SonicWall Capture Client

Stoppez les failles plus vite qu'il est humainement possible... en toute autonomie

La menace en constante expansion que représentent les ransomwares et autres attaques par logiciels malveillants montre que l'efficacité des solutions de protection client ne se mesure pas à la simple conformité des terminaux. La technologie d'antivirus classique est fondée sur des signatures, une approche depuis longtemps en proie à des difficultés et qui n'est pas parvenue à suivre le rythme des malwares et techniques d'évasion de dernière génération.

De plus, avec la généralisation du télétravail, de la mobilité et du BYOD, il est devenu urgent de fournir une protection cohérente de tous les terminaux, où qu'ils soient, doublée de renseignements sur les vulnérabilités applicatives et de l'application de règles Web. SonicWall Capture Client est une offre unifiée proposant diverses fonctionnalités EPP et EDR à l'intention des terminaux.

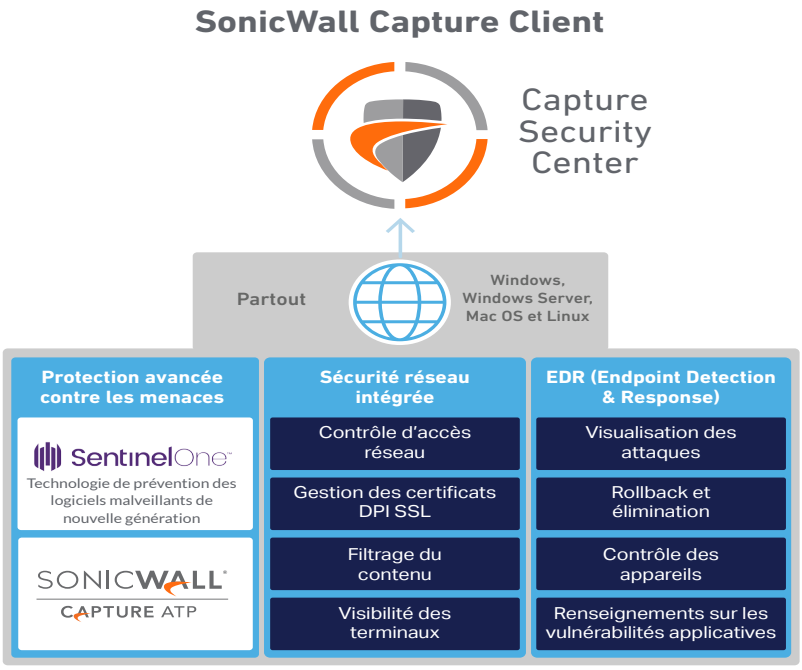
AVANTAGES

- Bénéficiez d'une détection efficace et directement exploitable des menaces
- Gestion centralisée dans le cloud avec de vraies fonctionnalités de mutualisation pour renforcer la sécurité du réseau et des terminaux
- Relevez le niveau de sécurité et armez les équipes IT d'une solution conviviale et intuitive pour combattre l'ennemi

La sécurité des terminaux adaptée à votre entreprise

Lisez la présentation : sonicwall.com

FICHE TECHNIQUE



Capture Client applique une protection contre les menaces évoluées basée sur le comportement et alimentée par l'antivirus de nouvelle génération SentinelOne.

Intégration de Capture ATP pour une sécurité encore plus efficace, des délais de réponse plus brefs et un coût total de possession réduit.

Fonctionnalités et avantages

Surveillance continue des comportements

- Visualisez les profils d'activité complets des fichiers, applications et processus et du réseau
- Protégez-vous contre les malwares agissant avec ou sans fichier
- Offrez une vue à 360 degrés des attaques avec des informations exploitables

Chasser les menaces avec une visibilité en profondeur

- Utilisez la visibilité en profondeur pour traquer les menaces en fonction d'indicateurs comportementaux et autres IOC (indicateurs de compromission) sur les appareils Windows, MacOS et Linux couverts
- Automatisez la chasse et la réaction aux menaces avec des règles et alertes personnalisées

Intégration de Capture ATP (Advanced Threat Protection)

- Chargez automatiquement les fichiers suspects sur des appareils Windows en vue d'une analyse avancée en sandbox
- Trouvez les menaces dormantes avant qu'elles ne s'exécutent, comme des logiciels malveillants comportant un délai de temporisation
- Référence à la base de données des verdicts de fichiers de Capture ATP sans avoir à charger les fichiers dans le cloud

Fonctionnalités uniques de rollback

- Prise en charge de règles éliminant totalement les menaces
- Restaurez des terminaux de manière autonome vers un état connu « bon » précédant le lancement de l'activité malveillante

Diverses techniques heuristiques sur plusieurs niveaux

- Exploitez la veille cloud, l'analyse statique avancée et la protection comportementale dynamique
- Protégez contre les logiciels malveillants connus et inconnus et remédiez-y avant, pendant ou après une attaque

Renseignements sur les vulnérabilités applicatives

- Cataloguez chaque application installée et tout risque associé
- Examinez les vulnérabilités connues avec des détails sur les CVE et les niveaux de gravité signalés
- Utilisez ces données pour hiérarchiser les corrections et réduire la surface d'attaque

Contrôle réseau des terminaux

- Ajoutez des contrôles de type pare-feu au niveau des terminaux
- Utilisez une base de règles de quarantaine supplémentaire pour gérer les appareils infectés

Remote Shell[1]

- Plus besoin d'être en contact physique avec les appareils pour dépanner, modifier des configurations locales ou réaliser des enquêtes forensiques

Pas besoin de scans réguliers ni de mises à jour périodiques

- Assurez le plus haut niveau de protection à tout moment, sans entraver la productivité des utilisateurs
- Recevez un scan complet à l'installation et bénéficiez d'une surveillance en continu les activités suspectes par la suite

Intégration aux pare-feux SonicWall en option

- Appliquez l'inspection approfondie des paquets du trafic chiffré (DPI SSL) sur les terminaux
- Déployez facilement des certificats de confiance au niveau de chaque terminal
- Dirigez les utilisateurs non protégés vers une page de téléchargement de Capture Client avant tout accès à Internet lorsqu'ils sont derrière un pare-feu

Filtrage du contenu

- Bloquez les adresses IP et domaines de sites malveillants
- Augmentez la productivité des utilisateurs en limitant la bande passante ou en restreignant l'accès aux contenus Web répréhensibles ou non productifs

Contrôle des appareils

- Empêchez les appareils potentiellement infectés de se connecter à des terminaux
- Utilisez des règles d'autorisation granulaires

Fonctionnalités de Capture Client		
Fonctionnalité	Advanced	Premier
Gestion, reporting et analyse cloud (CSC)	✓	✓
Intégrations de sécurité réseau		
Visibilité et exécution au niveau terminal	✓	✓
Déploiement de certificats DPI SSL	✓	✓
Filtrage du contenu	✓	✓
Protection avancée des terminaux		
Anti-malware de nouvelle génération	✓	✓
Sandboxing Capture Advanced Threat Protection	✓	✓
ActiveEDR (Endpoint Detection and Response)		
Visualisation des attaques	✓	✓
Rollback et élimination	✓	✓
Contrôle des appareils	✓	✓
Vulnérabilités applicatives et renseignements	✓	✓
Reconnaissance des terminaux non autorisés		✓
Contrôle réseau des terminaux		✓
Chasse aux menaces et renseignements ActiveEDR		
Chasse aux menaces avec une visibilité en profondeur		✓
Remote Shell[1]		✓
Catalogue d'exclusions		✓

[1] Remote shell sera disponible à la demande sur un nouveau compte (avec 2FA activée) directement sur la console S1.

Capture Client – configuration requise | SonicWall

Bonnes pratiques de sécurité globale des terminaux Processus pour les MSSP et les entreprises distribuées

Lisez le dossier : www.sonicwall.com

À propos de SonicWall

SonicWall offre une solution de cybersécurité sans limites pour l'ère de l'hyper-distribution, dans une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. En connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant de véritables économies, SonicWall comble le fossé commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour plus d'informations, rendez-vous sur www.sonicwall.com.

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