Advanced Malware Detection and Protection

2.0

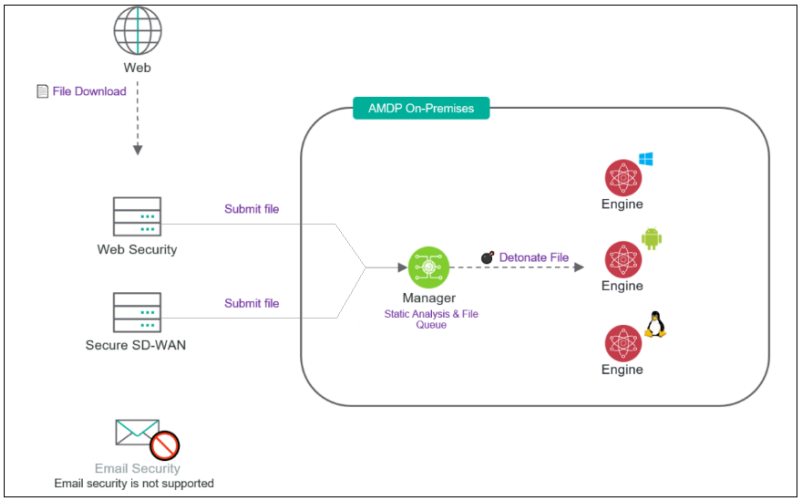
On-Premises Release Notes

Revision A

Contents

Introduction

The Forcepoint Advanced Malware Detection and Protection (AMDP) is a next-generation Advanced Sandbox that safeguards organizations from today's advanced malware attacks. AMDP supports Windows, Linux and Android OS file types, to detect malicious threats beyond static analysis capabilities. Forcepoint AMDP seamlessly integrates with Forcepoint FlexEdge Secure SD-WAN and Forcepoint Web Security On-Premises solution.



Key benefits

- **Zero-day threat detection**: Detect the most elusive and advanced malware threats and unknown variants.
- **Secure file submissions**: File Submissions remain On-Premises and are never shared with Cloud services.
- **Comprehensive file support**: Malware analysis support for Windows, Linux, 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 Secure SD-WAN.

- **Static Analysis and Advanced Threat Report**: AMDP employs multiple scanning layers to detect advanced malware. AMDP is capable of doing quick threat score calculations through static file analysis in addition to sandbox detonation. AMDP scan results provide an Advanced Threat report, including MITRE ATT&CK insights for threat hunters, analysis of network vulnerabilities and security hardening.

Supported environments

The Forcepoint AMDP supports following:

- **Product Integrations**:
  - Forcepoint Web Security On-Premises
  - Forcepoint FlexEdge Secure SD-WAN
- **Operating systems**:
  - Windows, Linux, Android
- **File sizes**:
  - Forcepoint Web Security: 62MB
  - Forcepoint FlexEdge Secure SD-WAN: 100MB

Supported file types

Forcepoint Web Security

ARCHIVE	MS OFFICE	EXECUTABLE FILES
.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	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	MISC	LINUX
.ps1xml, .psc1, .psm1, .gb, .gba, .asp, .jnlp	.apk, .dex	.xml, .txt,	.elf, .sh

Resolved and known issues

There are no resolved issues in this release. Click here to view the known issues list for Forcepoint On-Premises Advanced Malware Detection and Protection 2.0 in the Forcepoint Knowledge Base.

You must log on to the Customer Hub to view the list.

Other resources

Forcepoint Cyber Institute Hackstack links:

- Introduction to AMDP
- Understanding AMDP Architecture and Traffic Flow
- Working with Different File Types in AMDP
- Zero-day threat blocking with AMDP
- Reviewing AMDP threat reports
- AMDP and Data Sovereignty

Published 29 January 2024