Security

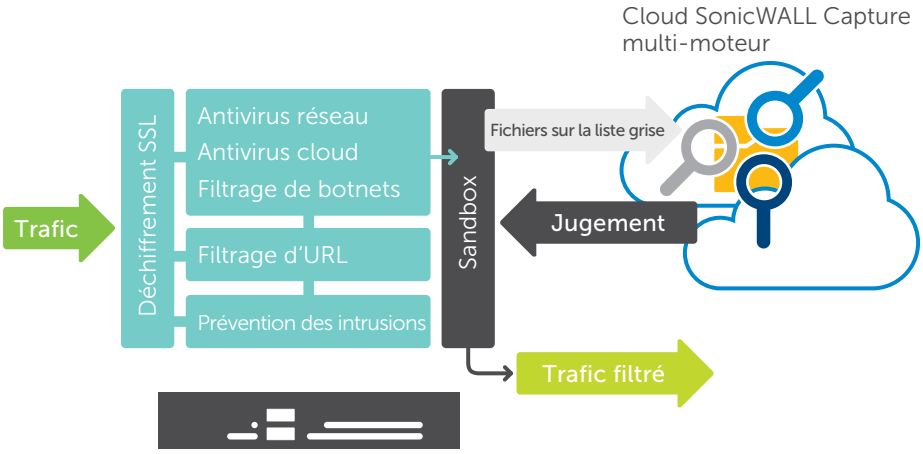
Dell SonicWALL Capture Advanced Threat Protection Service

Décuplez l'efficacité de votre sandbox pour une protection de pointe

Pour une protection efficace contre les menaces zero-day, les entreprises ont besoin de solutions intégrant des technologies d'analyse des malwares 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, Dell SonicWALL Capture Advance Threat Protection Service – un service cloud proposé avec les pare-feux Dell SonicWALL – détecte et bloque 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 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 n'impose pas de limites dans la taille des 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 Dell 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.



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

Avantages :

- Sécurité haute efficacité
- Délais de réponse brefs
- Coût total de possession réduit

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

Fonctionnalités

Analyse multi-moteur des menaces évoluées : Dell SonicWALL Capture Service 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 programmes malveillants connus. Les fichiers suspects sont envoyés au service cloud Dell SonicWALL Capture pour être analysés. La plate-forme sandbox multi-moteur, qui inclut le sandboxing virtualisé, l'émulation complète du système et une 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.

Analyse de nombreux types de fichiers de toute taille : le service assure l'analyse de pratiquement tous les types de fichiers, quelle que soit leur taille, notamment les programmes exécutables (PE), DLL, PDF, documents MS Office, archives, JAR et APK, ainsi que de divers systèmes d'exploitation comme Windows, Android et Mac OSX. 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.

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 Dell SonicWALL Capture pour empêcher toute infiltration plus poussée. Le malware est alors soumis à l'équipe Dell SonicWALL de renseignement sur les menaces pour y être analysé plus en profondeur et intégré aux bibliothèques de signatures de l'antivirus au niveau de la 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.

Le tableau de bord du service Dell SonicWALL Capture affiche le nombre de fichiers malveillants et anodins filtrés au cours des 30 derniers jours.

Plates-formes prises en charge :

Le service Dell SonicWALL Capture est pris en charge par les appliances de sécurité réseau Dell SonicWALL suivantes exécutant SonicOS version 6.2.5 ou supérieure :

SuperMassive 9600
SuperMassive 9400
SuperMassive 9200

NSA 6600
NSA 5600
NSA 4600
NSA 3600
NSA 2600

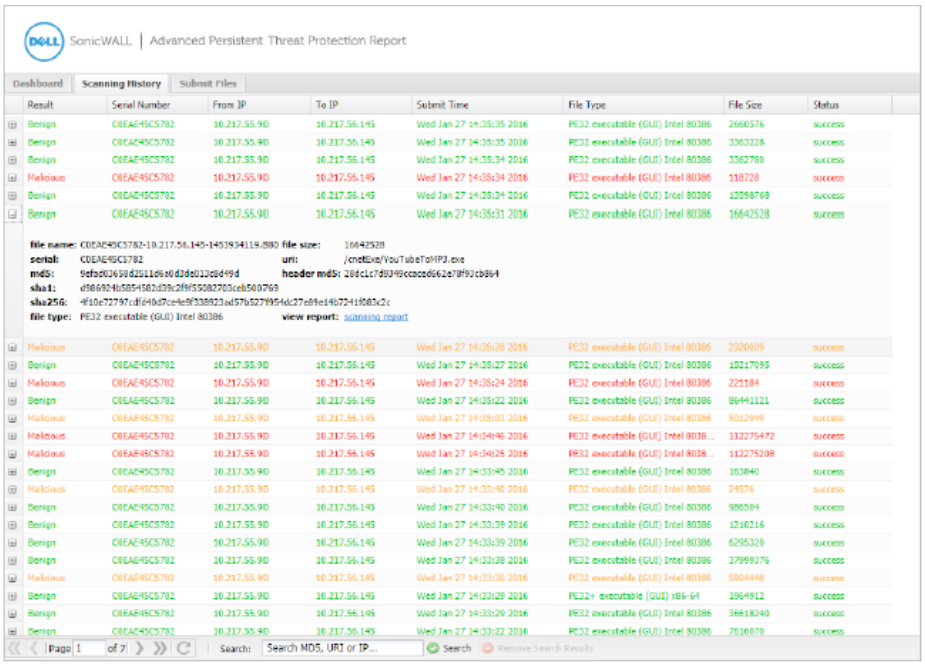
TZ600
TZ500 et TZ500 Wireless
TZ400 et TZ400 Wireless
TZ300 et TZ300 Wireless

SOHO Wireless

Reporting et alertes : le service Dell SonicWALL Capture 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. Ils contiennent notamment des données sur la session et des informations sur le système d'exploitation ainsi que sur l'activité de ce dernier et du réseau. Les alertes journal du pare-feu notifient l'envoi de fichiers suspects au service Dell SonicWALL Capture , avec le résultat de l'analyse.

A propos de Dell Security

Dell Security vous aide à créer et à entretenir une base de sécurité solide avec des solutions interconnectées à l'échelle de l'entreprise. Des terminaux et utilisateurs aux réseaux, données et identités, les solutions Dell Security limitent les risques et réduisent la complexité d'ensemble pour vous permettre de vous concentrer sur votre cœur de métier. www.dell.com/security



Le rapport historique des fichiers liste l'ensemble des fichiers filtrés et analysés, ainsi que le verdict rendu.
Un rapport d'analyse détaillé est également disponible pour les fichiers analysés.

Dell
5455 Great America Parkway, Santa Clara, CA 95054
www.dell.com/security
Si vous êtes situé en dehors de l'Amérique du Nord, vous trouverez les coordonnées des bureaux locaux sur notre site Internet.

Datasheet-SonicWALL-APTSandboxing-US-VG-27700