FICHA TÉCNICA

Serie FortiSandbox™

Mitigación proactiva multicapa de amenazas

FortiSandbox

Los cibercriminales más sofisticados actualmente cada vez más sortean las soluciones de antimalware tradicionales e insertan en profundidad amenazas persistentes avanzadas en las redes. Estos ataques altamente dirigidos evaden la detección basada en firmas al enmascarar la naturaleza malintencionada de muchas formas: compresión, cifrado, polimorfismo, y la lista de técnicas continúa. Algunos incluso han comenzado a evadir los entornos de SandBoxing virtuales mediante la detección de VM, «bombas de tiempo» y otros. Combatir los ataques actuales requiere un enfoque amplio e integrado (algo más que antimalware). Más que un SandBoxing virtual o incluso más que un sistema de supervisión separado.

FortiSandbox ofrece una solución sólida de detección y mitigación proactivas, información sobre las amenazas que requiere acción, y una implementación sencilla e integrada. En su base es un SandBoxing único y de doble nivel, complementado por el antimalware premiado de Fortinet y la inteligencia de amenazas de FortiGuard integrada opcional. En FortiSandbox se encuentran empaquetados años de experiencia sobre amenazas de Fortinet, y están disponibles ahora in situ.

Mitigación y detección proactivas

Los códigos sospechosos están sujetos a filtrados previos multicapa antes de la ejecución en el SO virtual para el análisis conductual en detalle. Los filtrados previos de gran eficacia incluyen un cribado realizado por nuestro motor AV, consultas a las bases de datos de amenazas basadas en la nube y una simulación independiente del SO con un emulador de códigos, seguido por la ejecución en el entorno de tiempo de ejecución virtual completo. Cuando se detecta el código malintencionado, los resultados se envían para la creación de firmas antimalware, así como actualizaciones para otras bases de datos de amenazas.

Información que requiere acción

Se presentan todas las clasificaciones (malintencionado y riesgo alto/medio/bajo) en un panel intuitivo. En los informes y registros enriquecidos, se ofrece información completa sobre amenazas desde la ejecución virtual (incluidos actividad del sistema, esfuerzos de explotación, tráfico web, descargas posteriores, intentos de comunicación y más).

Fácil implementación

FortiSandbox admite la inspección de muchos protocolos en una solución unificada y, por tanto, simplifica las operaciones y la infraestructura de red. Además, se integra con FortiGate como nueva capacidad en su marco de seguridad existente.

Es la combinación definitiva de mitigación proactiva, visibilidad de amenazas avanzadas y creación de informes extensa.

Características principales

- El entorno de tiempo de ejecución virtual seguro expone amenazas desconocidas
- Filtrados previos multicapa exclusivos para una detección de amenazas efectiva y rápida
- Creación de informes enriquecidos para ofrecer una visibilidad del ciclo de vida de las amenazas completa
- La inspección de muchos protocolos en un appliance simplifica la implementación y reduce los costes
- La integración con FortiGate supone una mejora y no duplica la infraestructura de seguridad
- Seguridad validada con pruebas NSS BDS (Breach Detection Systems)

OPCIONES DE IMPLEMENTACIÓN

FortiSandbox es el appliance de análisis de amenazas más flexible del mercado, ya que ofrece distintas opciones de implementación para los requisitos y configuraciones únicos de los clientes. Las organizaciones también pueden tener las tres opciones de entrada al mismo tiempo.

Independiente

Este modo de implementación depende de las entradas procedentes de los puertos de switch y/o cargas de archivos a demanda de los administradores mediante la GUI. Es la infraestructura más adecuada para agregar capacidades de protección a sistemas de protección contra amenazas existentes de distintos proveedores.

*FortiGate/FortiMail integrados

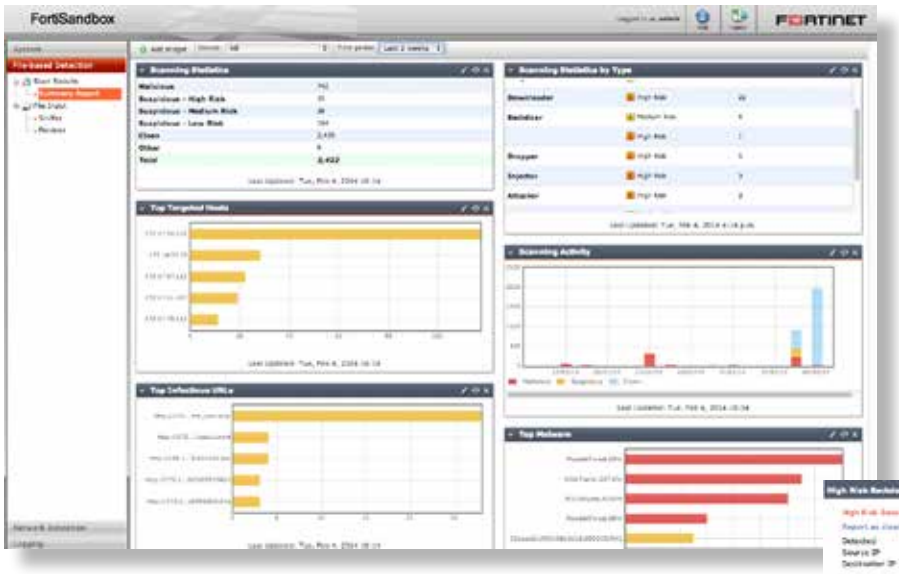
FortiGate, como puerta de enlace de seguridad de Internet, se puede configurar para enviar archivos sospechosos a FortiSandbox. Esta perfecta integración reduce la complejidad de la red y amplía las aplicaciones y los protocolos admitidos, incluidos los cifrados en SSL, como HTTPS.

* Requiere: FortiOS V5.0.4+, FortiMail V5.1+

FortiGate distribuido integrado

Esta implementación es atractiva para las organizaciones que cuentan con entornos distribuidos, donde se implementan FortiGates en las subsidiarias y se envían archivos sospechosos a un FortiSandbox ubicado de forma central. Esta configuración produce los beneficios del CTP más bajo y protege contra amenazas en las ubicaciones remotas.

CARACTERÍSTICAS

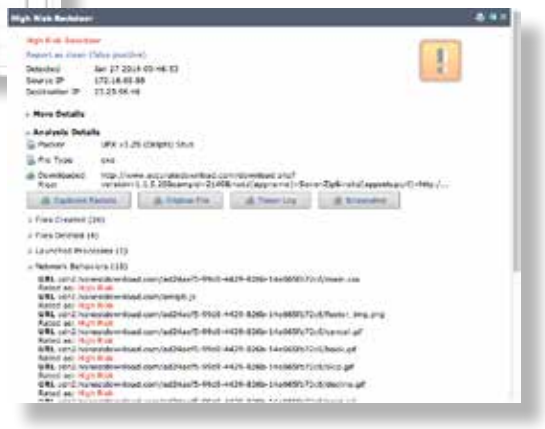


Widgets para paneles: estado de las amenazas en tiempo real

Tecnología de SandBoxing de VM

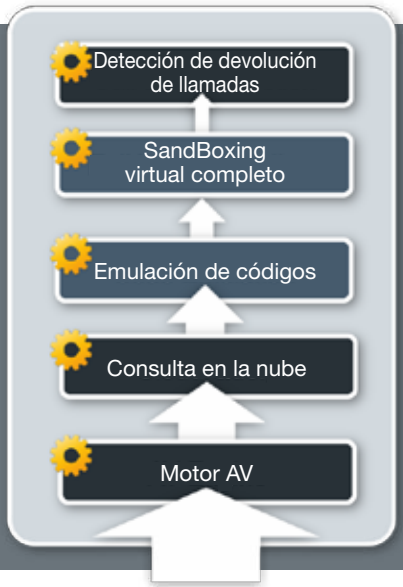
Complemente sus defensas establecidas con capacidades de última tecnología (a través del análisis de archivos sospechosos y de alto riesgo en un entorno contenido para descubrir el ciclo de vida de ataques completo con la detección de devolución de llamada y actividad del sistema).

Informe de análisis de archivos detallado



Herramientas de análisis de archivos

Los informes con paquetes capturados, archivos originales, registros de seguimiento y capturas de pantalla proporcionan una inteligencia de amenazas enriquecida y una información que requiere acción tras examinar los archivos. De esta forma se acelera la protección actualizada y las correcciones.



El procesamiento de archivos multicapa optimiza el uso de recursos que mejora la seguridad, la capacidad y el rendimiento

Motor AV
- Aplica la detección de AV de mejor calificación (95%+ reactivo y proactivo). Sirve como un filtrado previo eficiente.

Consulta en la nube
- Comprobación en tiempo real de la información de malware más reciente
- Acceso a la información compartida para la detección de malware instantánea

Emulación de códigos
- Simula rápidamente la actividad prevista
- Independiente del SO e inmune a la evasión/ofuscación

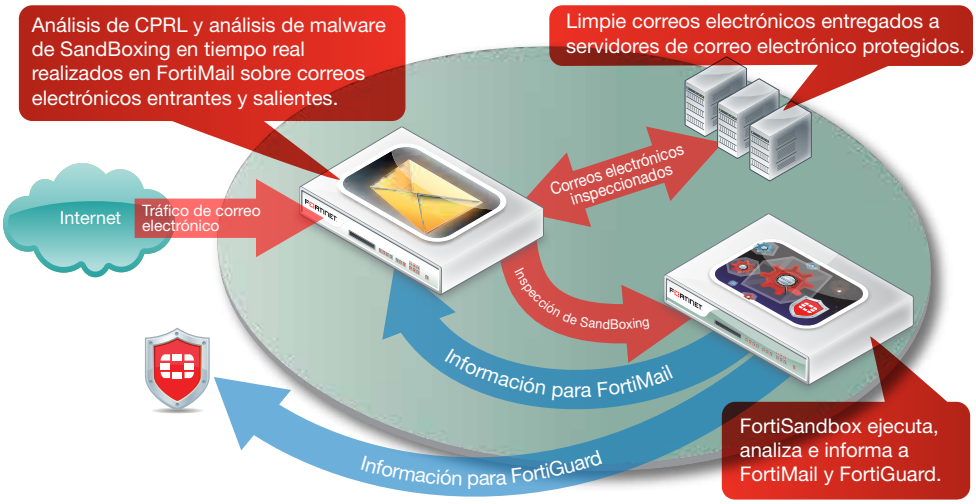
SandBoxing virtual completo
- Entorno de tiempo de ejecución seguro para la clasificación/el análisis conductual
- Expone la información del ciclo de vida de las amenazas completa

Detección de devolución de llamadas
- Identifica la exfiltración, la devolución de llamadas y el objetivo últimos

CARACTERÍSTICAS

Correcciones con FortiMail

Con muchas amenazas avanzadas, que comienzan con un correo electrónico dirigido con malware personalizado, ademas de ingeniería social que incita al usuario a abrirlo, las organizaciones están ampliando su puerta de enlace de correo electrónico seguro (SEG) con tecnología de SandBoxing integrada. Concretamente, la SEG retendrá mensajes mientras se realiza un análisis adicional en este entorno de tiempo de ejecución contenido y, en última instancia, aplicará políticas basadas en los resultados obtenidos.



FortiMail envía y encola contenido sospechoso

RESUMEN DE CARACTERÍSTICAS

Administración

Admite configuraciones WebUI y CLI

Creación de múltiples cuentas de administrador

Copia de seguridad y restauración de archivos de configuración

Correo electrónico de notificación cuando se detectan archivos malintencionados

Informe semanal para la lista de correo electrónico global y administradores de FortiGate

Página de búsqueda centralizada que permite a los administradores crear condiciones de búsqueda personalizadas

Actualizaciones automáticas de firmas frecuentes

Supervisión de estado de VM

Red/implementación

Soporte de enrutamiento estático

Entrada de archivos: Modo sin conexión/analizador de protocolos, carga de archivos a demanda, envío de archivos desde dispositivos integrados

API basada en web en la que los usuarios puede cargar muestras para explorar de forma indirecta

Opción para crear una red simulada de archivos explorados a los que acceder en un entorno de red cerrado

Integración de dispositivos:
- Entrada de envío de archivos: FortiGate, FortiMail
- Alojamiento de bases de datos de actualización: FortiManager
- Registro remoto: FortiAnalyzer, servidor de Syslog

Protección avanzada contra amenazas

Sandbox de SO virtual:
- Instancias de Windows simultáneas
- Técnicas antievasión: sleep calls, consultas de registro y procesos
- Detección de devolución de llamadas: visitas a URL malintencionadas, comunicación de C&C de botnet y tráfico de atacantes procedente de malware activado
- Descarga de paquetes capturados, archivos originales, registros de seguimiento y capturas de pantalla

Soporte para tamaños de archivos ilimitados, tamaño de archivo máximo configurable

Soporte de tipos de archivos:
- Archivado .tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj
- Archivos ejecutables (por ejemplo, .exe, .dll), PDF, documento de Windows Office y Javascript
- Archivos multimedia: .avi, .mpeg, .mp3, .mp4

Protocolos/aplicaciones admitidas:
- Modo de analizador de protocolos: HTTP, FTP, POP3, IMAP, SMTP, SMB
- Modo integrado con FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM y sus versiones equivalentes cifradas en SSL
- Modo integrado con FortiMail: SMTP, POP3, IMAP

Detección de amenazas de red en modo de analizador de protocolos: Identificación de actividades de botnet y ataques de red, visitas a URL malintencionadas

Opción para enviar archivos sospechosos automáticamente al servicio en la nube para el análisis manual y la creación de firmas

Supervisión e informes

Widgets de supervisión en tiempo real (visible por origen y opciones de periodo de tiempo): Estadísticas de resultados de detección, actividades de detección (a lo largo del tiempo), alojamientos dirigidos principales, malware principal, URL de infección principales, dominios de devolución de llamadas principales

Visor de eventos de obtención de detalles: Tabla dinámica con contenido de acciones, nombres de malware, clasificación, tipo, origen, destino, tiempo de detección y ruta de descarga

Registro: GUI, archivo de registro RAW de descarga

Generación de informes para archivos malintencionados: Informes detallados sobre características y comportamientos de archivos: modificación de archivos, comportamientos de procesos, comportamientos de registros, comportamientos de redes, instantánea de VM

Análisis posterior: Archivos descargables: archivos de muestreo, registros de seguimiento de SandBoxing y captura de PCAP

ESPECIFICACIONES

	FSA-1000D	FSA-3000D
Hardware		
Factor de forma	2 RU	2 RU
Interfaces de red totales	6 puertos de GE RJ45 2 ranuras de GE SFP	4 puertos de GE RJ45 2 ranuras de GE SFP 2 ranuras de 10 GE SFP+
Capacidad de almacenamiento	4 TB (máx. 8 TB)	8 TB (máx. 16 TB)
Alimentación	2 PSU redundantes	2 PSU redundantes
Sistema		
Tecnología de SandBoxing de VM (archivos/hora)	160	560
Detección de AV (archivos/hora)	6000	15 000
Número de VM	8	28
Dimensiones		
Altura x Anchura x Longitud (pulg.)	3,5 x 17,2 x 14,5	3,3 x 19,0 x 29,7
Altura x Anchura x Longitud (mm)	89 x 437 x 368	84 x 482 x 755
Peso	27,60 lbs (12,52 kg)	71,5 lbs (32,5 kg)

	FSA-1000D	FSA-3000D
Entorno		
Consumo de energía (promedio / máx.)	115 / 138 W	392 / 614,6 W
Corriente máxima	100 V / 5 A, 240 V / 3 A	110 V / 10 A, 220 V / 5 A
Disipación térmica	471 BTU/h	2131,14 BTU/h
Fuente de alimentación	100–240 V CA, 60–50 Hz	100–240 V CA, 60–50 Hz
Humedad	5–95% sin condensación	20–90% sin condensación
Rango de temperatura de funcionamiento	32–104 °F (0–40 °C)	50–95°F (10–35°C)
Rango de temperatura de almacenamiento	-13–158°F (-25–70°C)	-40–149°F (-40–65°C)
Cumplimiento		
Certificaciones	FCC Parte 15 Clase A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	

	FSA-VM
Requisitos de hardware	
Soporte de hipervisor	VMware ESXi versión 5.0 o posterior
CPU virtuales (mín. / máx.)	4 / ilimitado (Fortinet recomienda que el número de vCPU coincidan con el número de Windows VM +4.)
Memoria virtual (mín. / máx.)	8 GB / ilimitado
Almacenamiento virtual (mín. / máx.)	30 GB / 16 TB
Interfaces de red virtuales totales (mín.)	6
Sistema	
Tecnología de SandBoxing de VM (archivos/hora)	Dependiente de hardware
Detección de AV (archivos/hora)	Dependiente de hardware
Número de VM	2 a 52 (actualización con licencias adecuadas)

INFORMACIÓN DE SOLICITUD

Producto	SKU	Descripción
FortiSandbox 1000D	FSA-1000D	Sistema de protección avanzada contra amenazas: 6 GE RJ45, 2 ranuras de GE SFP, PSU redundante, 6 licencias de Windows XP y 2 licencias de Windows 7 incluidas.
FortiSandbox 3000D	FSA-3000D	Sistema de protección avanzada contra amenazas: 4 GE RJ45, 2 ranuras de GE SFP, PSU redundante, 22 licencias de Windows XP y 6 licencias de Windows 7 incluidas.
FortiSandbox-VM	FSA-VM-BASE	Licencia base para FortiSandbox-VM apilable. Incluye (1) licencia de Windows XP y (1) de Windows 7 VM. Expansión máxima de FSA-VM limitada a 52 VM totales.
Accesorios opcionales	**SKU**	**Descripción**
1 módulo transceptor GE SFP SX	FG-TRAN-SX	1 módulo transceptor SX GE SFP para todos los sistemas con ranuras SFP y SFP/SFP+.
1 módulo transceptor GE SFP LX	FG-TRAN-LX	1 módulo transceptor LX GE SFP para todos los sistemas con ranuras SFP y SFP/SFP+.
10 módulos transceptores GE SFP+, alcance corto	FG-TRAN-SFP+SR	10 módulos transceptores GE SFP+, alcance corto para todos los sistemas con ranuras SFP y SFP/SFP+.
10 módulos transceptores GE SFP+, alcance largo	FG-TRAN-SFP+LR	10 módulos transceptores GE SFP+, alcance largo para todos los sistemas con ranuras SFP y SFP/SFP+.

España
Camino Cerro de los Gamos,
1. Edificio 1. Pl. 1
28224 Pozuelo de Alarcón
Madrid – España
Ventas: +34 91 790 11 16

SEDE GLOBAL
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
Estados Unidos
Tel: +1 408 235 7700
www.fortinet.com/sales

OFICINA DE VENTAS
EMEA
120 rue Albert Caquot
06560, Sophia Antipolis,
Francia
Tel: +33 4 8987 0510

OFICINA DE VENTAS
APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel: +65 6513 3730

OFICINA DE VENTAS EN LATINOAMÉRICA
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Álvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480