

# 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 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 logiciels malveillants ni 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 endpoints, 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 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.

## Caractéristiques et avantages

La **surveillance continue des comportements** du terminal 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. Capture Client réalise une analyse complète au moment de l'installation et surveille en permanence toute activité suspecte par la suite.

L'**intégration de Capture Advanced Threat Protection (ATP)** télécharge automatiquement les fichiers suspects pour une analyse sandbox 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

## 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
- 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
- Filtrage du contenu
- Contrôle des appareils

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

Les **informations sur la vulnérabilité des applications** donnent aux administrateurs la possibilité de cataloguer chaque application sur chaque terminal protégé et tout risque associé. Le risque est basé sur la présence de vulnérabilités connues avec des détails sur les CVE et les niveaux de gravité rapportés pour cette version, fournissant à l'administrateur des renseignements exploitables pour hiérarchiser les correctifs et réduire la surface d'attaque du terminal.

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.

Le **filtrage de contenu** permet aux organisations de bloquer les adresses IP et les domaines des sites malveillants et d'augmenter la productivité des utilisateurs en limitant la bande passante ou l'accès à du contenu Web répréhensible ou improductif.

Le **contrôle des appareils** permet aux organisations de bloquer la connexion des appareils potentiellement infectés au terminal avec des politiques de liste blanche granulaires.

**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 et le filtrage de contenu.

La console de gestion est une plateforme mutualisée dans le cloud proposée sans frais supplémentaire. Elle fournit des rapports sur la protection des clients et sur la gestion des politiques, avec un soutien pour les politiques de contrôle d'accès granulaire, y compris la possibilité d'attribuer des politiques basées sur les attributs Microsoft Active Directory. 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.

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. 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

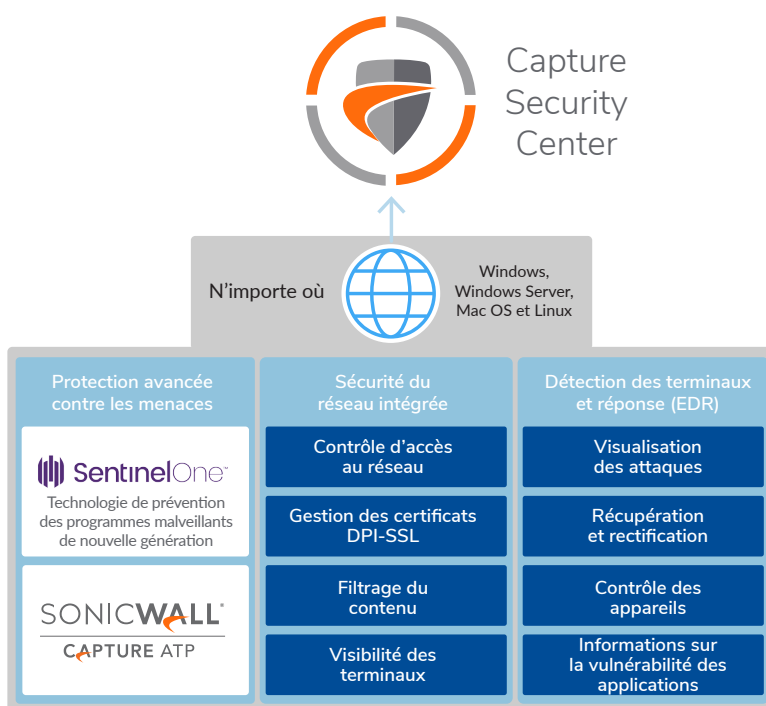
La solution SonicWall Capture Client se décline en deux versions :

**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, les informations sur la vulnérabilité des applications et le filtrage de contenu.

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

## SonicWall Capture Client



## COMPARAISON DES FONCTIONNALITÉS

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

## CONFIGURATION REQUISE

### Systemes 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

## UGS CAPTURE CLIENT

Produit	Validité	Référence
<b>ADVANCED</b>		
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
<b>BASIC</b>		
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 Boundless Cybersecurity 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 une percée économique, 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](http://www.sonicwall.com).