

# Forcepoint Advanced Malware Detection and Protection

Solución avanzada de sandbox diseñada para detectar y proteger contra malware avanzado y amenazas de día cero

## Beneficios clave

- › **Detección de amenazas de día cero** Detecte las amenazas de malware más esquivas y avanzadas y sus variantes desconocidas.
- › **Inteligencia colectiva compartida** Una vez que el Advanced Malware Detection and Protection (AMDP) identifica malware avanzado nuevo o sin categorizar, la firma del archivo se comparte entre las soluciones de seguridad de Forcepoint para proteger a los clientes y mejorar su inteligencia de seguridad.
- › **Soporte integral de archivos** Soporte de análisis de malware para tipos de archivos de Windows, Linux, macOS y Android.
- › **Bloqueo en línea** Aumente la protección de la red contra amenazas de día cero en tiempo real sin interrumpir la experiencia del usuario mediante el bloqueo en línea con FlexEdge Secure SD-WAN.

Cuando se trata de protegerse contra malware avanzado y exploits de día cero, las organizaciones enfrentan desafíos internos y externos aparentemente insuperables. Los actores de amenazas son más inteligentes y están más equipados que nunca y crean malware avanzado y en evolución diseñado para evadir las soluciones tradicionales.

New threat vectors have risen from the adoption of cloud environments and a distributed workforce. Han surgido nuevos vectores de amenazas a partir de la adopción de entornos de nube y una fuerza laboral distribuida. Los desafíos internos, como la falta de fuerza laboral capacitada en ciberseguridad y los equipos de TI abrumados, están demasiado preocupados como para centrarse en la búsqueda de amenazas. La detección y protección avanzada de malware de Forcepoint, impulsada por Hatching, A Recorded Future Company, permite a las organizaciones detectar amenazas de malware avanzadas y desconocidas, incluidos exploits de día cero.

AMDP es un Advanced Sandbox de última generación que protege a las organizaciones de los ataques de malware avanzado de hoy. AMDP es compatible con los sistemas operativos Windows, macOS (solo para despliegue en la nube), Linux y Android para brindar un soporte integral de archivos. Forcepoint AMDP se integra a la perfección con Forcepoint FlexEdge Secure SD-WAN y las soluciones de seguridad web. Esta estrecha integración proporciona inteligencia compartida en todas las soluciones de Forcepoint y protege a las organizaciones contra las amenazas de día cero. Las organizaciones también obtienen un aumento en la productividad, ya que se puede acceder a las políticas, paneles e informes a través de una sola consola.



**Forcepoint AMDP proporciona inteligencia compartida entre las soluciones Forcepoint y protege a las organizaciones contra amenazas de día cero**

## Especificaciones

### Integraciones de Productos

Forcepoint Web Security (Cloud, Hybrid, on- Premises)  
Forcepoint FlexEdge Secure SD-WAN

### Soporte del sistema operativo

Windows, MacOS (solo para despliegue en la nube),  
Linux, Android

### Soporte de tamaño de archivo

#### Seguridad web de Forcepoint

ARCHIVO	MS OFFICE
rar, 7z, gzip, tar, zip, arj, bz	doc, .docx, .dot, .dotx, .dotm, .docm, .xls, .xlsx, .xlt, .xlam, .xltm, .xlsm, .xlsb, .xltx, .xla, .ppt, .pptx, .pps, .pot, .ppsx, .potx, .ppsm, .pptm, .one
ARCHIVOS EJECUTABLES	
Archivos ejecutables Windows	

### Forcepoint FlexEdge Secure SD-WAN

ARQUIVO	SCRIPT	MS OFFICE
.zip, .7z, .ace, .cab, .daa, .gz, .rar, .tar, .eml, .iso, .lzh, .bz2, .bup, .mso, .msg, .vhd, .vbn, .tnef, .xz, .xar, .lz, .xex	.bat, .js, .vbe, .vbs, .ps1, .py, .cmd, .sh, .pl, .jse	.doc, .ppt, .xls, .rtf, .docx, .pptx, .xlsx, .docm, .dot, .dotx, .docb, .xlm, .xlt, .xltx, .xlsm, .xltm, .xlsb, .xla, .xlam, .xll, .xlw, .pps, .ppsx, .pptm, .potm, .potx, .ppsm, .pot, .ppam, .sldx, .sldm, .dotm, .one
DOCUMENTOS DE OPEN OFFICE	ARCHIVOS EJECUTABLES	SCRIPT
.oxt, .ott, .oth, .odm, .odt, .otg, .odg, .otp, .odp, .ots, .ods, .odc, .odf, .odb, .odi	exe, .dll, .lnk, .elf, .msi, .scr, .deb, .url, .jar, .com, .cpl, .appx	.bat, .js, .vbs, .jse, .ps1, .py, .pyc, .pyo, .cmd, .sh, .pl, .vbe
OTROS ARCHIVOS	ANDROID	MAC OS
.ps1xml, .psc1, .psm1, .gb, .gba, .asp, .jnlp	.apk, .dex	macho, .scpt, .pkg, .app, .dm
MISC	LINUX	
.xml, .txt,	.elf, .sh	

### Opciones de despliegue

Nube (SaaS) y en las instalaciones

### Soporte de tamaño de archivo

Forcepoint Web Security: 62MB  
Forcepoint FlexEdge Secure SD-WAN:100MB

### Soberanía de datos

Retención de datos: solo se conserva el hash del archivo y la puntuación de amenazas Retención del informe de amenazas: 1 año La retención de datos cumple con el RGPD

Conozca más y programe una demo gratuita, visite [Advanced Malware Detection and Protection](#)