AI POWERED

HORNETSECURITY

FACT SHEET

ADVANCED THREAT PROTECTION

Protección avanzada de correos electrónicos y datos basada en IA, incluso frente a las amenazas más sofisticadas.

Los ciberdelincuentes trabajan incansablemente para desarrollar nuevas ciberamenazas, lo que dificulta que el software de seguridad se mantenga actualizado y proteja a los usuarios de los nuevos métodos de ataque emergentes. El ransomware, el fraude del CEO, el phishing y los ataques combinados son sólo ejemplos de los peligros que acechan en el ciberespacio.

Con el auge de las herramientas de IA ampliamente disponibles, los ciberdelincuentes pueden crear sin esfuerzo correos electrónicos de phishing de aspecto impecable e incluso eludir las medidas de seguridad y utilizar herramientas de generación de texto de inteligencia artificial para crear códigos maliciosos.

Con Advanced Threat Protection, no tendrá que preocuparse por nada de lo anterior. Utilizando la IA a su favor, Advanced Threat Protection lo mantiene por delante de los ciberdelincuentes, protegiéndolo de ataques de día cero e incluso de las amenazas más sofisticadas.

¿Qué se ve afectado?

E-Mail

¿Cómo te ayuda Advanced Threat Protection?

Análisis forense selectivo basado en IA

Detecta amenazas nuevas e incluso las más sofisticadas.

Motor Sandbox

Prueba los adjuntos de correo electrónico en busca de archivos maliciosos en un entorno controlado.

Informes

Obten una visión completa de todos los intentos de ataque, alertas de seguridad, informes ATP y análisis forense.

¿Qué mejora?

Buzones de correo electrónico seguros

FILETYPES

- EXE
- PDF
- OFFICE
- ARCHIVE

BINARY ANALYTICS

- MACRO
- URL
- METADATA
- OBFUSCATION
- OBJECTS
- JAVASCRIPT
- HEURISTIC
- STATIC ANALYSIS
- ZERO HOUR THREAT OUTBREAK DETECION

SANDBOX

500+ BEHAVIOURAL ANALYSIS SENSORS

- ANTI VM EVASION DETECTION
- MACHINE LEARNING ENGINE
- FILESYSTEM MONITOR
- NETWORK TRAFFIC ANALYSIS
- PROCESS- AND REGISTRY MONITOR
- FORENSIC MEMORY ANALYSIS

REPORTING AND DATA ANALYTICS

- LIVE THREAT MONITOR
- SECURITY ALERTS
- ATP-REPORTS
- FORENSIC INFORMATION

Advanced Threat Protection Sandbox vs. Ransomware y virus polimórficos

HORNETSECURITY

FACT SHEET

ATP-Engines	Funcionalidad y ventajas
Sandbox Engine	Los archivos adjuntos de los correos electrónicos se analizan en busca de posibles códigos maliciosos ejecutando el archivo sospechoso en un entorno de prueba virtual e identificando los efectos potencialmente peligrosos. Si se descubre que el documento enviado con el correo electrónico es malware, el correo se traslada directamente a la cuarentena.
Secure Links	Se acabaron los clics arriesgados en los enlaces de los correos electrónicos. Secure Links sustituye el enlace original por una versión reescrita que pasa por la pasarela web segura de Hornetsecurity. Secure Links utiliza inteligencia artificial, incluido el machine learning y el aprendizaje profundo, para proporcionar protección avanzada contra el phishing, incluso en ataques de onda corta y muy selectivos. Los algoritmos de machine learning supervisado y no supervisado analizan más de 47 características de URL y páginas web, buscando comportamientos maliciosos, técnicas de ofuscación y redireccionamientos de URL, mientras que los modelos de visión por ordenador analizan imágenes para extraer características relevantes utilizadas en ataques de phishing, como logotipos de marcas, códigos QR y texto sospechoso incrustado dentro de imágenes.
URL Scanning	Deja el documento adjunto a un correo electrónico en su forma original y sólo comprueba el destino de los enlaces contenidos en él.
Freezing	Los correos que no se pueden clasificar claramente de inmediato, pero los que son sospechosos, se retienen durante un corto período de tiempo. El correo electrónico corporativo se somete a una nueva revisión con firmas actualizadas.
Malicious Document Decryption	Los archivos adjuntos codificados de los correos electrónicos se descifran mediante módulos de texto adecuados dentro de un correo electrónico. Por último, el documento desencriptado se somete a un análisis de virus más profundo.
AI-powered Targeted Fraud Forensics	**Fraud attempt analysis:** Comprueba la autenticidad e integridad de los metadatos y el contenido del correo. **Identity spoofing recognition:** Detección y bloqueo de identidades falsas de remitentes. **Intention recognition system:** Alerta sobre patrones de contenido que indican una intención maliciosa. **Spy-out detection:** Defensa contra ataques de espionaje de información confidencial. **Feign facts identification:** Análisis del contenido del mensaje independientemente de la identidad, para identificar datos ficticios. **Targeted attack detection:** Detección de ataques dirigidos a personas particularmente vulnerables.
QR Code Analyzer	El QR code Analyzer de Hornetsecurity es capaz de detectar códigos QR incrustados directamente en un correo electrónico o una imagen. Todos los códigos QR se detectan y escanean a la velocidad de la luz en busca de contenido malicioso. Admite todos los tipos de imágenes comunes, como GIF, JPEG, PNG y BMP.