SOPHOS
Security made simple.

Deep Learning de Intercept X

Intercept X combina el Deep Learning con la mejor tecnología antiexploits, la tecnología anti-ransomware CryptoGuard, el análisis de causa raíz y mucho más para ofrecer la protección para endpoints más completa de la industria. Esta combinación de funciones única permite que Intercept X detenga la más amplia variedad de amenazas para endpoints.

Aspectos destacados

- El motor de detección de malware de mayor rendimiento
- Evita el malware conocido y nunca antes visto
- Bloquea el malware antes de que se ejecute
- No depende de firmas
- Protege incluso cuando el host está desconectado
- Detecta malware en aproximadamente 20 milisegundos
- Se entrena con cientos de millones de muestras
- Probado en VirusTotal desde agosto de 2016
- Clasifica los archivos como maliciosos, aplicaciones no deseadas o benignas
- Funciona directamente sin formación adicional
- Ocupa muy poco espacio (menos de 20 MB)
- Se centra en ejecutables portátiles de Windows

La mayor parte de la seguridad actual es reactiva y demasiado lenta. Mientras que el volumen y la complejidad de los ataques de endpoints han ido en aumento, los enfoques antiguos tienen dificultades para seguir el ritmo. Por ejemplo, SophosLabs analiza más de 400 000 muestras de malware nuevas cada día. Para dificultar aún más este reto, SophosLabs ha comprobado que el 75 % del malware es específico para una única organización.

El Deep Learning, una forma avanzada de aprendizaje automático, está ayudando a cambiar la forma de afrontar la seguridad de endpoints, e Intercept X lidera el cambio. Al integrar el Deep Learning, Intercept X está cambiando el enfoque de la seguridad de endpoints para proteger contra amenazas desconocidas, que pasa de reactivo a predictivo.

El Deep Learning frente a otros tipos de aprendizaje automático

"Intercept X utiliza una red neuronal de Deep Learning que funciona como el cerebro humano... El resultado en un elevado índice de precisión tanto para programas maliciosos existentes como de día cero, así como un índice menor de falsos positivos".

Informe de ESG Lab, diciembre de 2017

Aunque muchos productos afirman utilizar el aprendizaje automático, no todo el aprendizaje automático se crea de la misma manera. En Sophos, usamos el Deep Learning para detectar malware. El Deep Learning, también llamado "redes neuronales de aprendizaje profundo" o "redes neuronales", está inspirado en la forma en la que funciona el cerebro humano. Es el mismo tipo de aprendizaje automático que suele usarse para el reconocimiento facial, el procesamiento del lenguaje natural, los vehículos sin conductor y otros campos avanzados de la ciencia y la investigación informática.

El Deep Learning ha superado sistemáticamente a otros modelos de aprendizaje automático, como los bosques aleatorios, la agrupación mediante el algoritmo k-means o las redes bayesianas, pero requiere enormes cantidades de datos y potencia computacional para crear un modelo eficaz. En Sophos, esto ha sido sencillo gracias a la recopilación de malware y las tareas de análisis de SophosLabs durante los últimos 30 años y a la telemetría que recibimos de nuestros más de 100 millones de endpoints cada día.

Deep Learning de Intercept X

El Deep Learning cuenta con varias ventajas inherentes en comparación con otros tipos de aprendizaje automático utilizados habitualmente en la seguridad de endpoints:

Más inteligente: Los modelos de Deep Learning procesan datos a través de múltiples capas de análisis, como las neuronas en el cerebro humano, y cada capa hace el modelo mucho más potente. Analiza las relaciones complejas entre distintas funciones de entrada. Esto le permite detectar automáticamente la mejor combinación y manipulación de entradas, imposibles de determinar para los humanos. Gracias a ello, el modelo de detección de malware de Deep Learning de Sophos es capaz de detectar programas maliciosos que pasarían inadvertidos a otros motores de aprendizaje automático.

Más escalable: El Deep Learning se adapta con elegancia a cientos de millones de muestras de entrenamiento. Esto es importante teniendo en cuenta que SophosLabs analiza 2,8 millones de muestras de malware nuevas cada semana. Dado que puede seguir procesando enormes cantidades de datos de entrenamiento, nuestro modelo puede "memorizar" todo el panorama de amenazas observable como parte de su proceso de aprendizaje. Como puede procesar muchos más datos, el Deep Learning puede predecir amenazas actualmente con mayor precisión, a la vez que se mantiene al día con el paso del tiempo.

Más ligero: Los enfoques de aprendizaje automático tradicionales dan lugar a modelos de enorme tamaño, que a menudo pueden ocupar muchos gigabytes en el disco. Sin embargo, el enfoque de Deep Learning de Sophos genera modelos muy comprimidos. El modelo de Deep Learning de Sophos es increíblemente pequeño, menos de 20 MB en el endpoint, con prácticamente un impacto nulo en el rendimiento.

Funciones del Deep Learning de Sophos

Sophos ofrece una experiencia en Deep Learning con el motor de detección de malware de mayor rendimiento de la industria:

Experiencia: A diferencia de la competencia, somos expertos en el aprendizaje automático de ciberseguridad desde hace mucho tiempo y nuestros modelos de Deep Learning de detección de malware llevan en entornos de producción desde hace años. Nuestro equipo de científicos de datos creó el modelo de detección de malware de Sophos con tecnología de la DARPA. En el año 2010, la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa (DARPA) de EE. UU. creó el Cyber Genome Program a fin de revelar el "ADN" del malware y otras ciberamenazas. Ese fue el origen de lo que es hoy el algoritmo incorporado en Intercept X.

Probado: Hemos sido abiertos y transparentes con nuestros modelos. Además de ofrecer información detallada sobre nuestra metodología en conferencias del sector como Black Hat, no nos hemos negado a que terceros independientes pongan a prueba nuestro modelo. El modelo se ha probado en VirusTotal desde agosto de 2016 y ha obtenido muy buenos resultados en pruebas independientes de terceros como NSS Labs. En todos los casos, ha demostrado ser sumamente eficaz con un porcentaje reducido de falsos positivos.

"Una de las mejores puntuaciones de rendimiento que hemos visto en nuestras pruebas".

Maik Morgenstern, director tecnológico de AV-TEST

Rendimiento: La tecnología de Deep Learning de Sophos es increíblemente rápida. En menos de 20 milisegundos, el modelo puede extraer millones de características de un archivo, efectuar un análisis profundo y determinar si es benigno o malicioso. Todo este proceso tiene lugar antes de que se ejecute el archivo.

SophosLabs: Uno de los aspectos más importantes de cualquier modelo son los datos que se utilizan para el aprendizaje. Nuestro equipo de científicos de datos forma parte del grupo SophosLabs, lo que les da acceso a cientos de millones de muestras y les permite crear las mejores predicciones posibles en nuestros modelos. La integración entre los dos grupos también conlleva un mejor etiquetado de datos (y, por tanto, un mejor modelado). El intercambio bidireccional de información sobre amenazas y datos del mundo real entre el equipo de científicos de datos y los investigadores de amenazas mejora continuamente la precisión de nuestros modelos.

"Intercept X detuvo cada uno de los ataques complejos avanzados con que lo retamos".

Informe de ESG Lab, diciembre de 2017

Pruébelo gratis hoy mismo

Regístrese en es.sophos.com/interceptx para probarlo gratis durante 30 días

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

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

SOPHOS