne.

Nous controns les menaces avancées sur tous les principaux vecteurs d'attaque. Si les cybermenaces actuelles se cantonnaient aux simples malwares transmis par des fichiers, les antivirus basés sur les signatures et autres solutions de prévention statiques pourraient être suffisants. Malheureusement, les menaces avancées ne limitent pas leur arsenal aux fichiers exécutables. Les entreprises doivent se protéger contre toutes sortes d'attaques : malwares exécutés en mémoire, exploits de document et de navigateur, scripts lancés par des attaquants internes et ainsi de suite. En d'autres termes, si l'attaque n'utilise aucun fichier, les antivirus d'ancienne ou de nouvelle génération laissent votre entreprise sans défense.

SentinelOne Endpoint Protection Platform (EPP) offre une protection contre tous les principaux types de cyberattaques. Notre technologie ne repose pas sur des signatures ou des analyses heuristiques, dont l'efficacité est limitée aux attaques basées sur des fichiers. SentinelOne détecte les menaces de façon dynamique, grâce à l'analyse de leur comportement. Nous surveillons le système du point de vue des processus, ce qui nous permet d'identifier les principaux types de cyberattaques, quel que soit leur modus operandi.

LA PROTECTION DE SENTINELONE EPP :

Malwares avancés

Ransomwares, chevaux de Troie, vers, backdoors

Attaques sans fichier

Malwares exécutés en mémoire

Exploits

Exploits de document et de navigateur

Attaques basées sur des scripts

Powershell, PowerSploit, WMI, VBS

Attaques par vol d'identifiants

Récupération des identifiants, Mimikatz, tokens

Notre approche globale de la protection couvre toutes les étapes du cycle de défense contre les menaces.

Il faut se rendre à l'évidence, les solutions de simple prévention ne suffisent plus pour protéger les serveurs critiques et les postes des utilisateurs contre les attaques sophistiquées actuelles. En matière de protection des postes de travail de nouvelle génération, les approches les plus efficaces sont celles qui couvrent toutes les étapes du cycle de défense contre les menaces et qui combinent prévention, détection et intervention. SentinelOne EPP réunit toutes ces fonctionnalités critiques au sein d'une plate-forme unique. Notre solution ne se contente pas de réduire la surface d'attaque globale grâce à des listes blanches et listes noires, ou de bloquer les menaces connues par une prévention statique.

En plus de contrer les menaces avant l'exécution, SentinelOne EPP détecte dynamiquement les malwares avancés, les exploits et les attaques internes basées sur des scripts. Elle offre en outre des fonctionnalités intelligentes de limitation des risques et de correction, entièrement intégrées. Les entreprises peuvent définir des règles personnalisées qui exécutent automatiquement certaines actions en cas de détection d'une attaque, neutralisant presque instantanément les menaces.

Notre solution assure une visibilité totale sur les serveurs et les postes de travail, ainsi qu'une vue complète de chaque attaque.

Vous ne pouvez pas espérer protéger correctement un poste de travail si vous ne savez pas exactement quels processus et applications il exécute. L'agent léger autonome de SentinelOne assure une surveillance rigoureuse de toutes les activités de chaque système au niveau du noyau et de l'espace utilisateur. Cette vue complète nous permet de détecter efficacement les attaques les plus furtives dès l'exécution, en nous appuyant sur une connaissance approfondie du comportement normal des systèmes et des applications.

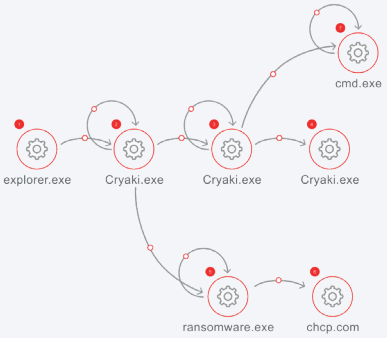
Nous analysons toutes les activités surveillées pour effectuer des investigations en temps réel, assorties d'une reconstitution intuitive de l'attaque. Cette analyse globale et historique offre des informations cruciales sur tous les événements survenus au cours de l'attaque, en partant de son point d'origine et en retraçant sa progression au fil des postes de travail et autres systèmes.

ACTIONS AUTOMATISÉES, DÉCLENCHÉES PAR DES RÈGLES :

- Alerte de l'équipe de sécurité
- Suppression des processus malveillants
- Mise en quarantaine des fichiers infectés
- Déconnexion du réseau des postes de travail compromis

NEUTRALISATION DES MODIFICATIONS APPORTÉES PAR LES CYBERATTAQUES :

- Nettoyage des processus infectés des postes de travail
- Restauration des fichiers à l'état antérieur à l'attaque



SENTINELONE PROTÈGE LES POSTES DE TRAVAIL ET SERVEURS CRITIQUES SUIVANTS :

- Windows 7, 8, 8.1 et 10
- Windows Server 2008 R2 et 2012 R2
- Mac OS X 10.9.x, 10.10.x et 10.11
- Red Hat Linux, CentOS 6.5 et versions ultérieures, Ubuntu 12.04 et 14.04 LTS

PLATES-FORMES VIRTUELLES

- vSphere
- Microsoft Hyper-V
- Citrix Xen Server, Xen Desktop, Xen App

Nous protégeons une large gamme de plates-formes de serveurs et postes de travail, tant physiques que virtuelles.

Les environnements informatiques actuels comprennent de nombreux systèmes d'exploitation et types de postes de travail différents. La protection de pointe de SentinelOne s'étend aux postes de travail Windows, Mac OS et Linux. Évolutive, elle permet de protéger des centaines de milliers de postes utilisateur et serveurs critiques à l'échelle de toute l'entreprise.

La solution offre un coût total de possession (TCO) jusqu'à cinq fois inférieur aux approches NGEP multisolutions.

Le déploiement d'une panoplie de solutions NGEP (Next-Generation Endpoint Protection) qui couvrent individuellement les fonctions de prévention, de détection et d'intervention implique un grand nombre d'agents et de consoles de gestion. Cette approche nécessite en outre une équipe de sécurité étoffée pour en assurer la gestion et introduit un risque de problèmes d'interopérabilité, susceptibles de compromettre la productivité. SentinelOne EPP réunit toutes les fonctionnalités critiques des solutions NGEP au sein d'une plate-forme unique, facile à gérer, ne nécessitant qu'un seul agent léger sur le poste de travail. Le coût total de possession (TCO) de SentinelOne EPP est jusqu'à cinq fois inférieur à celui des approches intégrant plusieurs solutions disparates.

SentinelOne™

Pour en savoir plus sur la plate-forme de protection des postes de travail de nouvelle génération de SentinelOne et l'avenir de la protection des postes de travail, consultez notre site à l'adresse : sentinelone.com