SOLUTION BRIEF

Deep Instinct Prevention Platform

DETIENE RANSONWARE ANTES DE QUE COMIENCE A CIFRAR	PREVIENE **> 99%** ATAQUES CONOCIDOS, DESCONOCIDOS, ZERO-DAY	GARANTIZA **< 0,1%** FALSOS POSITIVOS	**< 20 MS** EN PREVENCIÓN DE MALWARE

Cada día se descubren 350.000 piezas nuevas de malware, y este número crece exponencialmente. Los ataques de "zero-day", "ransomware", "filed-based", "fileless", "supply chain", y "adversarial AI" continúan cambiando y evadiendo su detección, lo que hace que sea extremadamente difícil evitar que los delincuentes cibernéticos se infiltren en su red híbrida. El camino a seguir para recuperar el control es un enfoque innovador que priorice la prevención gracias al aprendizaje profundo ("Deep-Learning").

Hoy en día, el trabajo descentralizado como nueva norma, la continua transformación digital y las redes distribuidas ha hecho que la informática se acerque más al límite. Proteger sus terminales y estaciones de trabajo nunca ha sido más importante.

Pero no es solo el terminal. Los delincuentes cibernéticos pueden infectar los sistemas a través de archivos almacenados en la nube, archivos cargados a través de aplicaciones y descargados en los clientes, y archivos que los usuarios finales están descargando desde Internet. Los antivirus tradicionales solo evitarán las amenazas conocidas. EDR ("Endponint Detection and Response") por sí solo no es suficiente para detener lo desconocido antes de que se ejecute en su red.

Debemos repensar nuestro enfoque de la prevención.

Plataforma de prevención de Deep Instinct

La plataforma de prevención de Deep Instinct detiene amenazas conocidas, desconocidas y de día cero con la mayor precisión y tasa de falsos positivos más baja de la industria. Para su organización, esto significa un riesgo reducido, una mayor eficiencia del SOC y el saber que los atacantes han perdido su ventaja. Con una precisión en detección de amenazas conocidas, desconocidas y de día cero mayores del 99 %, una tasa de falsos positivos garantizada menor del 0,1 %, junto con una garantía de indemnización por ataques "ransomware" de 3 millones de euros respaldada por Munich Re, la plataforma de prevención de Deep Instinct cumple su promesa de una verdadera prevención.

Deep Instinct previene las amenazas antes de su ejecución, a diferencia de las soluciones tradicionales de detección y respuesta, que buscan comportamientos después de que el atacante ya haya instalado sus piezas de malware en su red. La plataforma de prevención de Deep Instinct reduce el riesgo de una intrusión al enfrentarse antes a los atacantes y detener las amenazas 750 veces más rápido de lo que el ransomware más rápido conocido puede comenzar a cifrar.

Deep Instinct previene los ataques en el punto final con análisis dinámico de múltiples capas y estático de extremo a extremo. Para enfrentarse al atacante incluso antes, Deep Instinct también previene el malware más allá del punto final al escanear los archivos en tránsito de sus aplicaciones y flujos de trabajo, así como el almacenamiento en la nube local, privada y pública y las pasarelas web, para evitar la carga o descarga de archivos maliciosos a la vez que garantiza la integridad de su entorno.

Deep Instinct impulsado por Deep Learning

Deep Instinct es la única empresa de ciberseguridad que aprovecha una red neuronal basada en el aprendizaje profundo ("Deep Learning") que aprende de forma autónoma y mejora dinámicamente a medida que recibe más datos.

El aprendizaje profundo es la forma más avanzada de IA Inteligencia Artificial), inspirada en la capacidad del cerebro para pensar y aprender con el tiempo. Nuestra vasta red neuronal ha sido entrenada durante más de cinco años con cientos de millones de archivos para prevenir amenazas de manera autónoma.

El aprendizaje profundo difiere del aprendizaje automático básico en varias líneas principales:

El aprendizaje automático básico requiere un experto en el ámbito humano, lo que lo hace lento y propenso a errores, y solo se entrena en el 2% de los datos disponibles. El aprendizaje profundo se entrena con el 100 % de los datos disponibles sin procesar y puede realizar automáticamente correlaciones no lineales de los datos. Con redes neuronales basadas en aprendizaje profundo diseñadas específicamente para la ciberseguridad, las decisiones se toman más rápido, con mayor precisión y con mucha mayor eficacia.

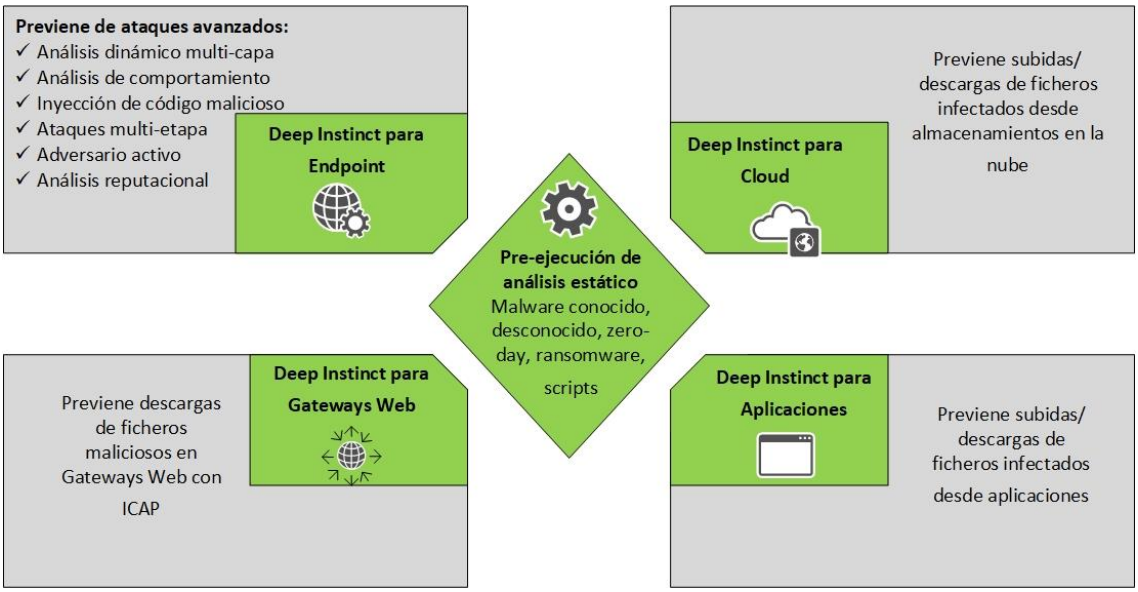
Un modelo de aprendizaje profundo es autosuficiente y no requiere actualizaciones frecuentes en la nube ni intervención humana constante.

En última instancia, el aprendizaje profundo es lo que permitirá a las organizaciones hacer realidad la prevención, prediciendo y deteniendo las amenazas antes de que se ejecuten y comprometan su entorno.

Lo que diferencia al producto

- Se integra con las soluciones de seguridad existentes para mejorar la eficiencia, la eficacia y centrarse en lo que realmente importa: detener los ataques.
- Reduce la carga de los equipos de seguridad para examinar los falsos positivos.
- Mejora las capacidades de búsqueda de amenazas con alertas de alta fidelidad y calificación de actividad sospechosa

Plataforma de Prevención de Deep Instinct



Deep Instinct para Endpoint

Deep Instinct para "Endpoint" (punto final) proporciona seguridad multicapa de extremo a extremo. En el momento en que un atacante intenta introducir un código útil malicioso en el punto final de destino, Deep Instinct lo previene, antes de que éste se ejecute.

Pre-ejecución: Análisis Estático

El motor de análisis estático de Deep Instinct protege de más del 99% de ataques de malware, tanto conocido como desconocido, incluyendo ataques de "ransomware", "zero-day", "filed-based", y "script-based".

- Malware conocido
- Malware desconocido & variantes
- Ataques file-based
- Zero-Day
- Ransomware
- Scripts comunes

En-ejecución: Análisis Dinámico del Comportamiento

Usando un enfoque de varias capas para la prevención, Deep Instinct emplea capas de análisis dinámico adicionales para detectar y automatizar las respuestas a las amenazas más avanzadas, incluidas las siguientes:

- Ataques "fileless" como inyección de código malicioso y robo de credenciales.
- Scripts avanzados como "shellcode" desconocido.
- Ataques multi-etapa.
- Ataques de Adversario Activo.

Además, Deep Instinct proporciona contexto adicional para comprender la gravedad y las tácticas de una amenaza, que incluye:

- Eventos sospechosos para la captura de amenazas
- Mapeo MITRE ATT&CK

Pos-Ejecución: Análisis automático

En la última capa de análisis automatizado, Deep Instinct puede anular las decisiones preventivas tomadas, basándose en la reputación o en la política.

Todos los eventos prevenidos se envían a la consola de Deep Instinct y se pueden integrar con su SIEM, SOAR, EDR u otras soluciones de seguridad a través de REST API, Syslog o SMTP.

Deep Instinct más allá del Endpoint

Escaneo de archivos en tránsito

Deep Instinct entiende que el punto final no es su único vector de ataque. Los archivos maliciosos pueden cargarse sin saberlo en su entorno híbrido distribuido o descargarse a sus clientes. Deep Instinct evita los archivos maliciosos al escanear los archivos en tránsito para garantizar la integridad de su almacenamiento en la nube local, privado y público y sus aplicaciones personalizadas, y evita las descargas de archivos maliciosos en la puerta de enlace web.

Deep Instinct para la Nube

Los archivos infectados almacenados en nubes públicas o privadas aumentan el riesgo de una filtración durante la descarga. Deep Instinct evita que los archivos maliciosos se carguen o descarguen de su almacenamiento en la nube pública o privada.

Deep Instinct para Aplicaciones

Su organización corre un riesgo mayor debido a las cargas de archivos internos y externos a través de sus aplicaciones personalizadas. Deep Instinct analiza los archivos en tránsito para asegurarse de que los archivos cargados a través de sus aplicaciones personalizadas y descargados en sus clientes estén libres de malware.

Deep Instinct para Gateways Web

Las soluciones tradicionales de AV e ICAP no detendrán las amenazas desconocidas en el proxy/gateway web.

Si actualmente estás utilizando un proxy web para filtrar el tráfico, Deep Instinct escaneará los archivos para evitar que los usuarios accedan a archivos maliciosos desde Internet. Deep Instinct se conecta con el protocolo ICAP para convertirse en el servidor ICAP y utiliza nuestro motor estático de aprendizaje profundo para capturar más del 99 % del malware conocido y desconocido.