Forcepoint

Fiche Technique

Détection et protection avancées de Forcepoint contre les programmes malveillants

Solution de sandbox avancée conçue pour détecter et protéger contre les malwares avancés et les menaces de type « zero-day »

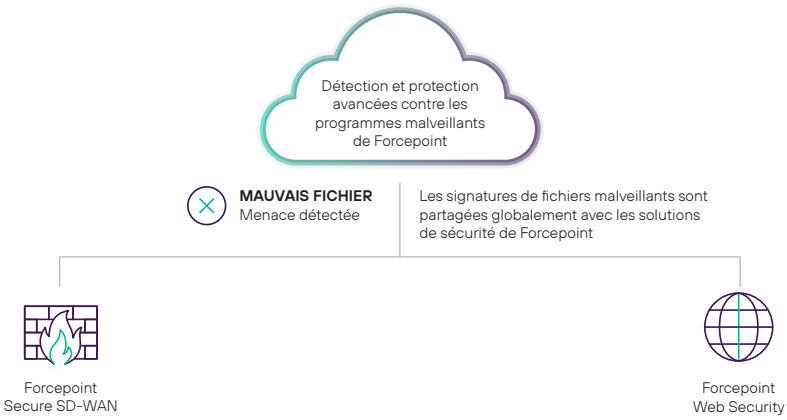
Principaux avantages :

- **Détection des menaces zero-day :** Détection des menaces de programmes malveillants les plus insaisissables et avancées ainsi que leurs variantes inconnues.
- **Intelligence partagée collective :** Une fois que la solution AMDP identifie un nouveau programme malveillant ou non catégorisé, la signature du fichier est partagée entre les solutions de sécurité de Forcepoint pour protéger les clients et améliorer leurs informations de sécurité
- **Support complet pour les fichiers :** support d'analyse des programmes malveillants pour Windows, Linux, macOS (déploiement cloud uniquement) et les fichiers de type Android.
- **Blocage en ligne :** Augmentez la protection du réseau contre les menaces inconnues en temps réel sans perturber l'expérience de l'utilisateur, grâce à un blocage en ligne avec Forcepoint Secure SD-WAN.

Lorsqu'il s'agit de se protéger contre les programmes malveillants avancés et les exploits « zero-day », les entreprises sont confrontées à des défis internes et externes apparemment insurmontables. Les acteurs de la menace, plus intelligents et plus équipés que jamais, créent des programmes malveillants en constante évolution conçus pour échapper aux solutions traditionnelles.

Forcepoint Advanced Malware Detection and Protection, fourni par Hatching, appartenant à Recorded Future, permet aux entreprises de détecter les menaces de programmes malveillants inconnues et avancées, y compris les exploits « zero-day ».

AMDP est une sandbox avancée de nouvelle génération qui protège les entreprises des attaques de programmes malveillants. AMDP prend en charge les systèmes d'exploitation Windows, macOS (déploiement cloud uniquement), Linux et Android pour fournir une prise en charge complète des fichiers. Forcepoint AMDP s'intègre de manière transparente avec Forcepoint Secure SD-WAN et les solutions de sécurité Web. Cette intégration étroite fournit une intelligence partagée entre les solutions Forcepoint et protège les entreprises contre les menaces de type « zero-day ». Les entreprises gagnent également en productivité car les politiques, les tableaux de bord et les rapports sont accessibles via une console unique.



Forcepoint AMDP fournit des informations partagées à travers les solutions Forcepoint et protège les entreprises contre les menaces de type « zero-day »

Spécifications

Intégrations de produits
- Forcepoint Web Security (Cloud, hybride, sur site)
- Forcepoint Secure SD-WAN

Systèmes d'exploitation supportés
- Windows, MacOS (déploiement cloud uniquement), Linux, Android

Options de déploiement
- Cloud (SaaS) et sur site

Prise en charge de la taille des fichiers
- Forcepoint Web Security: 62 Mo
- Forcepoint Secure SD-WAN : 100 Mo

Souveraineté des données
- Conservation des données : Seuls sont conservés le hachage des fichiers et le score de menace
- Conservation du rapport sur les menaces : 1 an
- La conservation des données est conforme au RGPD

Prise en charge des types de fichiers

Forcepoint Web Security

ARCHIVER	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
FICHIERS EXÉCUTABLES	
Windows Executable files	

Forcepoint Secure SD-WAN

ARCHIVER	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 OPEN OFFICE	**FICHIERS EXÉCUTABLES**	**LANGAGES 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
AUTRES FICHIERS	**ANDROID**	**MAC OS**
.ps1xml, .psc1, .psm1, .gb, .gba, .asp, .jnlp	.apk, .dex	macho, .scpt, .pkg, .app, .dm
MISC	**LINUX**	
.xml, .txt,	.elf, .sh	

Pour en savoir plus et planifier une démonstration gratuite, visitez la page de détection et de protection avancées des programmes malveillants