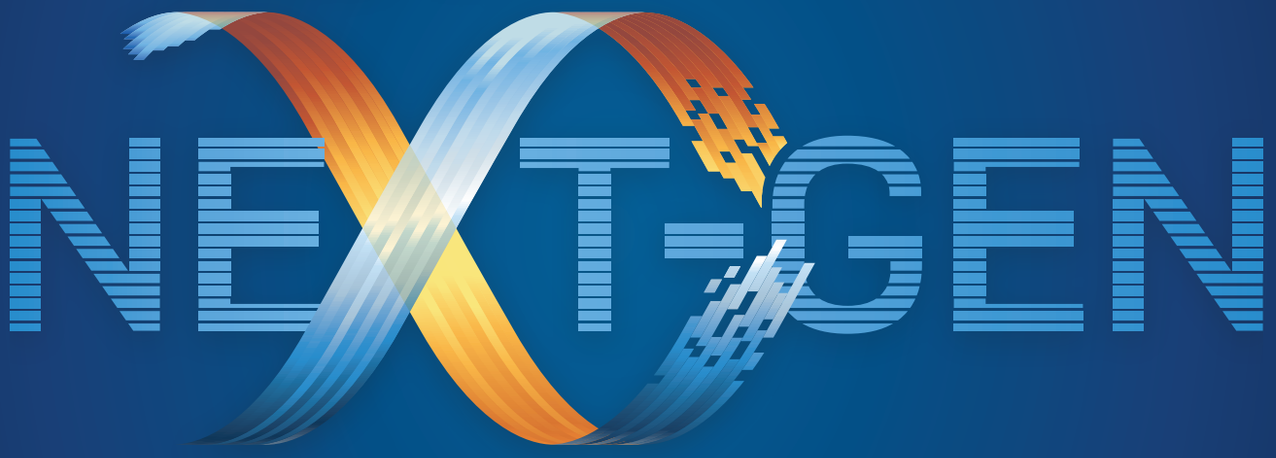
SOPHOS | discover



PROTECTION ENDPOINT NEXT-GEN
ÉVOLUTION OU RÉVOLUTION ?

Après la révolution Next-Gen Firewall de ces dernières années, une nouvelle révolution Next-Gen est cours dans le domaine de la sécurité des systèmes Endpoint.

Au-delà du débat pour savoir s'il s'agit d'une révolution ou d'une simple évolution, il est certain qu'une série de nouvelles technologies est en train de rapidement émerger, en apportant une contribution significative à la lutte contre les menaces avancées.

Cette évolution n'est pas le fruit du hasard : la dernière série d'attaques de ransomware a été la plus dévastatrice jamais observée, la digitalisation de l'économie rend la continuité des services informatiques de plus en plus critique et les nouvelles législations telles que le RGPD augmentent encore les enjeux.

Ces dernières années, les grandes entreprises ont expérimenté avec succès ces nouvelles technologies de protection Endpoint Next-Gen dans leurs SOC. Elles sont maintenant prêtes pour une large démocratisation.

Dans ce document, nous examinons pourquoi et comment ces technologies font la différence.

RÉSUMÉ

Une révolution de la protection Endpoint Next-Gen est en cours

Ces dernières années, les grandes entreprises ont expérimenté avec succès dans leurs SOC (Security Operation Center) un ensemble de nouvelles technologies de protection Endpoint Next-Gen qui sont maintenant prêtes pour une large démocratisation.

Issues des recherches de laboratoires et de start-ups spécialisées, ces technologies commencent maintenant à être intégrées dans les solutions de protection Endpoint des principaux acteurs du domaine de la sécurité, suite à des acquisitions et des développements internes.

Une réponse à de nouvelles menaces et de nouveaux défis

Ces technologies ont été conçues pour répondre aux attaques modernes telles que les attaques discrètes et ciblées de type APT (Advanced Persistent Threats) et les assauts massifs et répétés de menaces potentiellement dévastatrices, telles que les ransomwares WannaCry et NotPetya. Ces technologies sont les bienvenues à un moment où la digitalisation de tous les secteurs de l'économie rend la continuité des services informatiques toujours plus critique et où les législations se renforcent, à l'image du Règlement Général sur la Protection des Données (RGPD) de l'Union Européenne.

Élever le niveau de sécurité

S'il n'existe pas de définition unique de ces technologies de protection Endpoint Next-Gen, elles partagent le même but de protéger contre les nouvelles menaces avancées grâce à des approches technologiques innovantes.

Une de leurs caractéristiques marquantes est d'abandonner le mode réactif pour une approche purement prédictive, capable de bloquer des menaces inconnues et mouvantes. On utilise souvent le terme de protection « sans signatures » pour décrire un ensemble de technologies couvrant l'Intelligence Artificielle, les anti-exploits et diverses techniques de protection contre des attaques sans fichiers.

Dans cette liste figure aussi en bonne place la nécessité d'avoir des outils d'analyse plus complets et donnant une visibilité plus large, afin de mieux répondre et remédier aux attaques.

Un autre champ d'innovation est la synchronisation des niveaux de protection, pour qu'ils fonctionnent comme un seul système. Echanger des informations en temps réel entre les protections Endpoint et Réseaux réduit ainsi les angles morts, permet d'automatiser les ripostes et diminue considérablement le temps de réponse.

Un complément aux solutions de protection traditionnelles

Ces technologies de protection Endpoint Next-Gen ne signent pas pour autant la fin des protections Endpoint traditionnelles. Elles fournissent de nouvelles protections, bienvenues dans le cadre d'une stratégie multi-niveaux indispensable pour relever les défis des nouvelles menaces, dans un contexte toujours plus exigeant.

Sophos offre le meilleur des deux mondes en matière de protections Endpoint traditionnelles et Next-Gen

Grâce à l'acquisition de spécialistes riches d'une décennie d'expérience dans les technologies Next-Gen de Deep Learning et d'anti-exploit, Sophos est en mesure de fournir le meilleur des deux mondes en matière de protections Endpoint traditionnelles et Next-Gen, intégrées dans une console d'administration centrale optimisée pour la simplicité et synchronisées avec ses solutions de protection réseaux.

1. ÉVOLUTION DES MENACES : DE NOUVELLES ATTAQUES DÉVASTATRICES

Quelles sont les évolutions des menaces les plus notables ?

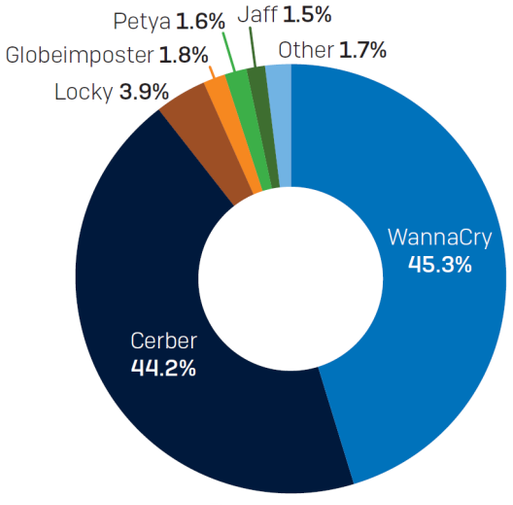
L'évolution récente la plus notable de l'environnement des menaces est sans conteste la succession ininterrompue d'attaques de ransomware qui a démarré avec Locky début 2016 pour culminer avec WannaCry et NotPetya ces derniers mois. Si ce type d'attaque n'est pas nouveau (Cryptolocker date de 2013), l'ampleur et l'impact de cette nouvelle vague est sans précédent.

- Locky a marqué le début de cette vague grâce à une combinaison de techniques d'ingénierie sociale bien conçues et de dissimulation dans des technologies trop souvent autorisées en entreprise, comme les Macros de la suite Microsoft Office, VBScript ou JavaScript. Ses victimes ont vu les données de leurs postes de travail chiffrées et retenues en otage contre le versement d'une rançon en Bitcoins. Avec Locky, les Comités de Direction ont soudain pris conscience du potentiel de nuisance des ransomwares.

- WannaCry a innové en n'utilisant pas uniquement les canaux de diffusion habituels, par courriels ou sites Web infectés. Il a également exploité une vulnérabilité dans le service Windows SMB, qui permet aux systèmes et imprimantes de partager des fichiers sur les réseaux locaux, pour prendre en otage des centaines de milliers de systèmes dans le monde. C'est la résurgence d'une dynamique de diffusion virale qui avait fait les beaux jours des infections par vers à la fin des années 2000 (Sasser, Conficker ...).

  Un correctif de Microsoft était disponible déjà depuis des semaines, mais la plupart des entreprises ne l'avaient pas entièrement déployé. WannaCry ne s'est pas seulement attaqué aux postes mais également aux serveurs, ciblant les bases de données SQL et les fichiers Microsoft Exchange.

- Comme WannaCry, NotPetya s'est diffusé comme un ver, en exploitant les mêmes failles de sécurité critiques volées à l'Agence Nationale de Sécurité américaine (connues sous le nom de code EternalBlue au sein de la NSA). Contrairement à WannaCry, NotPetya s'attaquait au secteur de boot, afin de bloquer l'accès au disque, même à partir d'un autre système. Une autre différence notable est que les victimes n'arrivaient pas à joindre les attaquants pour payer la rançon. Les chercheurs des SophosLabs estiment que les créateurs de NotPetya l'ont utilisé comme une expérimentation ou un outil de destruction massive de données.



Ransomwares
Avril à octobre 2017
(Source: SophosLabs)

Cette même période a vu l'essor des services de RaaS (Ransomware as a Service), avec notamment le ransomware Cerber, ainsi qu'une continuation de la diffusion des Kits d'Exploits. Tous ces services aident la communauté des cybercriminels à créer des attaques sophistiquées avec un minimum d'effort ou d'expertise et à diffuser très rapidement les nouveaux exploits de vulnérabilités.

Quel a été l'impact de ces attaques sur les entreprises ?

Ces attaques ont eu un impact considérable. Contrairement à la période précédente, caractérisée par des attaques silencieuses de vol de données, nous sommes entrés dans nouvelle phase d'attaques destructrices et médiatiques.

La cybersécurité s'est retrouvée sur le bureau des Comités de Direction, dans un contexte où la continuité des services informatiques est de plus en plus critique pour la bonne marche de leurs opérations.

La fuite massive de données personnelles annoncée par Equifax envoie un message clair : les négligences en matière de sécurité peuvent coûter leurs postes non seulement au RSSI et au DSI, mais aussi au PDG lui-même.

Quels sont les enseignements de ces attaques de ransomware ?

Les attaques de ransomware ne sont que la partie émergée de l'iceberg. Les mêmes stratégies et tactiques sont largement utilisées dans des attaques plus silencieuses et moins médiatiques. Les enseignements suivants sont pertinents pour la vaste majorité des menaces avancées :

- **Bloquer le dialogue avec le centre de Commande & Contrôle peut neutraliser une menace.**

  Comme la plupart des menaces modernes, les ransomwares doivent communiquer avec le centre de Commande & Contrôle du pirate pour être pleinement efficaces. Si cette communication est rompue, le ransomware ne reçoit pas les clés de chiffrement et est neutralisé. La détection et le blocage des communications avec les centres de Commande & Contrôle est donc un composant important de toute stratégie de défense.

- **Les techniques de défense spécifiques contre des catégories d'attaques sont supérieurement efficaces.**

  Même si les techniques de détection traditionnelles fournissent une bonne protection contre la plupart des attaques de ransomware, les techniques de protection spécifiques contre cette menace sont supérieures.

  En se concentrant sur le processus de chiffrement des ransomwares, elles sont capables de bloquer les attaques de ransomwares inconnus et de restaurer les fichiers chiffrés. Dans le cas particulier de NotPetya, une parade mise en oeuvre par Sophos Intercept X est encore plus précise, puisqu'elle met en œuvre une fonction, Sophos WipeGuard, qui empêche spécifiquement les modifications malveillantes du secteur de boot.

  En protégeant les utilisateurs des attaques de WannaCry, NotPetya et des autres ransomwares, Sophos Intercept X illustre la valeur et l'efficacité de ce type de protection contre des catégories d'attaques spécifiques.

- **Bloquer les Exploits est une haute priorité.**

  L'exploitation des vulnérabilités EternalBlue par WannaCry et NotPetya nous rappelle l'importance d'une bonne protection contre les Exploits. La plupart des attaques réussies exploitent des vulnérabilités. Même si des correctifs sont le plus souvent disponibles, l'expérience montre que la plupart des organisations prennent des mois à les déployer, laissant le champ libre aux Exploits.

  La mise en place de technologies anti-exploit à large spectre devrait être une priorité haute.

- **Les outils d'analyse de l'origine des attaques permettent de restaurer les systèmes attaqués.**

  Les techniques anti-ransomware dédiées sont en mesure de restaurer les fichiers chiffrés après la détection d'une attaque. Ceci est rendu possible par une supervision et un enregistrement continus des événements systèmes.

  Ceci permet le nettoyage en profondeur et la restauration du système dans son état d'origine avant le début de l'attaque. Cet outil d'analyse donne également des informations précieuses sur l'origine de l'attaque, son cheminement et les ressources affectées.

- **Les systèmes Mac et les mobiles ne sont pas immunisés.**

  WannaCry et NotPetya exploitaient des vulnérabilités Windows et ne concernent donc pas les systèmes Mac et Android. Cependant, ces plateformes ne sont pas immunisées contre les attaques. Les deux ont subi des attaques de ransomware sur la période et leurs utilisateurs doivent en être conscients et se protéger.

2. ÉVOLUTION DES ENVIRONNEMENTS ET DES LÉGISLATIONS

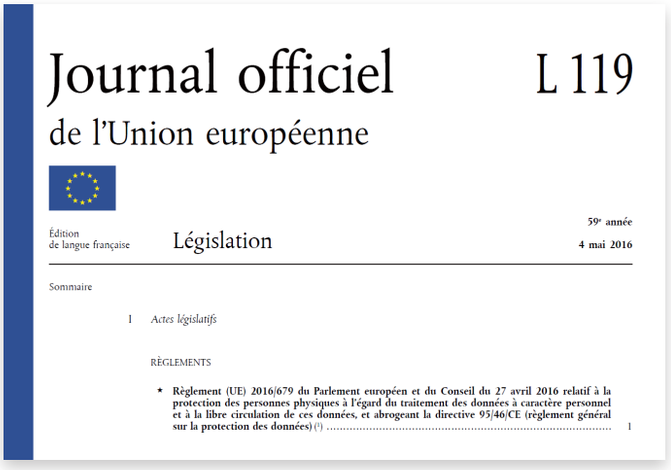
Quelles évolutions des environnements IT impactent la sécurité des entreprises ?

La digitalisation massive de l'économie rend la continuité des services informatiques critiques pour les entreprises de tous les secteurs. Comparé à il y a seulement trois ans, les coûts d'une interruption de service sont montés en flèche. Il est donc grand temps pour les entreprises de toute taille de renforcer leur infrastructure de sécurité.

La généralisation des outils et des pratiques de mobilité a également créé un environnement plus complexe à gérer et à protéger pour les départements informatiques.

Enfin, les législateurs renforcent les lois qui protègent les données personnelles pour les adapter à l'ère du digital, ce qui complique encore les choses.

Quel est l'impact du RGPD sur la sécurité ?


Journal officiel L 119
de l'Union européenne
Édition de langue française
Législation
59e année
4 mai 2016
Sommaire
I Actes législatifs
RÈGLEMENTS
* Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (1) 1

En janvier 2012, l'Union Européenne a initié une réforme pour moderniser la Directive CE 95/46 de 1995 sur la protection des données personnelles. Publié en mai 2016 au Journal officiel de l'Union Européenne, le nouveau Règlement Général sur la Protection des Données (RGPD) UE 2016/679 entrera automatiquement en application le 25 mai 2018.

Dans les articles 7 à 21, au cœur du texte, le Règlement donne un plus grand contrôle aux citoyens sur les données personnelles que détiennent les entreprises et organismes publics. Consentement clair et explicite lors de la collecte, droit d'accès, droit à l'oubli, droit à la portabilité et limitation du recours au profilage sont quelques-uns des nouveaux droits institués par ce texte. Les entreprises et organismes publics doivent s'y préparer, ce qui nécessite avant tout la mise en place de procédures et de services pour être en mesure de répondre aux nouvelles exigences.

Dans son article 32, il demande également aux organisations de s'assurer de la sécurité du traitement des données à caractère personnel. Si le texte met en avant l'utilité de techniques telles que le chiffrement pour y parvenir, il n'impose pas de solutions ni de limitations sur les mesures à mettre en œuvre. Dans les pages Web dédiées au RGPD, la CNIL oriente pour les actions à mener vers son **Guide sur la sécurité des données personnelles**. Ce Guide rappelle en 17 fiches que cette sécurité dépend des bonnes pratiques de sécurité qui couvrent l'ensemble du système d'information et en particulier les postes de travail, les serveurs, les mobiles et le réseau.

Les risques introduits par ce nouveau règlement sont importants. Ils concernent d'abord l'image, en raison de la notification obligatoire des violations de données à la CNIL (Article 33) et éventuellement aux personnes concernées (Article 34). Ils concernent également les amendes administratives que la CNIL pourra imposer en cas de violation au règlement (Article 83). Celles-ci pourront s'élever à 20 millions d'Euros ou 4% du chiffre d'affaires annuel mondial total de l'exercice précédent, dans le cas d'une entreprise, le montant le plus élevé étant retenu.

C'est donc le bon moment pour s'intéresser au renforcement du niveau de sécurité de votre infrastructure.

3. TECHNOLOGIES DE PROTECTION NEXT-GEN: ÉLEVER LE NIVEAU DE SÉCURITÉ

Que sont ces technologies Endpoint Next-Gen et d'où viennent-elles ?

Ces dernières années, des centres de recherche et des start-ups spécialisées ont innové et introduit sur le marché de nouvelles technologies pour combattre les menaces avancées.

Certaines se sont concentrées sur la résolution de problèmes majeurs et anciens, tels que les Exploits. L'analyse des activités en mémoire pour détecter ce type d'attaque, qui échappe aux technologies basées sur l'analyse de fichiers, s'est révélée particulièrement efficace et applicable à d'autres menaces telles que les ransomwares. C'est la voie suivie par la société SurfRight, acquise par Sophos en décembre 2015, qui a élaboré les technologies anti-exploit et anti-ransomware intégrées aujourd'hui dans Sophos Intercept X.

Quelques-unes ont été développées dans des laboratoires de recherche avancée, avant d'être expérimentées et déployées par les grandes entreprises. C'est le cas des fonctionnalités de Deep Learning de Sophos Intercept X, issues de l'acquisition d'Invincea en février 2017. Démarrées dans le cadre d'un projet pour l'agence américaine de recherche avancée dans le domaine de la défense (DARPA) avant d'être commercialisées par Invincea, ces technologies ont reçu la reconnaissance d'organismes de test comme AV-Test.org et d'analystes tels que Forrester et Gartner. Sophos Intercept X leur ouvre la voie d'une large démocratisation.

D'autres sont nées des besoins des SOC (Security Operation Center) de grandes entreprises. En cherchant comment mieux enregistrer et corréler les événements des systèmes Endpoint (sur les fichiers, les processus, les registres, la mémoire ...) pour mieux analyser et comprendre les attaques, ils ont suscité l'émergence des solutions EDR (Endpoint Detection and Response). Très utiles entre les mains expertes d'équipes bien entraînées dans les SOC, ces technologies sont malheureusement souvent très complexes à maîtriser. Des éditeurs tels que Sophos proposent de les démocratiser par des approches comme les fonctions Root Cause Analysis et Deep Cleaning de Sophos Intercept X.

Toutes ces technologies sont fort diverses. Cependant, une des caractéristiques communes les plus significatives est de laisser de côté les approches réactives pour privilégier un modèle prédictif, capable de bloquer des menaces inconnues et mouvantes. On utilise ainsi souvent le terme de protection « sans signatures ».

Comment fonctionnent les protections anti-ransomware Next-Gen ?

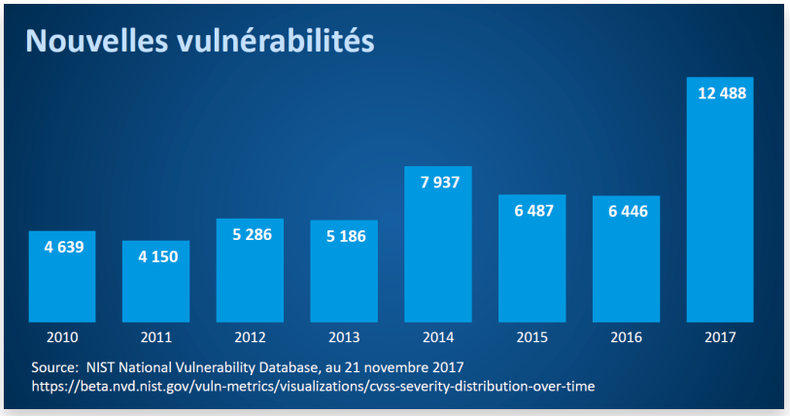
La protection anti-ransomware est un défi difficile à résoudre. La plupart des éditeurs détectent les attaques de ransomware par les mêmes méthodes anciennes, à savoir la détection des variantes de malwares spécifiques impliquées dans l'attaque. Comme il est facile de créer de nouveaux logiciels qui chiffrent ou rendent inutilisables les documents stratégiques, il n'est pas surprenant que les attaques de ce type se soient multipliées.

Les anti-ransomwares Next-Gen, tels que la capacité CryptoGuard de Sophos Intercept X, détectent les séquences de chiffrement de fichiers rapides typiques des ransomwares. Lorsqu'une telle séquence est détectée, CryptoGuard vérifie d'abord s'il s'agit d'un outil légitime comme Sophos SafeGuard, la solution de chiffrement d'entreprise de Sophos. Si tel n'est pas le cas, le processus est interrompu et les fichiers venant juste d'être chiffrés sont restaurés dans leur état initial.

En surveillant le comportement des attaques de ransomware plutôt qu'essayer de détecter les innombrables variantes pouvant être créées, CryptoGuard est capable de détecter plus de 99% des nouvelles variantes de ransomwares sans avoir à modifier son modèle de surveillance comportementale.

Pourquoi les protections anti-exploit sont-elles si cruciales ?

Les Exploits profitent des failles de logiciels légitimes, tels qu'Adobe Flash, Microsoft Office ou Windows lui-même, pour infecter les systèmes. Ils sont couramment utilisés lors de cyberattaques : plus de 90% des violations de données déclarées montrent l'utilisation d'un exploit à une ou plusieurs étapes du déroulement de l'attaque.



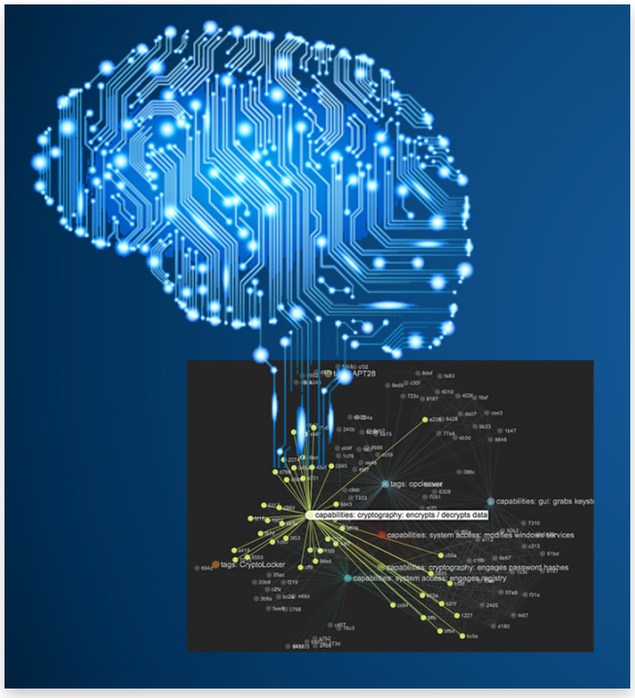
Les Exploits existent depuis plus de 30 ans. Il n'est donc pas étonnant que la majorité des éditeurs de sécurité revendique un certain niveau de prévention des Exploits. Cependant, l'étendue et le degré de protection varient de manière significative d'un éditeur à l'autre. Pour certains, il s'agit d'une simple case de plus à cocher, au moindre coût de développement possible, tandis que pour d'autres il s'agit d'un composant majeur de leur stratégie.

La technologie anti-exploit de Sophos Intercept X protège contre une gamme étendue de techniques d'Exploit. Une telle approche de la sécurité entièrement sans signature ne requiert aucune connaissance préalable des malwares. Intercepter les techniques d'attaque est une manière incroyablement efficace de protéger les systèmes Endpoint modernes. Les principales techniques contre lesquelles Sophos Intercept X protège sont énumérées ci-dessous :

Enforce Data Execution Prevention (DEP) ..... Empêche les dépassements abusifs de mémoire tampon
Mandatory Address Space Layout Randomization (ASLR) ..... Prévient l'abus d'emplacements de code prédictibles
Bottom Up ASLR ..... Améliore le caractère aléatoire de l'allocation d'emplacements de code
Null Page (Null Dereference Protection) ..... Bloque les exploits venant de la page Zéro
Heap Spray Allocation ..... Zones de mémoire courantes pré-allouées pour bloquer les attaques
Dynamic Heap Spray ..... Bloque les attaques qui diffusent des séquences suspectes dans la mémoire dynamique
Stack Pivot ..... Bloque les attaques contre le pointeur de retour de fonction de la pile
Stack Exec (MemProt) ..... Bloque le code d'un pirate sur la pile
Stack-based ROP Mitigations (Caller) ..... Bloque les attaque communes de type "Return-Oriented Programming"
Branch-based ROP Mitigations (Hardware Augmented) ..... Bloque les attaques ROP avancées
Structured Exception Handler Overwrite Protection (SEHOP) ..... Bloque l'utilisation abusive du gestionnaire d'exceptions
Import Address Table Filtering (IAF) (Hardware Augmented) ..... Bloque les pirates cherchant les adresses des API dans l'IAT
Load Library ..... Empêche le chargement de bibliothèques à partir des chemins UNC
Reflective DLL Injection ..... Empêche le chargement d'une bibliothèque depuis la mémoire sur un processus hôte
VBScript God Mode ..... Empêche l'utilisation abusive de VBScript dans IE pour exécuter du code malveillant
WoW64 ..... Bloque les attaques visant la fonction 64 bits du processus WoW64
Syscall ..... Bloque les pirates tentant de contourner les points de branchement (hooks) de sécurité
Hollow Process ..... Bloque les attaques utilisant des processus légitimes pour cacher du code malveillant
DLL Hijacking ..... Donne la priorité aux bibliothèques du système pour les applications téléchargées
Application Lockdown ..... Bloque les attaques logiques contournant les mitigations
Java Lockdown ..... Empêche les attaques utilisant abusivement Java pour lancer des exécutables Windows
Squiblydoo AppLocker Bypass ..... Empêche regsvr32 d'exécuter à distance des scripts et du code
CVE-2013-5331 & CVE-2014-4113 via Metasploit ..... Charges virales en mémoire: Meterpreter & Mimikatz

Quels sont les bénéfices des technologies d'Intelligence Artificielle telles que le Deep Learning ?

L'Intelligence Artificielle a fait d'énormes progrès ces dernières années et peut désormais être utilisée d'une manière fiable pour effectuer des évaluations en pré-exécution sans signatures de n'importe quel fichier, afin de déterminer s'il s'agit d'un malware, d'un logiciel potentiellement indésirable ou d'une application légitime.



Chez Sophos, nous avons suivi une approche unique pour nos fonctionnalités d'apprentissage automatisé : nous avons fortement investi dans des technologies avancées de Deep Learning par réseaux de neurones.
Elles se distinguent des méthodes de Machine Learning courantes, encore très présentes dans les solutions de sécurité mais actuellement délaissées par les chercheurs les plus en pointe, car ne répondant plus aux enjeux actuels sur le volume de traitement de données

Au lieu de réaliser des analyses heuristiques ou par signatures comme l'antivirus classique le fait, les réseaux neuronaux d'apprentissage profond sont capables de sélectionner les critères de détection qui correspondent le plus précisément aux malwares. Le modèle de Deep Learning apprend ce qu'il faut rechercher dans le code, comment les pirates essaient de contourner les détections, comment ils développent leur logiciel et comment le logiciel se déploie et s'exécute. Ces informations sont évaluées par un algorithme de Deep Learning à multiples couches de neurones. Il évalue toute similarité du logiciel avec les malwares et les logiciels potentiellement indésirables et, en fonction du résultat, le classe comme malveillant, potentiellement indésirable ou légitime. Tout ceci s'effectue en seulement 20 millisecondes avec un modèle d'environ 20 Mo sur disque.

Cette approche est capable d'intégrer la totalité des connaissances stockées dans les énormes bases de données de codes malveillants et d'applications légitimes de laboratoires d'analyse antimalware tels que les SophosLabs. C'est une prouesse hors de portée des bataillons d'analystes antimalware, aussi nombreux soient-ils. Qui plus est, elle rend possible leur mise en oeuvre dans des modèles de protection compacts, efficaces et simples à déployer. Ceci ouvre une nouvelle perspective révolutionnaire dans l'analyse antimalware.

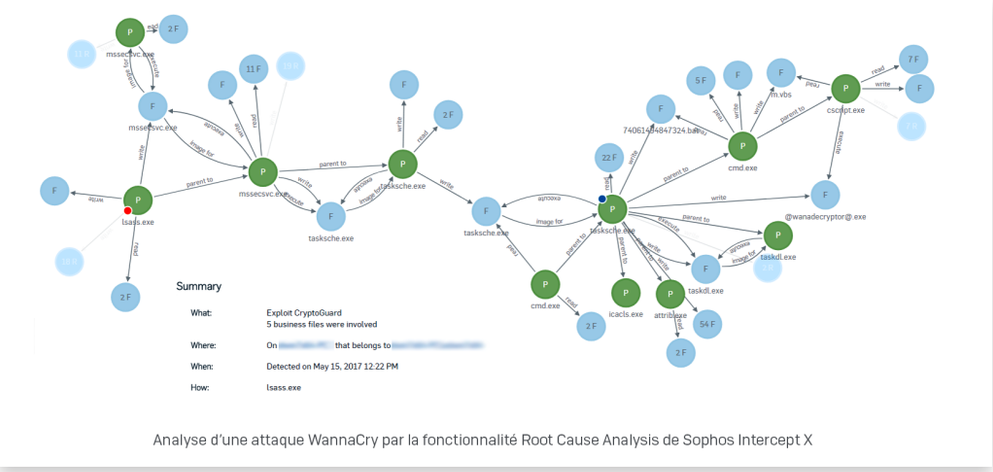
Pourquoi les entreprises ont-elles besoin d'outils pour analyser l'origine des attaques ?

Comment pouvez-vous répondre efficacement à une attaque si vous ne savez pas exactement ce qui s'est passé ?

Lorsqu'une activité malveillante est détectée sur un système, il est impératif que l'administrateur dispose d'informations pour comprendre la nature de l'incident, comment il s'est produit, comment il a été détecté et quelles sont les actions à prendre pour empêcher de futurs incidents similaires. Cette capacité à effectuer une analyse de l'attaque est typiquement le travail des SOC dotés d'applications de type SIEM (Security Information and Event Management) ou EDR sophistiquées. Malheureusement, le volume des détections d'activités suspectes à surveiller dans une entreprise ordinaire peut facilement surcharger une équipe de sécurité informatique souvent déjà en sous-effectif.

Pour répondre à ce défi, certaines solutions de protection Endpoint Next-Gen telles que Sophos Intercept X incluent une analyse automatique des causes et du cheminement de l'attaque, avec des recommandations sur les prochaines étapes

à mener pour mieux se protéger. L'analyse détaillée des attaques offre une visualisation simple, immédiate et graphique de l'intégralité de l'attaque : comment elle a démarré, à quel stade elle a été détectée et tout ce qui s'est passé entre les deux événements. Elle offre également des informations détaillées sur les composants impliqués dans l'attaque, comme les clés de registre, les processus ou les connexions réseaux. Elle va même plus loin dans l'automatisation de la réponse aux incidents, en permettant un nettoyage en profondeur du système pour le restaurer dans son état de santé d'origine.



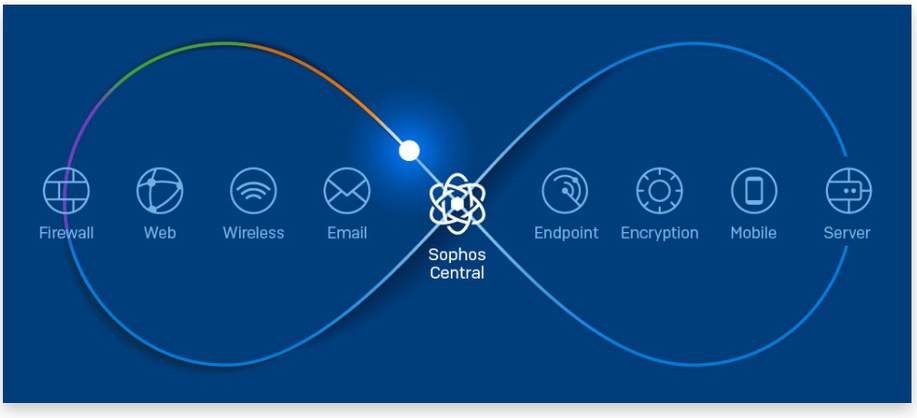
Analyse d'une attaque WannaCry par la fonctionnalité Root Cause Analysis de Sophos Intercept X

Quels sont les bénéfices de la synchronisation des sécurités Endpoint et Réseaux ?

La sécurité synchronisée permet aux solutions de sécurité Next-Gen Endpoint et Next-Gen Firewall de Sophos d'échanger en continu des informations importantes sur les comportements malveillants ou suspects dans tout l'écosystème informatique de l'entreprise. En utilisant une connexion directe et sécurisée appelée Sophos Security Heartbeat™, les protections Endpoint et réseau agissent comme un seul système intégré, permettant aux organisations de prévenir, détecter et résoudre les menaces en temps quasi réel, sans nécessiter d'augmenter la taille des équipes.

À titre d'exemple, lorsque le pare-feu Next-Gen de Sophos détecte une menace avancée ou une tentative de fuite de données confidentielles, il peut automatiquement utiliser Sophos Security Heartbeat™ pour prendre une série de mesures sur le réseau et les systèmes afin de limiter les risques et de bloquer la perte de données instantanément. De même, s'il découvre qu'un système protégé est compromis, la sécurité synchronisée permet l'isolement automatisé et quasi-immédiat de ce système d'extrémité, l'empêchant de divulguer des informations confidentielles ou d'envoyer des données à un centre de Commande et de Contrôle.

Ce type de découverte et de réponse aux incidents, qui pourrait prendre des semaines ou des mois, ne prend que quelques secondes grâce à la sécurité synchronisée.



4. LES SOLUTIONS ANTI-MALWARE TRADITIONNELLES SONT-ELLES OBSOLÈTES ?

Les nouveaux éditeurs spécialisés dans les technologies de protection Endpoint Next-Gen suggèrent que les solutions de protection Endpoint traditionnelles pourraient bientôt être obsolètes. Qu'en est-il réellement ?

Il est depuis longtemps largement reconnu que l'analyse par signatures à elle seule ne suffit plus. De par sa nature propre, cette technique peut uniquement reconnaître ce qu'elle connait déjà. Elle offre cependant une première ligne de défense efficace et rapide contre ce qui est déjà connu, utile quand elle est couplée avec d'autres techniques de protection.

En plus de la technologie de détection par signatures, les solutions de protection Endpoint traditionnelles fournissent une très large gamme de fonctions de sécurité, rarement présentes dans les solutions Next-Gen :

RÉDUCTION DE LA SURFACE D'EXPOSITION

La prévention de l'exposition aux menaces évite aux utilisateurs de se retrouver sous le feu de mécanismes d'attaques ou de livraison de malwares. Elle est une composante essentielle de toute stratégie de sécurité.

- Sécurité du Web (blocage des sites Web infectieux et des serveurs de Commande et de Contrôle)
- Contrôle du Web (filtrage d'URLs en fonction des politiques de sécurité de l'entreprise)
- Contrôle des périphériques
- Contrôle des applications
- Contrôle des données (DLP)

PRÉVENTION DE L'EXÉCUTION

La prévention de l'exécution analyse les fichiers en amont, avant leur exécution, à la recherche de codes malveillants. Elle met en oeuvre un nombre important de technologies, en plus des traditionnelles signatures.

- Réputation des téléchargements
- Détection à base de signatures
- Analyse heuristique
- Emulation
- Sandboxing et Live Lookup

DÉTECTION LORS DE L'EXÉCUTION

Personne ne peut promettre une prévention parfaite dans 100% des cas. C'est pourquoi il est important de surveiller et détecter les activités malveillantes en cours d'exécution, aux niveaux applicatifs et réseaux.

- HIPS (analyse comportementale applicative)
- Détection du trafic malveillant (analyse comportementale réseaux)

Vous trouverez une description de chacune de ces technologies dans la section sur les fonctionnalités de Sophos Endpoint Protection Advanced.

5. SOLUTIONS DE PROTECTION ENDPOINT NEXT-GEN ET VISION DE SOPHOS

Quelle est l'origine des technologies de protection Endpoint Next-Gen de Sophos ?

Les principales technologies de protection Endpoint Next-Gen de Sophos proviennent de l'acquisition de deux sociétés pionnières dans ce domaine, aux performances éprouvées.

En décembre 2015, Sophos a fait l'acquisition de la société d'origine néerlandaise SurfRight, bien connue pour sa solution HitmanPro Alert. SurfRight apporte plus de dix ans d'expérience dans la mise au point d'une des meilleures solutions anti-exploit du marché, déjà déployée par des millions d'utilisateurs. Elle a également conçu une gamme étendue de protections Next-Gen allant de l'anti-ransomware au nettoyage en profondeur. Ces technologies ont été intégrées dans la solution Endpoint Next-Gen de Sophos Intercept X, lancée en septembre 2016. Sophos Intercept X a passé avec succès l'épreuve de la flambée de ransomwares qui ont sévi depuis cette date, dont les toutes récentes attaques de WannaCry et NotPetya, sans avoir nécessité de mise à jour.

En février 2016, Sophos a fait l'acquisition de la société Invincea, un des plus grands experts mondiaux dans le domaine des technologies de Deep Learning appliquées à la détection anti-malware. Invincea apporte plus de dix ans d'expérience de recherche et développements avancés, menés pour des organismes à la pointe de l'innovation tels que l'agence américaine de recherche avancée dans le domaine de la défense DARPA (American Defense Advanced Research Projects Agency). Cette solution a obtenu les meilleurs résultats de tous les éditeurs de solutions Endpoint Next-Gen lors des tests anti-malware d'organisations reconnues comme AV-Test.org. Les Data Scientits d'Invincea ont joint leur expertise à celle des analystes des SophosLabs pour entraîner leur moteur de Deep Learning sur l'ensemble des bases de données de malwares et de données légitimes des SophosLabs. Ceci a permis d'accroître encore l'étendue des capacités de détection et la précision de ces technologies, qui sont désormais disponibles avec Sophos Intercept X dans le cadre d'un programme d'accès anticipé.

Certaines technologies Endpoint Next-Gen ont-elles été développées en interne par Sophos ?

Absolument. Des capacités importantes telles que l'analyse des causes de l'attaque (Root Cause Analysis) et la Sécurité Synchronisée sont issues de projets de recherche et développements avancés internes.

Quelle est la vision de Sophos pour son offre Endpoint Next-Gen ?

L'objectif de Sophos Intercept X est de fournir un agent de protection Next-Gen qui exploite notre compréhension des méthodes les plus avancées utilisées par les pirates. Avec plusieurs centaines de milliers de nouvelles variantes de malwares créées chaque jour, le but est de détecter les méthodes utilisées par les pirates au lieu des millions d'échantillons individuels qui ont été collectés. Nous savons également que les attaques n'utilisent pas toujours les malwares ou que si un malware est utilisé il ne sera pas toujours transmis par fichier ou par exécutable pouvant être analysé. Les attaques modernes exploitent souvent des composants systèmes légitimes ou elles peuvent résider simplement dans l'espace mémoire d'un processus compromis. Pour fournir une protection complète, une nouvelle approche est nécessaire. Intercept X fournit cette nouvelle approche.

Nous sommes aussi conscients que beaucoup d'organisations souhaitent conserver leur protection Endpoint traditionnelle en place et simplement la compléter par des capacités de protection Next-Gen de pointe. C'est pourquoi Sophos Intercept X est conçue pour fonctionner conjointement avec n'importe quelle solution antivirus du marché. Bien entendu, elle peut également être déployée comme agent de protection unique et intégré avec Sophos Endpoint Protection Advanced.

Quelles sont les principales fonctions de sécurité fournies par Intercept X ?

Intercept X intègre une gamme étendue de fonctionnalités de protection Endpoint Next-Gen:

PRÉVENTION DE L'EXÉCUTION

Deep Learning[1]

Evaluation en pré-exécution sans signature de tout fichier exécutable pour déterminer s'il s'agit d'un malware, d'un logiciel potentiellement indésirable ou d'une application légitime.

[1] Disponible dans le cadre du programme d'accès anticipé Sophos

DÉTECTION LORS DE L'EXÉCUTION

CryptoGuard

Détection des activités malveillantes de chiffrement et restauration des fichiers chiffrés (anti-ransomware), se basant sur la détection des tentatives malveillantes de modification ou de chiffrement de fichiers.

WipeGuard

Détection et blocage des tentatives de chiffrement ou de modification malveillante du secteur de boot, à l'exemple de l'attaque menée par le ransomware NotPetya.

Prévention des exploits

Détection et blocage de plus de 20 techniques d'exploits utilisées pour compromettre les applications vulnérables (voir la liste dans la section détaillée sur les anti-exploits plus haut).

Verrouillage des applications

Prévention des comportements malveillants des applications, telles que les macros Word qui installent d'autres applications et les exécutent (navigateurs Web, plugins, Java, applications media, MS Office...).

Navigation sécurisée

Surveillance des interfaces cryptographiques, réseaux et de présentation des navigateurs Web, pour détecter les attaques de type « man-in-the-browser », courantes dans de nombreux chevaux de Troie bancaires.

RÉPONSES

Root Cause Analysis

Analyse visuelle et détaillée de l'origine de l'attaque, de son cheminement et des ressources affectées (fichiers, registres ...).

Sophos Clean

Elimination en profondeur des malwares et des applications potentiellement indésirables, et restauration de tous les éléments affectés (fichiers, base de registres ...).

Sophos Central

Gestion centralisée par la console Sophos Central, assurant la supervision, les alertes, l'édition de rapports et les API externes.

Synchronized Security

Synchronisation en temps réel des solutions Sophos pour partager les informations, automatiser les réponses et accélérer l'analyse.

Comment la solution Intercept X complète-t-elle les protections traditionnelles comme Sophos Endpoint Protection Advanced ?

Intercept X est un complément idéal pour les solutions de protection traditionnelles telles que Sophos Endpoint Protection Advanced, qui fournit elle-même des fonctions de sécurité essentielles:

RÉDUCTION DE LA SURFACE D'EXPOSITION

Sécurité et contrôle du Web — Blocage des sites Web infectieux et serveurs de Commande & Contrôle, ainsi que filtrage des URLs par catégories selon la politique de sécurité.

Contrôle des périphériques — Contrôle des périphériques amovibles (clés USB, disques amovibles …) selon la politique de sécurité sur l'échange et le stockage de données.

Contrôle des applications — Contrôle des applications pour éviter les versions obsolètes (navigateurs Web …) et les applications indésirables (téléchargement P2P …).

Contrôle des données (DLP): — Prévention de la fuite d'informations à caractère personnel ou confidentiel par l'analyse du contenu des fichiers sortants.

PRÉVENTION DE L'EXÉCUTION

Réputation du téléchargement — Détection des téléchargements dangereux, avec option de dialogue de confirmation pour les fichiers exécutables.

Scan à base de signatures — Détection par signatures offrant une première ligne de sécurité rapide et efficace contre les menaces connues.

Analyse heuristique — Blocage des nouvelles variantes et des malwares Zero-Day inconnus par une détection de combinaisons de génotypes précise et fiable.

Émulation — Exécution des programmes dans un environnement contrôlé pour dévoiler et révéler leurs composants exécutables malveillants.

Sandboxing & Live Lookup — Analyse en temps réel par Les SophosLabs des échantillons obtenus par les réseaux de Labs, Honeypots et solutions, puis accès par Live Lookup.

DÉTECTION LORS DE L'EXÉCUTION

Analyse comportement (HIPS): — Surveillance des processus à l'exécution pour bloquer les actions malveillantes, avec corrélation entre règles et génotypes suspects.

Détection du trafic malveillant — Blocage des tentatives de communications vers les serveurs de Commande & Contrôle ou de distribution de malwares.

RÉPONSES

Quarantaine et nettoyage — Neutralisation et mise en quarantaine des malwares, avant leur élimination lors du nettoyage.

Sophos Central — Gestion centralisée par la console Sophos Central, assurant la supervision, les alertes, l'édition de rapports et les API externes.

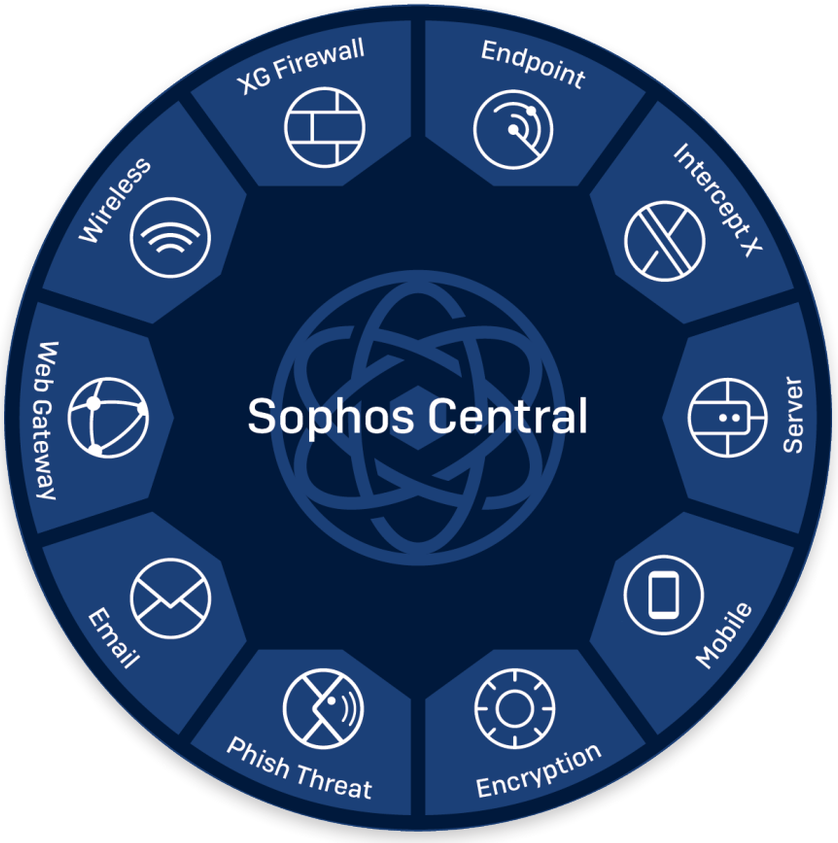
Synchronized Security — Synchronisation en temps réel des solutions Sophos pour partager les informations, automatiser les réponses et accélérer l'analyse.

Quelles sont les solutions gérées par la console d'administration Sophos Central ?

Sophos Intercept X et Sophos Endpoint Protection Advanced sont gérés par la même console d'administration Sophos Central.

Cette console permet également de gérer d'une façon unifiée les autres solutions de protection Sophos, telles que Sophos Server, Sophos Mobile, Sophos Encryption, Sophos Email, Sophos Web, Sophos Wireless et Sophos Phish Threat.

Ceci permet d'assurer une administration cohérente des principales fonctions de sécurité, pour créer et gérer simplement des politiques de sécurité centrées sur les utilisateurs.



Elle permet également de mettre en œuvre la synchronisation de la sécurité entre les produits, pour partager des informations contextuelles sur les événements suspects et automatiser la réponse aux menaces.

Cette synchronisation est particulièrement importante entre les protections Réseaux et Endpoint. Elle permet par exemple d'identifier et d'isoler automatiquement un système compromis au niveau réseau. Elle permet également d'identifier précisément l'origine (système, utilisateur et application) de l'intégralité du trafic réseau venant des systèmes, ce qui fait gagner un temps précieux dans l'analyse de l'origine des attaques et élimine un des angles morts des politiques de filtrage applicatif dont souffrent les firewalls Next-Gen actuels.

6. CONCLUSION

Il existe aujourd'hui de nombreuses définitions de la sécurité Endpoint Next-Gen. Ceci complique parfois le choix d'une technologie appropriée. Avec une surface d'attaque toujours plus étendue, une complexité accrue et un volume de risques croissants, que doivent gérer des équipes restreintes dans un contexte de pénurie d'experts en sécurité, la situation est de plus en plus difficile pour les équipes de sécurité informatique.

Les approches qui combinent de multiples produits d'éditeurs différents ajoutent une complexité inutile aux problèmes déjà rencontrés. Il est préférable de déployer des solutions qui soient simples et efficaces à la fois, automatisées et coordonnées, en un mot synchronisées, grâce à des innovations technologiques telles que Sophos Security Heartbeat™.

Grâce à l'acquisition et l'intégration de technologies Next-Gen bénéficiant de plus d'une décennie de recherche et de mise en œuvre dans les domaines du Deep Learning et de l'anti-exploit, Sophos est en mesure de proposer le meilleur des solutions de protection traditionnelles et de sécurité Next-Gen, le tout intégré dans une console d'administration unique Sophos Central et synchronisé avec sa protection réseaux XG Firewall.

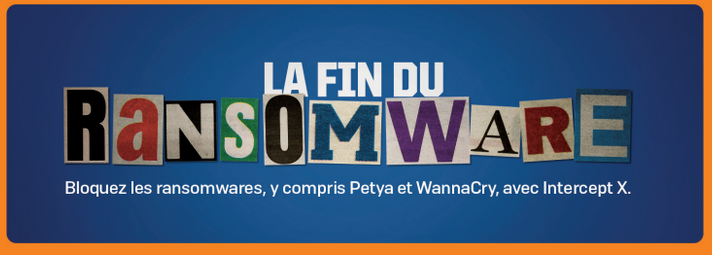
La bonne nouvelle est que ces fonctionnalités Next-Gen sont disponibles dès aujourd'hui chez Sophos et peuvent être évaluées facilement.

Pour en savoir plus et découvrir comment Sophos Intercept X et Sophos Endpoint Protection peuvent mieux protéger votre entreprise, consultez sophos.fr/intercept-x.

INTERCEPT X

Une nouvelle approche de la sécurité endpoint.

- Anti-Ransomware
- Protection contre les Exploits
- Technologies de Deep Learning
- Analyse de l'origine des attaques
- Rémédiation et nettoyage avancés
- 100% Next-Generation
- Complète les protections anti-virus classiques



SOPHOS

Security made simple.

Sophos Sarl | 80 Quai Voltaire | 95870 Bezons - Tel. 01 34 34 80 00
www.sophos.fr | Blog : sophosfrance.fr