SOPHOS
Security made simple.

Intercept X Deep Learning

Intercept X kombiniert Deep Learning mit branchenführender Anti-Exploit-Technologie, CryptoGuard-Anti-Ransomware, Ursachenanalyse und mehr: Das Ergebnis ist die marktweit umfassendste Endpoint-Sicherheit, die mit einer einmaligen Kombination leistungsstarker Funktionen mehr Endpoint-Bedrohungen stoppt als je zuvor.

Highlights

- Die branchenweit leistungsstärkste Malware-Erkennungsengine
- Wehrt bekannte und unbekannte Malware ab
- Blockiert Malware vor Ausführung
- Stützt sich nicht auf Signaturen
- Schützt auch dann, wenn der Host offline ist
- Erkennt Malware in rund 20 Millisekunden
- Auf Hunderte Millionen von Samples „trainiert“
- Seit August 2016 bewährt auf VirusTotal
- Klassifiziert Dateien als schädlich, potenziell unerwünschte Anwendungen (PUAs) oder unbedenklich
- Ist direkt und ohne zusätzliches Training einsatzbereit
- Extrem kleiner Footprint (weniger als 20 MB)
- Fokus auf übertragbare ausführbare Windows-Dateien

Heutige IT-Sicherheit ist meist reaktiv und viel zu langsam. Gleichzeitig nehmen Endpoint-Angriffe stetig zu und werden immer raffinierter. Daher stoßen herkömmliche Abwehrmechanismen zusehends an ihre Grenzen. Die SophosLabs analysieren täglich mehr als 400.000 neue Malware-Samples. 75 % dieser Malware wurde gezielt für bestimmte Unternehmen entwickelt.

Deep Learning, eine Weiterentwicklung des Machine Learning, revolutioniert die Endpoint-Sicherheit und Intercept X steht an der Spitze dieser Revolution. Durch die Integration von Deep Learning verwandelt Intercept X reaktive Endpoint-Sicherheit in prädiktive Endpoint-Sicherheit und schützt zuverlässig vor unbekannten Bedrohungen.

Deep Learning im Vergleich zu anderen Arten des Machine Learning

„Intercept X nutzt ein neuronales Deep-Learning-Netzwerk, das wie ein menschliches Gehirn funktioniert … Mit dem Ergebnis, dass sowohl bereits bekannte als auch Zero-Day-Malware sehr genau erkannt und die False-Positive-Rate gesenkt wird.“

ESG Lab Report, Dezember 2017

Viele Anbieter werben damit, dass ihre Produkte auf Machine Learning basieren. Machine Learning ist jedoch nicht gleich Machine Learning. Bei Sophos setzen wir zur Erkennung von Malware auf das sogenannte „Deep Learning“. Deep Learning – oft auch als „neuronale Deep-Learning-Netzwerke“ oder „neuronale Netzwerke“ bezeichnet – ist von der Funktionsweise des menschlichen Gehirns inspiriert. Es handelt sich um dieselbe Art des Machine Learning, die auch häufig zur Gesichtserkennung, zur natürlichen Sprachverarbeitung, bei selbstfahrenden Autos und in weiteren anspruchsvollen Bereichen der Computerwissenschaft und -forschung zum Einsatz kommt.

Deep Learning war anderen Machine-Learning-Modellen in der Vergangenheit durchweg überlegen (einschließlich Random Forest, K-Means-Clustering und Bayesschen Netzen), ist jedoch zur Erstellung eines effektiven Modells auf riesige Datenmengen und eine hohe Rechenleistung angewiesen. Bei Sophos konnten wir diese Herausforderung mühelos meistern: Unsere SophosLabs sammeln und analysieren bereits seit 30 Jahren Malware-Daten und unsere mehr als 100 Mio. Endpoints liefern uns täglich Telemetriedaten.

Deep Learning hat wesentliche Vorteile gegenüber anderen Arten des Machine Learning, die gewöhnlich in Endpoint-Security-Produkten zum Einsatz kommen:

Intelligenter: Deep-Learning-Modelle verarbeiten Daten über mehrere Analyseebenen – genau wie Neuronen im menschlichen Gehirn. Jede Ebene trägt zu einer erheblichen Performance-Steigerung des Modells bei. Deep Learning ermöglicht die automatische Erkennung relevanter Eigenschaften und von deren Abhängigkeiten untereinander, was in dieser Komplexität von Menschen nicht bewältigbar wäre. Auf diese Weise kann unser Deep-Learning-Modell auch Malware erkennen, die andere Machine Learning Engines übersehen.

Skalierbarer: Deep Learning lässt sich problemlos auf Hunderte Millionen Training-Samples skalieren. Dieser Punkt ist entscheidend, weil die SophosLabs wöchentlich 2,8 Mio. neue Malware-Samples analysieren. Unser Modell kann unbegrenzt riesige Mengen von Trainingsdaten aufnehmen und ist so in der Lage, sich im Rahmen des Trainingsprozesses die gesamte beobachtbare Bedrohungslandschaft einzuprägen. Da das Modell weit mehr Eingaben verarbeiten kann, sagt Deep Learning Bedrohungen heute genauer vorher und bleibt auch in Zukunft immer auf dem neuesten Stand.

Kompakter: Herkömmliche Machine-Learning-Ansätze führen zu riesigen Modellgrößen und beanspruchen viele Gigabytes auf der Festplatte. Unser Deep-Learning-Ansatz hingegen generiert stark komprimierte Modelle. Das Deep-Learning-Modell von Sophos ist äußerst kompakt (weniger als 20 MB auf dem Endpoint), sodass die Performance praktisch nicht beeinträchtigt wird.

Sophos Deep Learning – Konkurrenzlos

Unsere Deep-Learning-Funktionen stellen wir mit unserer Malware-Erkennungsengine bereit, die branchenweit die leistungsstärkste ist:

Erfahren: Anders als unsere Wettbewerber sind wir schon seit langer Zeit Machine-Learning-Experten auf dem Gebiet der Cybersecurity und betreiben unsere Deep-Learning-Modelle zur Erkennung von Malware bereits seit Jahren in Produktionsumgebungen. Das Sophos-Malware-Erkennungsmodell wurde von unserem Datenwissenschaftlerteam mit DARPA-gestützter Technologie entwickelt. 2010 entwickelte die US-Behörde Defense Advanced Research Projects Agency (DARPA) ihr Cyber Genome Program, um die „DNA" von Malware und Cyberbedrohungen aufzudecken. Dies war der Ursprung des Algorithmus, der nun in Intercept X eingebettet ist.

Bewährt: Wir waren und sind in Bezug auf unsere Modelle offen und transparent. Wir haben die Einzelheiten unserer Methodologie auf Branchenkonferenzen wie Black Hat vorgestellt und durch unabhängige Dritte testen lassen. Unser Modell hat sich seit August 2016 auf VirusTotal bewährt und von unabhängigen Testinstituten wie den NSS Labs Top-Bewertungen erhalten. In allen Fällen hat es sich als hocheffektiv erwiesen und generiert sehr wenige False Positives.

„Einer der besten Performance Scores, den wir bei unseren Tests jemals beobachten konnten."

Maik Morgenstern, CTO, AV-TEST

Performance: Unsere Deep-Learning-Technologie ist extrem schnell. In weniger als 20 Millisekunden ist das Modell in der Lage, Millionen von Eigenschaften aus einer Datei zu extrahieren, eine Tiefenanalyse durchzuführen und zu ermitteln, ob eine Datei unbedenklich oder schädlich ist. Der gesamte Prozess läuft vor der Dateiausführung ab.

SophosLabs: Einer der wichtigsten Aspekte bei jedem Modell sind die für das Training verwendeten Daten. Unser Datenwissenschaftlerteam ist Teil der SophosLabs-Gruppe und hat daher Zugriff auf Hunderte Millionen von Samples. So kann das Team die bestmöglichen Vorhersagen in unsere Modelle integrieren. Die Integration zwischen den beiden Gruppen führt auch zu einer besseren Datenkennzeichnung (und somit zu einer besseren Modellierung). Der bidirektionale Austausch von Bedrohungsdaten und Feedback aus der Praxis zwischen dem Datenwissenschaftlerteam und den Bedrohungsanalysten führt zu einer kontinuierlichen Optimierung unserer Modelle.

„Intercept X hat jeden komplexen, hochentwickelten Angriff gestoppt, mit dem wir die Lösung konfrontiert haben".

ESG Lab Report, Dezember 2017

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion
unter www.sophos.de/interceptx

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

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

SOPHOS