Service SonicWall Capture Advanced Threat Protection

Détecter et bloquer les attaques inconnues et zero-day

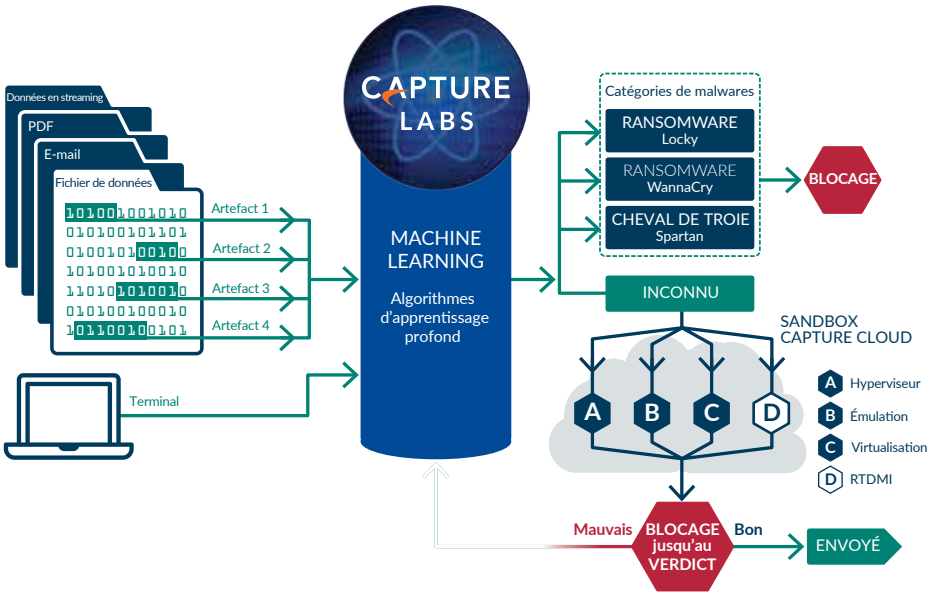
Pour une protection efficace contre les menaces zero-day, les entreprises ont besoin de solutions intégrant des technologies d'analyse des logiciels malveillants et capables de détecter les techniques d'évasion évoluées, aujourd'hui et demain.

Afin de protéger les clients face aux dangers croissants des menaces zero-day, SonicWall Capture Advanced Threat Protection Service – un service Cloud proposé avec les pare-feux SonicWall – détecte et peut bloquer toute menace évoluée au niveau de la passerelle jusqu'à ce que l'analyse ait rendu son verdict. Ce service est la seule détection des menaces évoluées à offrir un mécanisme de sandboxing multicouche, comprenant la technologie SonicWall Real-Time Deep Memory Inspection (RTDMI™), des techniques de virtualisation et d'émulation complète du système, pour analyser le code suspect. Un puissant cocktail qui intercepte davantage de menaces que les solutions de sandbox à un seul moteur, spécifiques à un environnement et plus faciles à contourner.

La solution filtre le trafic et en extrait le code suspect pour l'analyser. Mais à la différence d'autres solutions de passerelle, elle analyse un vaste éventail de tailles et de types de fichiers. L'infrastructure globale de renseignement sur les menaces fournit rapidement les signatures correctives pour les nouvelles menaces identifiées à toutes les appliances de sécurité réseau SonicWall, coupant ainsi court à toute propagation. Les clients bénéficient d'une sécurité haute efficacité, de délais de réponse brefs et d'un coût total de possession réduit.

Avantages :

- Efficacité accrue de la protection contre les menaces inconnues
- Déploiement des signatures en temps quasi réel pour éviter toute propagation
- Coût total de possession réduit
- Blocage des fichiers au niveau de la passerelle jusqu'au verdict
- Plusieurs moteurs traitent les fichiers en parallèle pour un verdict rapide
- Le moteur RTDMI de SonicWall bloque les logiciels malveillants grand public inconnus via des techniques d'inspection de la mémoire en temps réel



Une solution Cloud multi-moteur pour stopper les attaques inconnues et zero-day au niveau de la passerelle

Une protection optimale contre les menaces zero-day : la solution est conçue pour intégrer dynamiquement les nouvelles technologies d'analyse des logiciels malveillants dès que le paysage des menaces évolue.

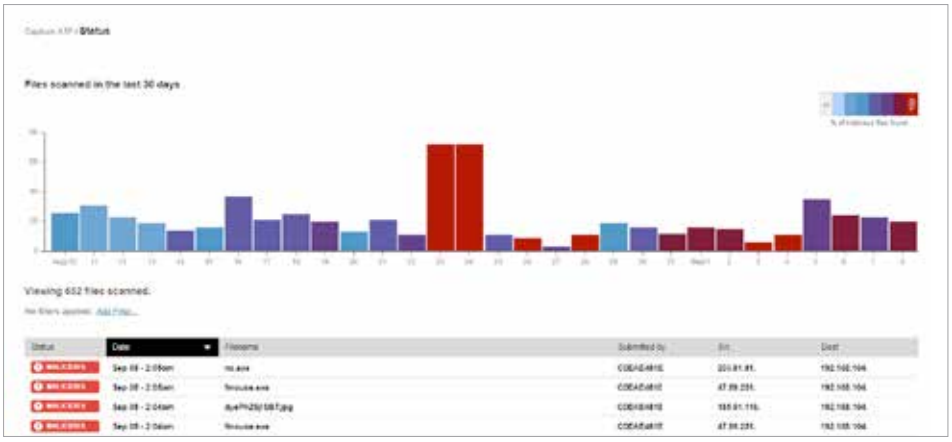
Fonctionnalités

Analyse multi-moteur des menaces évoluées : le service SonicWall Capture ATP complète le travail de protection du pare-feu en détectant et prévenant les attaques zero-day. Le pare-feu inspecte le trafic, puis détecte et bloque les intrusions et logiciels malveillants connus. Les fichiers suspects sont envoyés au service Cloud SonicWall Capture ATP pour être analysés. La plateforme sandbox multi-moteur, qui inclut RTDMI, sandboxing virtualisé, émulation complète du système et technologie d'analyse au niveau de l'hyperviseur, exécute le code suspect et analyse son comportement, offrant ainsi une visibilité complète sur l'activité malveillante, tout en permettant d'éviter les tactiques d'évasion et en maximisant la détection des menaces zero-day.

Real-Time Deep Memory Inspection (RTDMI) : notre technologie Real-Time Deep Memory Inspection en instance de brevet vient améliorer le service multi-moteur SonicWall Capture ATP. Le moteur RTDMI détecte et bloque de manière proactive les logiciels malveillants inconnus et les menaces zero-day grand public via une inspection directe en mémoire. Grâce à son architecture en temps réel, la technologie RTDMI de SonicWall est précise, réduit le nombre de faux positifs et limite les attaques sophistiquées.

Analyse de nombreux types de fichiers : le service assure l'analyse d'un vaste éventail de tailles et types de fichiers, notamment les programmes exécutables (PE), DLL, PDF, documents MS Office, archives, JAR et APK, ainsi que de divers systèmes d'exploitation comme Windows et Android. Les administrateurs peuvent personnaliser la protection en sélectionnant ou excluant les fichiers à envoyer dans le Cloud pour analyse, selon le type du fichier, sa taille, l'expéditeur, le destinataire ou le protocole. Ils peuvent aussi soumettre manuellement des fichiers au service Cloud.

Bloquer jusqu'au verdict : pour empêcher les fichiers potentiellement malveillants de pénétrer sur le réseau, les fichiers envoyés au service Cloud pour y être analysés peuvent être retenus à la passerelle jusqu'à ce qu'un verdict soit rendu.



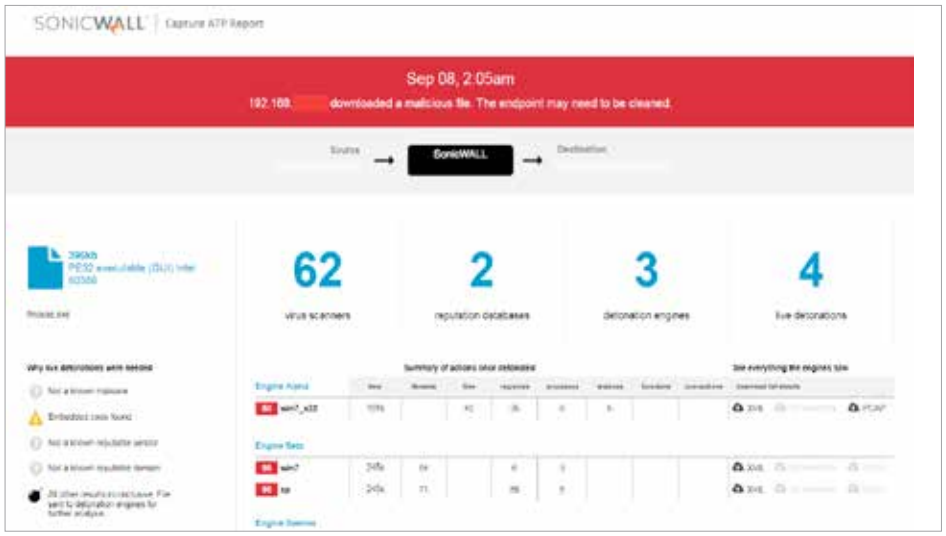
La page de reporting SonicWall Capture ATP affiche en un clin d'œil les résultats journaliers. Les barres de couleur indiquent les jours auxquels des logiciels malveillants ont été détectés. Les administrateurs peuvent cliquer sur les résultats journaliers et appliquer des filtres pour voir rapidement fichiers malveillants et résultats.

Déploiement rapide des signatures correctives : lorsqu'un fichier est identifié comme étant malveillant, une signature est immédiatement mise à la disposition des pare-feux ayant un abonnement à SonicWall Capture ATP pour empêcher toute infiltration plus poussée. Le malware est alors soumis à l'équipe de recherche sur les menaces SonicWall Capture Labs pour y être analysé plus en profondeur et intégré aux bibliothèques de signatures de l'antivirus de passerelle et de l'IPS. Il sera en outre envoyé dans les 48 heures aux bases de données d'URL, d'IP et de réputation de domaine.

Rapports et alertes : le service SonicWall Capture ATP fournit un tableau de bord concis de l'analyse des menaces, ainsi que des rapports détaillant les résultats d'analyse des fichiers envoyés au service, à savoir source, destination et récapitulatif ainsi que les détails relatifs à l'action des logiciels malveillants une fois déclenchés. Les alertes journal du pare-feu notifient l'envoi de fichiers suspects à SonicWall Capture ATP, avec le résultat de l'analyse.

À propos de nous

SonicWall s'engage depuis plus de 27 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution automatisée de détection et de prévention des failles en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 215 pays et territoires, leur permettant de se concentrer sans crainte sur leur cœur de métier.



Un rapport d'analyse détaillé est également disponible pour les fichiers analysés afin de faciliter les possibilités de correction.

PLATEFORMES PRISES EN CHARGE

SonicWall Capture ATP est pris en charge par les pare-feux SonicWall suivants exécutant SonicOS version 6.2.6 ou supérieure :

NS*sp* 12800
NS*sp* 12400

NS*a* 9650
NS*a* 9450
NS*a* 9250
NS*a* 6650
NS*a* 5650
NS*a* 4650
NS*a* 3650
NS*a* 2650

TZ600 Series
TZ500 Series
TZ400 Series
TZ300 Series

NSv 1600
NSv 800
NSv 400
NSv 300
NSv 200
NSv 100
NSv 50
NSv 25
NSv 10

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

DataSheet-CaptureAdvancedThreatProtection-US-VG-MKTG4093