SONICWALL

SonicWall Capture Client

La menace sans cesse croissante des ransomware et des autres attaques par programmes malveillants a prouvé que les solutions de protection client ne peuvent pas être évaluées en se basant seulement sur la conformité des terminaux. La technologie antivirus traditionnelle utilise une approche basée sur les signatures. Elle est attaquée depuis longtemps et n'a pas su suivre le rythme des programmes malveillants et des techniques d'évasion émergents. De plus, avec la prolifération des télécommunications, de la mobilité et du BYOD, il y a un besoin urgent de fournir une protection cohérente des terminaux, où qu'ils soient.

SonicWall Capture Client est une offre unifiée pour les terminaux, dotée de plusieurs fonctionnalités de protection. Avec un moteur de protection contre les programmes malveillants de nouvelle génération optimisé par SentinelOne, Capture Client applique des techniques de protection contre les menaces évoluées, comme l'apprentissage automatique, l'intégration d'un sandbox réseau et la récupération du système. Capture Client tire également parti de l'inspection approfondie du trafic TLS chiffré (DPI-SSL) sur les pare-feu SonicWall en installant et en gérant des certificats TLS de confiance.

Capture Client co-existe avec les plateformes Global VPN Client de SonicWall et les règles pour tous les produits peuvent être gérées depuis une même console de gestion dans le cloud. Capture Client peut être facilement ajouté à n'importe quel client déployé, soit par des règles de groupe Microsoft Active Directory ou par une toute autre technique de déploiement tierce, ou encore via la fourniture d'URL personnalisées depuis lesquelles des clients peuvent se télécharger et s'installer automatiquement et silencieusement, sans intervention supplémentaire. Et, lorsqu'il est intégré aux pare-feu SonicWall, Capture Client offre une expérience silencieuse sans intervention pour le déploiement sur des clients non protégés.

Caractéristiques et avantages

Une **surveillance continue des comportements** du client contribue à créer un profil complet de l'activité des fichiers, des applications et des processus, ainsi que de l'activité des réseaux. Cela permet une protection contre les programmes malveillants basés ou non sur fichier et fournit une vue des attaques à 360° avec des renseignements exploitables pertinents pour les investigations.

Parmi les **multiples techniques heuristiques sur plusieurs niveaux** pour la protection, on peut citer les renseignements sur le cloud, l'analyse statique avancée et la protection comportementale dynamique. Ces dernières contribuent à protéger et à agir contre des programmes malveillants connus et inconnus.

L'absence de nécessité d'analyses régulières ou de mises à jour périodiques permet un niveau de protection optimal à tout moment, sans freiner la productivité de l'utilisateur.

L'intégration de Capture Advanced Threat Protection (ATP) télécharge automatiquement les fichiers suspects pour une analyse avancée via une manipulation des codes que les terminaux ne peuvent pas réaliser. Bloquez davantage de menaces avant leur exécution, comme les programmes malveillants, avec des reports de synchronisation intégrés. Les administrateurs peuvent également se reporter à la base de données de Capture ATP des verdicts de fichiers, sans avoir besoin de télécharger des fichiers vers le cloud pour l'analyse.

Les capacités uniques de récupération prennent également en charge les règles qui non seulement suppriment la menace complètement, mais restaurent également un client ciblé à son état antérieur avant l'activité du programme malveillant. Ainsi, il n'y a plus besoin de

Avantages

- Gestion indépendante dans le cloud
- Synergie avec les pare-feu SonicWall
- Application de règles de sécurité
- Gestion des certificats DPI-SSL
- Surveillance continue des comportements
- Déterminations très précises grâce à l'apprentissage automatique
- Multiples techniques heuristiques sur plusieurs niveaux
- Capacités uniques de récupération
- Établissement simplifié de listes blanches/noires
- Sandbox cloud Capture Advanced Threat Protection (ATP) pour l'analyse automatisée des programmes malveillants
- Partage de renseignements sur les menaces sans téléchargement pour une inspection manuelle des fichiers
- Protection contre les menaces sur le Web
- Contrôle des appareils

faire de restauration manuelle en cas de ransomware et d'attaques similaires sur Windows.

La console de gestion dans le cloud réduit la présence et les dépenses liées à la gestion. Elle améliore également la capacité à déployer et appliquer une protection des terminaux, quel que soit leur emplacement.

L'intégration facultative aux pare-feu SonicWall de génération 6 et supérieure permet un déploiement sans intervention et une conformité améliorée des terminaux. De plus, elle permet l'application de l'inspection approfondie des paquets du trafic chiffré (DPI-SSL) en déployant des certificats fiables à chaque terminal.

La fonction de protection contre les menaces sur le Web et de contrôle des appareils permet aux organisations de bloquer des sites et des adresses IP malveillants, ainsi que d'empêcher des appareils potentiellement infectés et inconnus de se connecter au terminal.

Gestion centralisée et reporting sur la protection client : la console de gestion dans le cloud de SonicWall fonctionne comme un écran unique permettant de gérer toutes les règles des clients, notamment la protection contre les programmes malveillants de nouvelle génération, la gestion des certificats DPI-SSL, le filtrage de contenu et les VPN.

La console de gestion est une plateforme mutualisée dans le cloud proposée sans frais supplémentaire. Elle fournit une fonction de gestion des règles et de reporting sur la protection client, avec une prise en charge des règles de contrôle d'accès granulaire. Cela permet aux fournisseurs de services gérés de gérer et d'établir des rapports sur des clients de plusieurs acheteurs. En même temps, chacun de ces acheteurs peut uniquement gérer et établir des rapports sur ses propres clients.

Cette solution fonctionne également comme une plateforme d'investigation pour aider à identifier la cause racine des menaces de programmes malveillants détectés et fournit des renseignements exploitables afin d'éviter toute récurrence. Par exemple, un administrateur peut facilement consulter quelles applications s'exécutent sur un client. Cela peut ainsi aider à identifier les machines qui peuvent exécuter des logiciels vulnérables ou non autorisés.

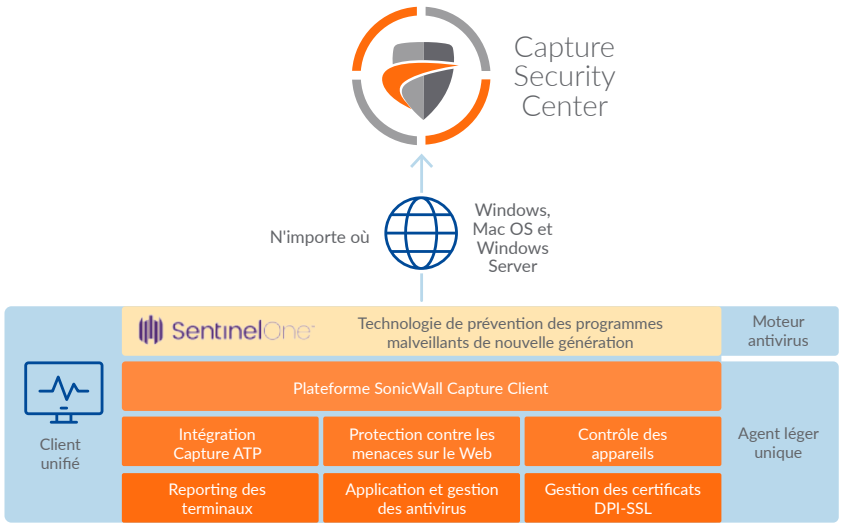
Offres et prise en charge de plateforme

La solution SonicWall Capture Client se décline en deux versions :

SonicWall Capture Client Basic fournit toutes les fonctions de protection et de correction des programmes malveillants de nouvelle génération, ainsi que des capacités de prise en charge DPI-SSL.

SonicWall Capture Client Advanced fournit toutes les fonctions mentionnées ci-dessus pour la version Basic, plus des capacités de récupération avancées, l'intégration de Capture ATP, la visualisation des attaques et la protection contre les menaces sur le Web.

Les deux offres sont disponibles pour Windows 7 ou toute version ultérieure, ainsi que pour Mac OSX.



CONFIGURATION REQUISE

Systèmes d'exploitation
Windows 7 et version ultérieure
Windows Server 2008 R2 et version ultérieure
Mac OS/OSX 10.10 et version ultérieure
Matériel
Processeur double cœur 1 GHz ou version supérieure
1 Go de RAM ou plus si requis par le système d'exploitation (2 Go recommandés)
Espace disque libre de 2 Go

COMPARAISON DES FONCTIONNALITÉS

Fonctionnalité	Capture Client Basic	Capture Client Advanced
Déploiement des certificats DPI-SSL	✓	✓
Application des pare-feu	✓	✓
Protection par antivirus de nouvelle génération (NGAV)	✓	✓
Établissement de listes blanches/noires des applications	✓	✓
Analyse automatisée de Capture Advanced Threat Protection (ATP)	–	✓
Partage des renseignements sur les menaces avec Capture ATP	–	✓
Correction/récupération	–	✓
Visualisation des attaques	–	✓
Protection contre les menaces sur le Web	–	✓
Contrôle des appareils	–	✓

UGS CAPTURE CLIENT		
Produit	Validité	Référence
ADVANCED		
SONICWALL CAPTURE CLIENT ADVANCED, 5 À 24 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1518
SONICWALL CAPTURE CLIENT ADVANCED, 5 À 24 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1519
SONICWALL CAPTURE CLIENT ADVANCED, 25 À 49 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1520
SONICWALL CAPTURE CLIENT ADVANCED, 25 À 49 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1521
SONICWALL CAPTURE CLIENT ADVANCED, 50 À 99 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1522
SONICWALL CAPTURE CLIENT ADVANCED, 50 À 99 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1523
SONICWALL CAPTURE CLIENT ADVANCED, 100 À 249 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1524
SONICWALL CAPTURE CLIENT ADVANCED, 100 À 249 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1525
SONICWALL CAPTURE CLIENT ADVANCED, 250 À 499 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1454
SONICWALL CAPTURE CLIENT ADVANCED, 250 À 499 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1455
SONICWALL CAPTURE CLIENT ADVANCED, 500 À 999 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1456
SONICWALL CAPTURE CLIENT ADVANCED, 500 À 999 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1457
SONICWALL CAPTURE CLIENT ADVANCED, 1 000 À 4 999 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1458
SONICWALL CAPTURE CLIENT ADVANCED, 1 000 À 4 999 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1459
SONICWALL CAPTURE CLIENT ADVANCED, 5 000 À 9 999 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1460
SONICWALL CAPTURE CLIENT ADVANCED, 5 000 À 9 999 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1461
SONICWALL CAPTURE CLIENT ADVANCED, PLUS DE 10 000 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1462
SONICWALL CAPTURE CLIENT ADVANCED, PLUS DE 10 000 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1463
BASIC		
SONICWALL CAPTURE CLIENT BASIC, 5 À 24 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1510
SONICWALL CAPTURE CLIENT BASIC, 5 À 24 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1511
SONICWALL CAPTURE CLIENT BASIC, 25 À 49 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1512
SONICWALL CAPTURE CLIENT BASIC, 25 À 49 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1513
SONICWALL CAPTURE CLIENT BASIC, 50 À 99 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1514
SONICWALL CAPTURE CLIENT BASIC, 50 À 99 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1515
SONICWALL CAPTURE CLIENT BASIC, 100 À 249 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1516
SONICWALL CAPTURE CLIENT BASIC, 100 À 249 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1517
SONICWALL CAPTURE CLIENT BASIC, 250 À 499 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1444
SONICWALL CAPTURE CLIENT BASIC, 250 À 499 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1445
SONICWALL CAPTURE CLIENT BASIC, 500 À 999 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1446
SONICWALL CAPTURE CLIENT BASIC, 500 À 999 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1447
SONICWALL CAPTURE CLIENT BASIC, 1 000 À 4 999 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1448
SONICWALL CAPTURE CLIENT BASIC, 1 000 À 4 999 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1449
SONICWALL CAPTURE CLIENT BASIC, 5 000 À 9 999 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1450
SONICWALL CAPTURE CLIENT BASIC, 5 000 À 9 999 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1451
SONICWALL CAPTURE CLIENT BASIC, PLUS DE 10 000 TERMINAUX avec support 24 h/24, 7 j/7	3ANS	02-SSC-1452
SONICWALL CAPTURE CLIENT BASIC, PLUS DE 10 000 TERMINAUX avec support 24 h/24, 7 j/7	1AN	02-SSC-1453

À propos de SonicWall

Depuis plus de 27 ans, SonicWall lutte contre la cybercriminalité pour défendre les PME, les grandes entreprises et les agences gouvernementales du monde entier. S'appuyant sur les travaux de recherche des Capture Labs de SonicWall, nos solutions primées de détection et de prévention des intrusions en temps réel sécurisent plus d'un million de réseaux et leurs e-mails, applications et données dans plus de 215 pays et territoires. Ces entreprises peuvent ainsi fonctionner plus efficacement sans crainte pour leur sécurité. Pour en savoir plus, rendez-vous sur www.sonicwall.com ou suivez-nous sur Twitter, LinkedIn, Facebook et Instagram.

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

Datasheet-CaptureClient-US-VG-MKTG5184