SONICWALL

SonicWall Capture Client

La menace sans cesse croissante des ransomwares 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 un système basé sur la signature, qui a fait l'objet d'une bataille de longue date et n'arrive plus à suivre le rythme des techniques d'évasion et des logiciels malveillants émergents. De plus, avec la prolifération des télécommunications, de la mobilité et des politiques « apportez votre propre appareil » (BYOD), il y a un besoin urgent de fournir une protection cohérente et une application des politiques Web à l'égard 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 multimoteur 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 coexiste avec SonicWall Global VPN Client 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. En outre, lorsqu'il est intégré aux pare-feu SonicWall, Capture Client offre une expérience sans intervention pour le déploiement sur des clients non protégés avec des capacités de contraintes d'application facultatives.

Gestion centralisée et élaboration de rapports sur la protection des clients

La console de gestion basée sur le cloud et le tableau de bord global de SonicWall ont été conçus pour donner aux prestataires de services de sécurité gérés (MSSP) un aperçu de la santé de leurs locataires en adoptant une perspective globale. Les administrateurs peuvent connaître la santé de chaque locataire, qui est évaluée selon le nombre d'infections, les vulnérabilités présentes, la version de Capture Client installée et l'identité des éléments et des personnes les plus bloqués par le filtrage de contenu. Ce tableau de bord peut également vous indiquer quels appareils sont en ligne et en cours de fonctionnement.

La Politique globale permet aux administrateurs d'appliquer une politique de référence unique pour tous les locataires, ce qui facilite la création de nouveaux locataires. Cela permet également aux MSSP d'établir rapidement des protections contre les nouvelles menaces pour tous les locataires visés par cette politique. Lorsque l'option « Héritage » est activée, tous les nouveaux locataires sont visés par la Politique globale. Lorsque cette option est désactivée, des politiques uniques peuvent être créées et modifiées pour les locataires individuels à tous les niveaux, du filtrage de contenu à la protection contre les logiciels malveillants, en passant par la gestion des certificats DPI-SSL.

Bénéficiez d'une prise en charge des politiques granulaires de contrôle d'accès, en ayant notamment la possibilité d'attribuer des politiques basées sur les attributs Microsoft Active Directory (par groupe d'utilisateurs par exemple). Cela permet aux prestataires de services gérés (MSSP et MSP) d'administrer et d'établir des rapports sur les clients de plusieurs acheteurs. En même temps, chacun de ces acheteurs peut uniquement gérer et établir des rapports sur ses propres clients.

La console de gestion 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.

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
- Informations sur la vulnérabilité des applications
- Capacités uniques de récupération
- Tableau de bord sur la santé globale pour tous les locataires
- Création de politiques globales en toute simplicité
- Classement simple dans la liste d'autorisation ou de blocage
- 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
- Filtrage du contenu
- Contrôle des appareils

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.

Caractéristiques et avantages

Surveillance continue des comportements

- Visualisez des profils complets sur l'activité des fichiers, des applications, des processus et du réseau
- Protégez-vous des logiciels malveillants basés sur des fichiers et sans fichiers
- Bénéficiez d'une vue à 360 degrés sur les attaques avec des renseignements exploitables

Multiples techniques heuristiques sur plusieurs niveaux

- Mettez à profit les renseignements infonuagiques, les analyses statiques avancées et la protection comportementale dynamique
- Protégez-vous des logiciels malveillants connus et inconnus et remédiez aux problèmes avant, pendant ou après une attaque

Nul besoin d'analyses régulières ou de mises à jour périodiques

- Offrez aux utilisateurs le plus haut niveau de protection en toutes circonstances, sans entraver leur productivité
- Bénéficiez d'une analyse complète au moment de l'installation et d'une surveillance en permanence de toute activité suspecte par la suite

Intégration de Capture Advanced Threat Protection (ATP) (pour les appareils Windows)

- Téléchargez automatiquement les fichiers suspects sur les appareils Windows pour une analyse sandbox avancée
- Identifiez les menaces latentes avant leur exécution, comme les programmes malveillants dotés de dispositifs d'exécution différée
- Consultez la base de données sur les verdicts de fichiers de Capture ATP, sans avoir besoin de télécharger des fichiers vers le cloud

Capacités uniques de récupération (pour Windows)

- Politiques de prise en charge qui éliminent complètement les menaces
- Restaurez l'état dans lequel les terminaux se trouvaient avant le début d'une activité malveillante
- Plus besoin de faire de restauration manuelle en cas de ransomware ou d'attaques similaires

Informations sur la vulnérabilité des applications (pour Windows et macOS)

- Répertoriez chaque application installée et tout risque connexe
- Passez en revue les vulnérabilités connues avec les détails des vulnérabilités et expositions courantes et les niveaux de gravité signalés
- Utilisez ces données pour classer par ordre de priorité les correctifs à appliquer et réduire la surface d'attaque

Intégration en option aux pare-feu SonicWall

- Instaurez l'application de l'inspection approfondie des paquets du trafic chiffré (DPI-SSL) sur les terminaux
- Déployez facilement des certificats fiables sur chaque terminal
- Orientez les utilisateurs non protégés vers une page de téléchargement de Capture Client avant d'accéder à Internet lorsqu'ils se trouvent derrière un pare-feu

Filtrage du contenu (pour Windows et macOS)

- Bloquez les adresses IP et les domaines des sites malveillants
- Augmentez la productivité des utilisateurs en limitant la bande passante ou en restreignant l'accès à du contenu Web répréhensible ou non productif

Contrôle des appareils (pour Windows et macOS)

- Empêchez les périphériques potentiellement infectés de se connecter aux terminaux
- Utilisez des politiques granulaires basées sur des listes d'autorisation

Offres et prise en charge de plateforme

La solution SonicWall Capture Client se décline en deux versions :

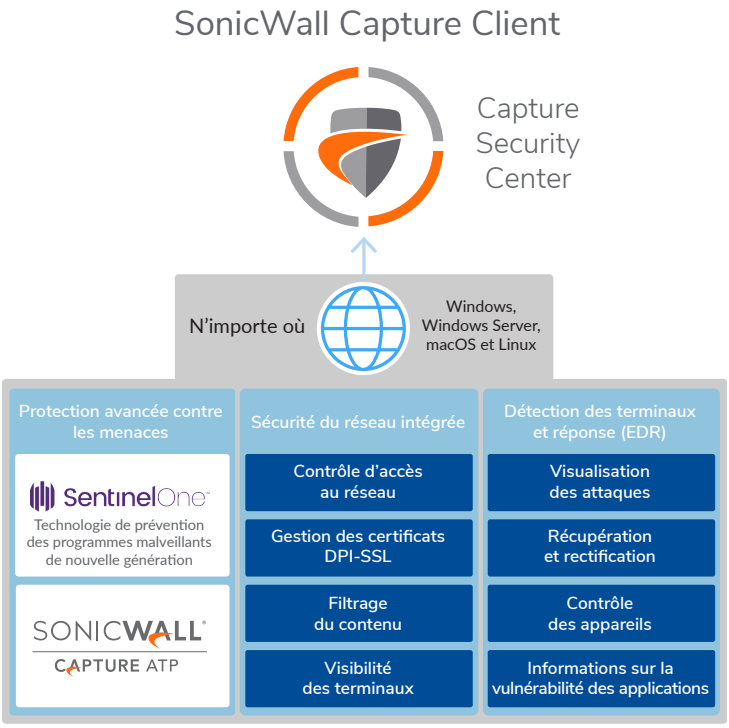
L'offre SonicWall Capture Client Basic regroupe :

- Tous les modules de protection contre les logiciels malveillants de nouvelle génération de SonicWall
- Fonctionnalités de correction
- Capacités de prise en charge DPI-SSL

L'offre SonicWall Capture Client Advanced regroupe :

- Tout ce qui est indiqué ci-dessus pour l'offre Basic
- Capacités avancées de récupération
- Intégration de Capture ATP
- Visualisation des attaques
- Informations sur la vulnérabilité des applications
- Filtrage du contenu

Les deux offres sont disponibles pour Windows 7 et versions ultérieures, Mac OS X et Linux (reportez-vous ci-dessous pour tout savoir sur la configuration requise).



COMPARAISON DES FONCTIONNALITÉS		
Fonctionnalité	**Basic**	**Advanced**
Gestion, reporting et analyse dans le cloud (CSC)	✓	✓
Sécurité du réseau intégrée		
Visibilité des terminaux	✓	✓
Déploiement des certificats DPI-SSL	✓	✓
Filtrage du contenu	–	✓
Protection avancée contre les menaces		
Anti-logiciel malveillant de nouvelle génération	✓	✓
Sandbox de Capture Advanced Threat Protection	–	✓
Détection des terminaux et réponse		
Visualisation des attaques	–	✓
Récupération et rectification	–	✓
Contrôle des appareils	–	✓
Informations et vulnérabilité des applications	–	✓

CONFIGURATION REQUISE
Systèmes d'exploitation
Windows 7 et versions ultérieures
Windows Server 2008 R2 et versions ultérieures
Mac OS/OSX 10.10 et versions ultérieures
Amazon Linux AMI
Red Hat Enterprise Linux RHEL v5.5-5.11, 6.5+, 7.0+
Ubuntu 12.04, 14.04, 16.04, 16.10
CentOS 6.5+, 7.0+
Oracle Linux OL (anciennement Oracle Enterprise Linux ou OEL) v6.5-6.9 et v7.0+
SUSE Linux Enterprise Server 12
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

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

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 en savoir plus, rendez-vous sur www.sonicwall.com.

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

Datasheet-CaptureClient-US-VG-2889