Forcepoint

Datasheet

Forcepoint Advanced Malware Detection and Protection

Solução de sandbox avançada projetada para detectar e proteger contra malware avançado e ameaças de dia zero

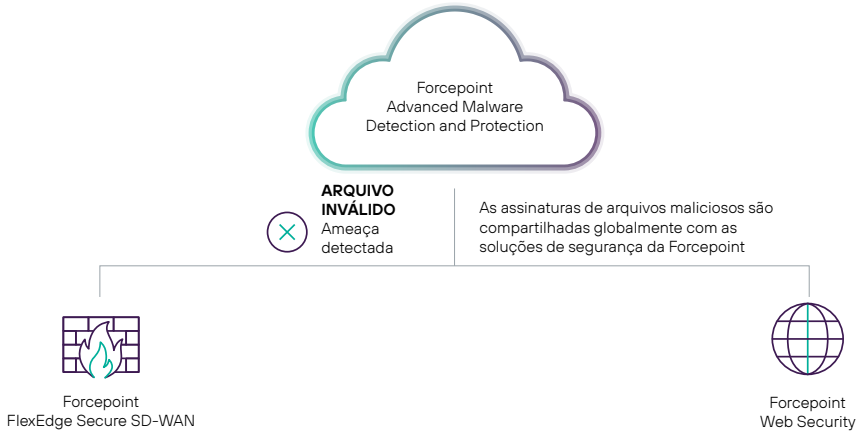
Principais benefícios

- **Detecção de ameaças de dia zero**
  Detecte as ameaças de malware mais evasivos e avançados e as variantes desconhecidas.
- **Inteligência compartilhada coletiva**
  Uma vez que o Advanced Malware Detection and Protection (AMDP) identifica o malware avançado novo ou não categorizado, a assinatura de arquivos é compartilhada nas soluções de segurança da Forcepoint para proteger os clientes e aprimorar sua inteligência de segurança.
- **Suporte abrangente de arquivos**
  Suporte para análise de malware para Windows, Linux, macOS (apenas implantação de nuvem) e tipos de arquivos Android.
- **Bloqueio em linha**
  Aumente a proteção de rede contra ameaças de dia zero em tempo real sem interromper a experiência do usuário por meio de bloqueio em linha com o FlexEdge Secure SD-WAN.

Quando se trata de proteger contra malware avançado e exploits de dia zero, as organizações enfrentam desafios internos e externos aparentemente insuperáveis. Os agentes de ameaças estão mais inteligentes e mais equipados do que nunca, criando malware avançado e em evolução projetado para escapar das soluções tradicionais.

Os novos vetores de ameaças surgiram com a adoção de ambientes de nuvem e de uma força de trabalho distribuída. Os desafios internos, como a falta de força de trabalho de cibersegurança qualificada e as equipes de TI sobrecarregadas, estão preocupadas demais para se concentrar na caça às ameaças. O Forcepoint Advanced Malware Detection and Protection, powered by Hatching, a Recorded Future Company, permite que as organizações detectem ameaças de malware desconhecido e avançado, incluindo exploits de dia zero.

O AMDP é um Advanced Sandbox de última geração que protege as organizações contra os ataques de malware avançado de hoje. O AMDP é compatível com Windows, macOS (apenas implantação de nuvem), Linux e sistemas operacionais Android para oferecer suporte abrangente de arquivos. O Forcepoint AMDP integra-se perfeitamente ao Forcepoint FlexEdge Secure SD-WAN e às soluções de web security. Essa integração rigorosa fornece inteligência compartilhada em todas as soluções da Forcepoint e protege as organizações contra ameaças de dia zero. As organizações também ganham um aumento de produtividade já que as políticas, painéis e relatórios são acessíveis por meio de um único console.



O Forcepoint AMDP fornece inteligência compartilhada em todas as soluções da Forcepoint e protege as organizações contra ameaças de dia zero

Especificações

Integrações de produtos

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

Sistemas operacionais compatíveis

Windows, MacOS (apenas implantação de nuvem), Linux, Android

Opções de implementação

Nuvem (SaaS) e on-premise

Tamanho de arquivos compatíveis

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

Soberania de dados

Retenção de dados: apenas o hash de arquivos e a pontuação de ameaças são retidos
Retenção de relatórios de ameaças: 1 ano
A retenção de dados está em conformidade com a LGPD

Tipos de arquivos compatíveis

Forcepoint Web Security

ARQUIVO	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
ARQUIVOS EXECUTÁVEIS	
Arquivos executáveis do 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, .xxe	.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
DOCUMENTS DO OPEN OFFICE	**ARQUIVOS EXECUTÁVEIS**	**LINGUAGENS DE 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
OUTROS ARQUIVOS	**ANDROID**	**MAC OS**
.ps1xml, .psc1, .psm1, .gb, .gba, .asp, .jnlp	.apk, .dex	macho, .scpt, .pkg, .app, .dm
MISC	**LINUX**	
.xml, .txt,	.elf, .sh	

Para saber mais e agendar uma demon gratuita, acesse Advanced Malware Detection and Protection