FIREEYE™

## FICHA TÉCNICA

# FireEye Detection On Demand

## Analice el contenido para detectar amenazas en cualquier punto de su flujo de trabajo

### ASPECTOS DESTACADOS

- Detecta y evita malware conocido y desconocido en cualquier lugar
- Despliega complementos con soporte de FireEye para navegadores y almacenamiento en la nube
- Obtiene un análisis contextual del malware detectado en formato JSON

**Introducción**
Las amenazas pueden venir y vienen desde cualquier lugar, y cada empresa se enfoca en el tema de la seguridad de manera diferente, según sus necesidades, industria y entorno. Pero la necesidad de contar con una capacidad validada de detección de amenazas respaldada mediante información con suficiente análisis contextual es algo que todas las empresas tienen en común para poder actuar.

Gracias a FireEye Detection On Demand, que está disponible para los clientes de FireEye a través de una API (Advanced Threat Intelligence), las organizaciones pueden enviar archivos de forma proactiva para asegurarse de que están protegidas contra las amenazas actuales, ya sea que estas ataquen las vulnerabilidades de los sistemas operativos Microsoft Windows, Apple OS X, o las de las aplicaciones.

FireEye Detection On Demand aprovecha el motor de detección FireEye Multi-Vector Virtual Execution™ (MVX) y el Intelligence Driven Analysis (IDA) para alcanzar rápidamente un veredicto sobre los archivos que se enviaron. MVX es un motor de análisis dinámico y sin firma que inspecciona el tráfico de red sospechoso para identificar ataques que evaden las defensas tradicionales basadas en políticas y en firmas. IDA es una recopilación de motores de reglas dinámicos y contextuales que detecta y bloquea la actividad maliciosa en tiempo real y retroactivamente, según la inteligencia más reciente de la máquina, del atacante y de la víctima.

**Detección de amenazas de alta gama en cualquier arquitectura de seguridad**
FireEye Detection On Demand es un servicio de detección de amenazas nativo de la nube que analiza rápidamente el contenido enviado para identificar malware residente. A diferencia de otras soluciones de seguridad de archivos basados en algoritmos de integridad, controles internos de políticas de amenazas o mecanismos estáticos de verificación, los envíos se procesan utilizando la misma tecnología que impulsa varias ofertas bien establecidas de FireEye.

El acceso a FireEye Detection On Demand se configura fácilmente a través de una API. Puede integrarse en el flujo de trabajo del centro de operaciones de seguridad (*Security Operations Center*, SOC), en los análisis SIEM [*Security Information and Event Management* (Información de seguridad y administración de eventos)], en repositorios de datos, aplicaciones web de clientes, etc. Brinda capacidades flexibles de análisis de archivos y contenido para identificar el comportamiento malicioso en cualquier sector que necesite la empresa.

Además de recibir un veredicto sobre cada archivo y pieza de contenido enviado a través de Detection On Demand, recibirá detalles contextuales de apoyo, como los cambios en archivos, registros, procesos y redes, así como también hallazgos importantes provenientes de FireEye Dynamic Threat Intelligence que se actualiza de manera continua.

## Cómo funciona Detection On Demand


FireEye Detection On Demand compara su envío con las tácticas y firmas conocidas más recientes de los perpetradores de amenazas, utilizando análisis estático, inteligencia artificial y aprendizaje automático. FireEye también determina la posibilidad de aparición de efectos secundarios o combinatorios en múltiples fases del ciclo de vida de ataques para descubrir exploits y malware nunca antes vistos.

**Figura 1.** Cómo funciona Detection On Demand.

### FireEye Developer Hub

Puede visitar el FireEye Developer Hub en https://fireeye.dev para explorar complementos y código de muestra y colaborar con la comunidad de desarrollo de FireEye sobre Detection On Demand.

### Cómo adquirirlo

Detection On Demand está disponible a través de los canales normales de FireEye o en forma directa a través de AWS (Advanced Threat Intelligence) Marketplace (para envíos de poco volumen).

Al adquirir el servicio, puede especificar su necesidad basada en el número de envíos que espera realizar en un solo año. Las compras mediante AWS Marketplace proporcionan una cuota de envío mensual, que se factura de forma anual. La velocidad de envío de archivos se limita a 100 archivos por minuto. La velocidad de envío de hash se limita a 200 hash por minuto.

Es posible que a los archivos y otros materiales que se envían a Detection On Demand se les asigne un valor de envío mayor que un envío; FireEye le comunicará los valores de envío estándar.

Para obtener más información sobre FireEye, visite: **www.FireEye.com**

**FireEye, Inc.**
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com



**Acerca de FireEye, Inc.**

FireEye es una empresa de seguridad basada en información. FireEye, que funciona como una extensión escalable y transparente de las operaciones de seguridad del cliente, ofrece una sola plataforma que combina tecnologías innovadoras de seguridad, inteligencia sobre amenazas similar a la de un Estado nación y los servicios de consultoría de fama mundial de Mandiant®. Gracias a este enfoque, FireEye elimina la complejidad y la carga de la seguridad cibernética para las organizaciones que desean estar preparadas y responder ante los ataques cibernéticos, además de prevenirlos.