SOPHOS
Security made simple.

Intercept X Deep Learning

Intercept X allie le Deep Learning avec des technologies inégalées anti-exploit, anti-ransomware (CryptoGuard) et d'analyse détaillée des attaques (RCA) pour constituer la protection Endpoint la plus complète du marché. Cette combinaison unique de fonctionnalités permet à Intercept X de stopper la plus grande variété de menaces.

Principaux avantages

- Le moteur de détection des malwares le plus performant du marché
- Protège contre les malwares connus et inconnus
- Bloque les malwares avant leur exécution
- Ne se repose pas sur les signatures
- Protège l'hôte même quand il est déconnecté
- Détecte les malwares en ~20 millisecondes
- Apprentissage sur des centaines de millions d'échantillons
- Reconnu par VirusTotal depuis août 2016
- Classe les fichiers comme malveillants, applications potentiellement indésirables (PUA) et inoffensifs
- Immédiatement opérationnel sans formation supplémentaire requise
- Très faible empreinte (moins de 20 Mo)
- Se concentre sur les fichiers Portable Executable de Windows

La plupart des solutions actuelles n'anticipent pas assez et sont trop lentes. Comme le volume et la complexité des attaques des systèmes d'extrémité ont continué de croître, les approches traditionnelles ont du mal à suivre le rythme. Pour exemple, les SophosLabs analysent plus de 400 000 nouveaux échantillons de malwares chaque jour. Pour rendre la tâche encore plus difficile, les SophosLabs ont trouvé que 75 % des malwares sont uniques à l'entreprise qu'ils attaquent.

Le Deep Learning, en tant que forme de Machine Learning, participe à la création d'une nouvelle approche de la sécurité Endpoint, et en la matière, Intercept X est précurseur. En intégrant le Deep Learning, Intercept X transforme la sécurité Endpoint d'une approche réactive vers une approche proactive.

Deep Learning vs. autres types de Machine Learning

« Intercept X utilise un réseau neuronal de Deep Learning qui fonctionne comme un cerveau humain… Cela se traduit par un taux élevé d'identification des malwares existants et Zero-Day, et par un faible taux de faux positifs. »

Rapport ESG Lab, décembre 2017

Alors que de nombreux produits prétendent utiliser le Machine Learning, ce dernier n'est pas toujours créé de manière égale. Chez Sophos, nous utilisons le Deep Learning pour détecter les malwares. Également connu sous le nom de « réseaux neuronaux profonds » ou « réseaux neuronaux », le Deep Learning a été conçu sur le modèle du cerveau humain. Il s'agit du même genre d'apprentissage automatique fréquemment utilisé pour la reconnaissance faciale, le traitement du langage naturel, les voitures sans chauffeur, et d'autres champs avancés de la recherche en informatique.

Le Deep Learning a systématiquement surpassé les autres modèles de Machine Learning, notamment les forêts d'arbres décisionnels, l'algorithme des k-moyennes ou les réseaux Bayésiens, mais pour que le modèle soit efficace, il nécessite une vaste quantité de données et de puissance de calcul. Chez Sophos, nous y sommes parvenus en toute simplicité grâce à la collection de malwares et aux efforts d'analyse des SophosLabs de ces 30 dernières années, ainsi qu'aux données télémétriques de plus de 100 millions de systèmes d'extrémité reçues chaque jour.

Le Deep Learning a des avantages intrinsèques par rapport aux autres types de Machine Learning couramment utilisés dans la sécurité Endpoint :

Plus intelligent : Un modèle de Deep Learning traite les données au travers de multiples couches d'analyse, exactement comme les neurones d'un cerveau humain, chaque couche renforçant la puissance du modèle. Il analyse des relations complexes entre des éléments d'entrée différents. Cela lui permet de découvrir automatiquement les meilleures combinaisons et manipulations possibles des entrées, calculs que le cerveau humain serait incapable de déterminer seul. Cela signifie que le modèle de détection des malwares par Deep Learning sera capable de détecter les malwares habituellement non identifiés par d'autres moteurs de Machine Learning.

Plus évolutif : Grâce à des centaines de millions d'échantillons test, le modèle de Deep Learning se développe avec la plus grande facilité. Ce qui est très important, compte tenu du fait que les SophosLabs analysent chaque semaine 2,8 millions de nouveaux échantillons de malwares. Pouvant ingérer une quantité astronomique de données, notre modèle peut « mémoriser » le panorama entier des menaces visibles dans le cadre du processus d'apprentissage. En traitant bien plus de données, le Deep Learning peut prédire plus précisément les menaces d'aujourd'hui, tout en continuant de rester à la pointe au fil du temps.

Plus léger : Les approches traditionnelles du Machine Learning aboutissent à des modèles de grande dimension, prenant parfois plusieurs gigaoctets sur le disque. À l'inverse, l'approche de Deep Learning de Sophos résulte en des modèles hautement compressés. Ces derniers sont en effet incroyablement petits, avec moins de 20 Mo sur le système d'extrémité, et ils n'ont presque aucune incidence sur les performances.

Les capacités de Deep Learning de Sophos

Sophos est un expert du Deep Learning grâce à son moteur de détection des malwares le plus performant du marché :

Expérimenté : Contrairement à nos concurrents, nous sommes des experts du Machine Learning en cybersécurité depuis très longtemps, et nous développons nos modèles de détection des malwares par Deep Learning depuis des années. Ces derniers ont été conçus par notre équipe d'analystes de données en suivant les règles de la DARPA (Defense Advanced Research Projects Agency) aux États-Unis. En 2010, la DARPA a créé le « Cyber Genome Program » pour découvrir l'« ADN » des malwares et des autres cyber menaces. Cette initiative est à l'origine de l'algorithme aujourd'hui présent dans Intercept X.

Éprouvé : Nous sommes ouverts et transparents avec notre modèle. En plus de présenter notre méthodologie lors de conférences de l'industrie, comme lors du Black Hat, nous n'avons pas hésité à proposer à des tiers indépendants de tester notre modèle. Il a ainsi été éprouvé sur VirusTotal depuis août 2016 et a reçu des scores élevés par des tiers l'ayant testé, comme NSS Labs. Dans tous les cas, il s'est montré extrêmement efficace avec un taux de faux positifs très bas.

« Un des meilleurs résultats de performance que nous n'ayons jamais vu dans nos tests. »

Maik Morgenstern, CTO, AV-TEST

Performances : La technologie de Deep Learning de Sophos est incroyablement rapide. En moins de 20 millisecondes, le modèle a été capable d'extraire des millions d'éléments d'un fichier, de réaliser une analyse profonde et de déterminer si le fichier est inoffensif ou malveillant. La totalité du processus se déroule avant même que le fichier ne s'exécute.

SophosLabs : Un des aspects les plus importants de n'importe quel modèle sont les données utilisées pour l'apprentissage. Notre équipe d'analystes de données fait partie intégrante de nos SophosLabs, leur permettant d'accéder à des centaines de millions d'échantillons. Il peuvent ainsi créer les meilleures prédictions possibles dans nos modèles. L'intégration entre ces deux groupes de recherche mène également à une meilleure catégorisation des données (et donc à un meilleur modèle). Le partage bidirectionnel de l'intelligence sur les menaces et des retours d'informations entre ces deux équipes améliore en continu la précision de nos modèles

« Intercept X a stoppé toutes les attaques complexes et avancées auxquelles nous l'avons soumis. »

Rapport ESG Lab, décembre 2017

Essayez-le gratuitement dès aujourd'hui

Inscrivez-vous pour participer à une évaluation gratuite de 30 jours sur sophos.fr/interceptx

Équipe commerciale France :
Tél. : 01 34 34 80 00
Email : info@sophos.fr

18-01-02 DS FR (2897-DD)

SOPHOS