Forcepoint

Datasheet

Forcepoint Advanced Malware Detection and Protection

Advanced sandbox solution engineered to detect and protect against advanced malware and zero-day threats

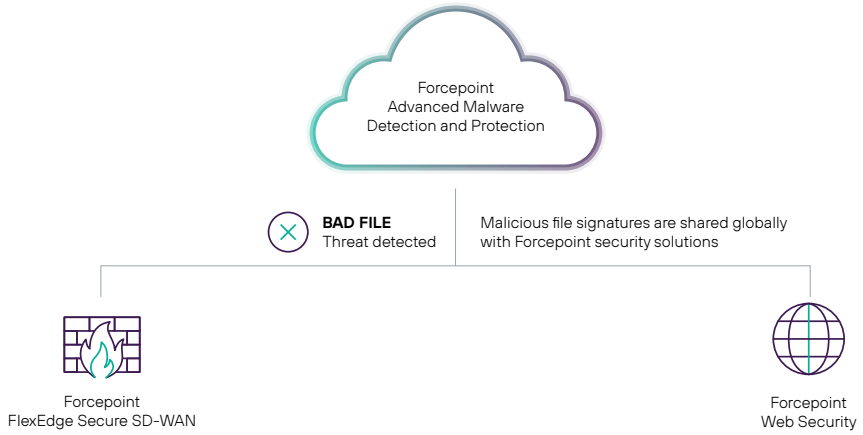
Key Benefits

- **Zero-day threat detection**
  Detect the most elusive and advanced malware threats and unknown variants.
- **Collective shared intelligence**
  Once Advanced Malware Detection and Protection (AMDP) identifies new or uncategorized advanced malware, the file signature is shared across Forcepoint security solutions to protect customers and enhance their security intelligence
- **Comprehensive file support**
  Malware analysis support for Windows, Linux, macOS (Cloud deployment only) and Android file types.
- **In-line blocking**
  Increase network protection against Zero-day threats in real-time without disrupting user experience through in-line blocking with FlexEdge Secure SD-WAN.

When it comes to protecting against advanced malware and zero-day exploits, organizations face seemingly insurmountable internal and external challenges. Threat actors are smarter and more equipped than ever before, creating advanced and evolving malware designed to evade traditional solutions.

New threat vectors have risen from the adoption of cloud environments and a distributed workforce. Internal challenges, such as a lack of skilled cybersecurity workforce and overwhelmed IT teams, are too preoccupied to focus on threat hunting. Forcepoint Advanced Malware Detection and Protection, powered by Hatching, A Recorded Future Company, enables organizations to detect unknown and advanced malware threats, including zero-day exploits.

AMDP is a next-generation Advanced Sandbox that safeguards organizations from today's advanced malware attacks. AMDP supports Windows, macOS (Cloud deployment only), Linux and Android operating systems to deliver comprehensive file support. Forcepoint AMDP seamlessly integrates with Forcepoint FlexEdge Secure SD-WAN and web security solutions. This tight integration provides shared intelligence across Forcepoint solutions and protects organizations against zero-day threats. Organizations also gain an increase in productivity as policy, dashboards, and reports are accessible through a single console.



Forcepoint AMDP provides shared intelligence across Forcepoint solutions and protects organizations against zero-day threats

Specifications

Product integrations

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

Operating System Support

Windows, MacOS (Cloud deployment only), Linux, Android

Deployment options

Cloud (SaaS) and On-Premise

File size support

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

Data sovereignty

Data Retention: Only file Hash and threat score is retained
Threat report retention: 1 year
Data retention is GDPR compliant

File type support

Forcepoint Web Security

ARCHIVE	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
EXECUTABLE FILES	
Windows Executable files	

Forcepoint FlexEdge Secure SD-WAN

ARCHIVE	SCRIPTING	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
OPEN OFFICE DOCUMENTS	**EXECUTABLE FILES**	**SCRIPTING LANGUAGES**
.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
OTHER FILES	**ANDROID**	**MAC OS**
.ps1xml, .psc1, .psm1, .gb, .gba, .asp, .jnlp	.apk, .dex	macho, .scpt, .pkg, .app, .dm
MISC	**LINUX**	
.xml, .txt,	.elf, .sh	

To learn more and schedule a free demo visit Advanced Malware Detection and Protection

© 2023 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.
[FP-Forcepoint AMDP Datasheet-US-EN] 13Dec2023