

SonicWall Capture Security appliance 1000

SonicWall Capture Security appliance™ (CSa) intègre la fonction Capture Advanced Threat Protection™ (ATP) et l'analyse sandbox des logiciels malveillants aux scénarios de déploiement sur site pour les clients soumis à des restrictions de conformité et de politique en ce qui concerne l'envoi de fichiers pour analyse dans le cloud, ou qui préfèrent que toutes leurs données restent au sein de leur organisation. CSa 1000 peut analyser les fichiers suspects provenant d'autres produits SonicWall afin d'assurer une détection rapide et hautement précise des menaces inconnues tout en permettant au client de rester en possession de ses fichiers. De plus, la fonctionnalité de l'API REST sur CSa offre les avantages de cette capacité d'analyse de fichiers très efficace aux équipes de renseignements sur les menaces, aux systèmes de sécurité tiers et à toute pile logicielle pouvant être intégrée aux API publiées.

CSa utilise une combinaison de vérifications basés sur la réputation, d'analyses statiques des fichiers et du moteur breveté Real-Time Deep Memory Inspection™ (RTDMI) de SonicWall pour l'analyse dynamique, afin de garantir un taux de détection des fichiers malveillants qui soit le meilleur, le plus efficace et le plus rapide possible. L'écosystème des produits de sécurité de SonicWall, déjà entièrement intégré à l'analyse Capture ATP dans le cloud, est capable d'appliquer la sécurité en ligne avec des fonctionnalités telles que le blocage jusqu'au verdict.

Les mêmes capacités sont prises en charge lorsque les produits SonicWall sont connectés à la série CSa au lieu de Capture ATP dans le cloud.

RTDMI

Le moteur d'analyse de fichiers RTDMI (Real-Time Deep Memory Inspection) de SonicWall, en instance de brevet, est une nouvelle méthode d'analyse des fichiers suspects qui surveille le comportement d'une application en mémoire. Le moteur RTDMI peut voir à travers toutes les techniques de brouillage ou de cryptage que les logiciels malveillants modernes peuvent déployer pour échapper au réseau et à l'analyse sandbox, offrant une détection extrêmement précise des attaques transmises par des documents, des fichiers exécutables, des fichiers d'archives et une variété d'autres types de fichiers.

Protection en temps réel

Les vérifications de la réputation et des renseignements au niveau mondial, les analyses statiques et la technologie RTDMI fonctionnent de concert pour fournir des résultats assez rapidement pour mettre en place des technologies telles que le blocage jusqu'au verdict dans les produits SonicWall. Cette capacité permet aux règles d'inspection des fichiers sur le pare-feu d'empêcher le téléchargement de fichiers suspects par l'utilisateur final jusqu'à ce que l'inspection complète soit terminée et qu'un verdict soit rendu par Capture ATP ou CSa.



Avantages :

- Inspection basée sur la mémoire avec RTDMI
- Analyse en plusieurs étapes avec vérification de la réputation, analyse statique et analyse dynamique
- Accès API pour l'analyse des menaces
- Prise en charge de nombreux types de fichiers
- Prise en charge du blocage jusqu'au verdict
- Haute efficacité sécuritaire
- Reporting et accès basés sur les rôles

La confiance et l'expérience de nombreux clients

- CSa combine la technologie Capture ATP de SonicWall, un service basé sur le cloud fiable et utilisé par plus de 150 000 clients à travers le monde, sous la forme d'un appareil.
- CSa reçoit également des mises à jour régulières des renseignements pour assurer sa synchronisation avec les renseignements sur les menaces recueillis à l'échelle mondiale via l'analyse de fichiers Capture ATP de SonicWall.

Reporting, analyse et administration

- CSa fournit un aperçu des fichiers soumis à partir de toutes les sources avec un tableau de bord et un historique des analyses de fichiers faciles à naviguer, fournissant un aperçu de la fréquence, des sources, des verdicts et d'autres informations sur les fichiers soumis pour analyse.
- Les capacités de reporting offrent une vision globale de la protection ATP dans toute l'organisation, avec la possibilité de programmer des rapports réguliers configurés en fonction des différents rôles.
- Les administrateurs peuvent accorder un accès granulaire à CSa 1000 à divers rôles, avec la possibilité de restreindre l'accès à n'importe quelle partie de l'interface utilisateur.
- Les analystes de sécurité peuvent accéder à l'historique des analyses et modifier la liste blanche/noire et les appareils autorisés, et signaler tout faux positif ou faux négatif suspecté.
- Les administrateurs réseau peuvent accéder à la configuration opérationnelle de l'appareil sans toutefois pouvoir consulter, pour des raisons de confidentialité, les fichiers soumis et leurs sources.



The Scanning History page shows a table of analyzed files with columns for Verdict, File Name, File Hash, Frequency Name, From, Type, and Destination. A detailed view of a malicious file (FILEXEXE) is shown on the right, including file info, imports info, and analysis results.

Verdict	File Name	File Hash	Frequency Name	From	Type	Destination
Malicious	5.exe	56474078-003396...	PE32 exe	...
Malicious	lg1.exe	55474078-003396...	PE32 exe	...
Malicious	Weekly_ZK_Declar...	5a7554e3a3114b...	PDF doc	...
Malicious	Weekly_ZK_Calendr...	90a02aa399a8b0...	PDF doc	...
Malicious	Weekly_ZK_Calendr...	42754e8f8e120e...	PDF doc	...
Malicious	x21.exe	c38050505d6287...	XZ comp	...
Malicious	17aab8f84545a13b...	17aab8f84545a13b...	XZ comp	...
Malicious	17aab8f84545a13b...	9488434f7896b...	XZ comp	...
Malicious	17aab8f84545a13b...	313a3951472a2a...	XZ comp	...
Malicious	17aab8f84545a13b...	b4aa657293282f...	XZ comp	...
Malicious	17aab8f84545a13b...	5aa857a9a92a7a...	XZ comp	...
Malicious	17aab8f84545a13b...	4f564780484808...	XZ comp	...
Malicious	17aab8f84545a13b...	68482626262626...	XZ comp	...
Malicious	x21.exe	c38050505d6287...	XZ comp	...
Malicious	38aa9534544444...	38aa9534544444...	XZ comp	...
Malicious	HACK.exe	95c10e03b08f0e...	PE32 exe	...
Malicious	prpqr.exe	c13623060e184c...	PE32 exe	...
Malicious	qbf.exe	24040840804808...	PE32 exe	...
Malicious	qbf0x3.dll	432326a8306830...	PE32 exe	...
Malicious	fwsh3.dll.1	a7706a80808080...	PE32 exe	...
Malicious	rsu3.dll.3	e285562355044...	PE32 exe	...
Malicious	mmap340.dll	334e94c3927070...	PE32 exe	...
Malicious	dlmmap.exe	6627a7a73a3a3a...	PE32 exe	...
Malicious	hax.exe	65a47961a54332...	PE32 exe	...
Malicious	dlh.exe	90a28282828282...	PE32 exe	...

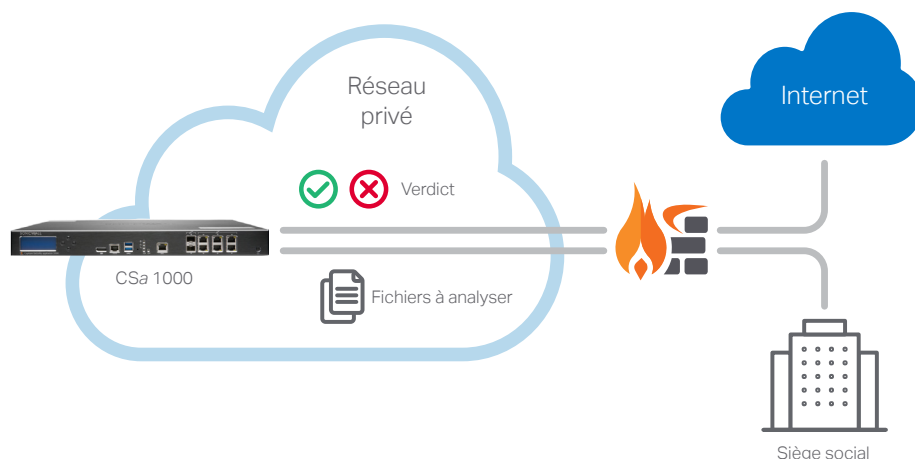
Fonctionnalités

- Recherche de réputation et de verdict global (configurable)
- Analyse statique et analyse dynamique avec RTDMI
- Liste blanche/liste noire sur le hachage/domaine
- Reporting planifié configurable
- Administration basée sur les rôles (rôles configurables)
- Gestion : HTTPS ou SSH via une interface de gestion dédiée ou une interface réseau régulière
- Accès à la console SSH
- Journalisation et alerte
- Reporting des faux positifs et faux négatifs avec mise automatique en liste blanche/liste noire
- Connectivité directe ou via VPN (avec adressage de l'adresse IP)
- Fonctionnement fermé du réseau
- Prise en charge de l'API REST pour la soumission et l'analyse de fichiers
- SE renforcé avec Secure Boot et chaîne de confiance anti-manipulation
- Journalisation locale

1. Le débit d'analyse dépend de la connectivité réseau, des types de fichiers et des niveaux de compression, et il peut varier par rapport aux valeurs publiées.
 2. Bien qu'il n'y ait pas de limite stricte, le nombre d'appareils sera déterminé par le nombre de fichiers soumis par chaque appareil. La plage recommandée à la publication est d'environ 250 appareils.
 3. Toutes les séries TZ, NSa et SuperMassive qui peuvent exécuter SonicOS 6.5.4.6 ou une version ultérieure. Non pris en charge sur les séries SuperMassive 9800 et NSsp 12000.

Options de déploiement

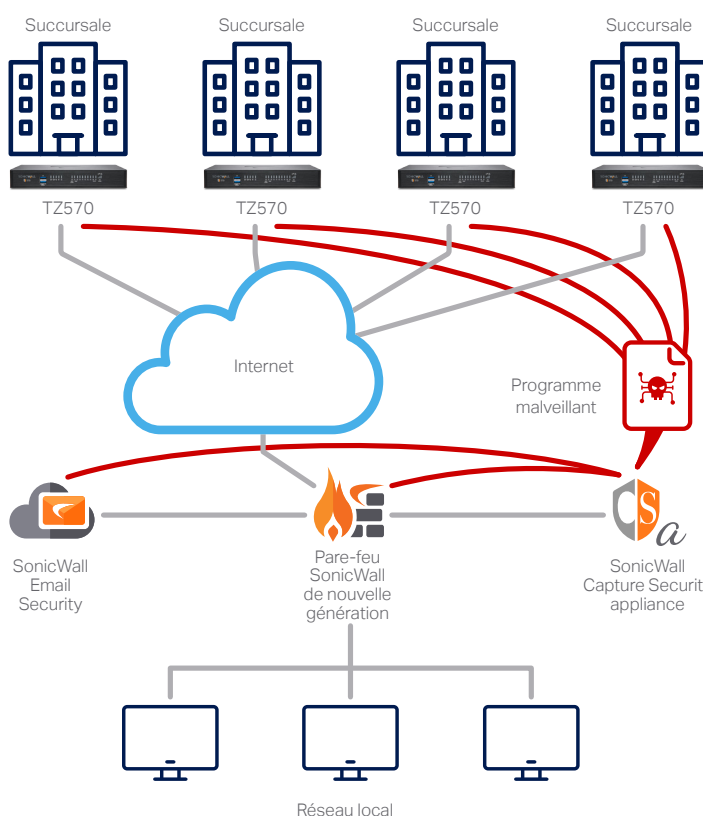
- Le déploiement de SonicWall CSa est simple et rapide, ne nécessitant qu'une configuration de base du réseau, du reporting et de l'accès des appareils autorisés pour commencer.
- CSa est compatible avec l'adressage des adresses IP et peut donc être déployé n'importe où tant qu'il est accessible par les appareils qui soumettent des fichiers pour analyse.



Il existe trois principales méthodes de déploiement de CSa 1000 :

Bureau unique/emplacement unique

- CSa peut être déployé n'importe où sur le réseau à condition que les produits qui l'utiliseront puissent l'atteindre via une adresse IP¹.
- Une fois CSa déployé, les pare-feu et les systèmes de sécurité de messagerie (d'autres solutions seront bientôt disponibles) peuvent être configurés pour rediriger les fichiers suspects vers CSa plutôt que vers le cloud pour l'analyse ATP.



Entreprise distribuée/sites multiples

- Plusieurs bureaux/succursales peuvent être configurés pour partager l'accès à un seul appareil CSa, déployé soit dans le centre de données du siège central, soit dans un centre de données distant accessible par tous les appareils.
- L'accès peut être direct sur Internet ou via VPN.
- La configuration de masse des systèmes SonicWall pour les diriger vers CSa peut se faire soit avec la solution GMS, soit avec des solutions de gestion centralisée NSM dans le cloud pour une configuration et un déploiement rapides.

Passerelle API REST

- CSa possède une interface API REST qui peut être utilisée pour soumettre des fichiers à des fins d'analyse, dont les résultats peuvent alors être examinés par les équipes de renseignements sur les menaces en utilisant leurs propres scripts, les intégrations du portail Web et d'autres produits de sécurité.
- Des instructions sur l'utilisation du script API pour CSa et des échantillons de code sont disponibles à l'adresse <https://github.com/sonicwall>

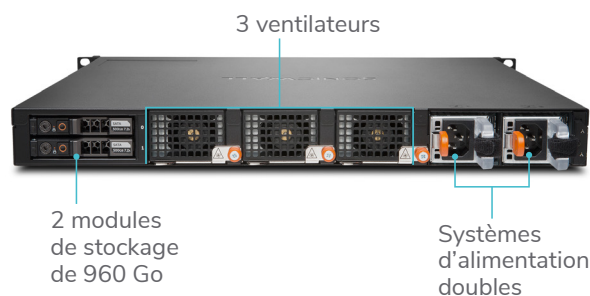
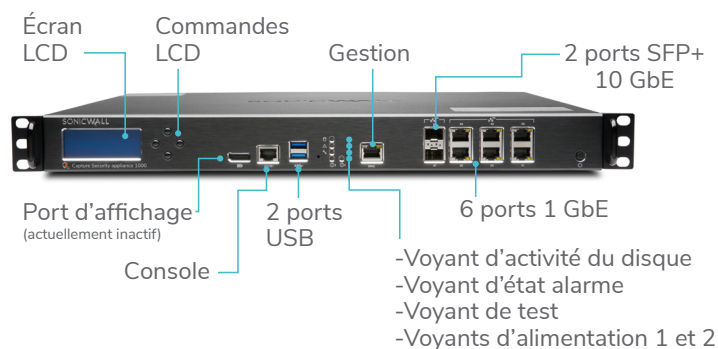
*¹ Les pare-feu SonicWall nécessitent également un accès UDP sur le port 2259.

1. Le débit d'analyse dépend de la connectivité réseau, des types de fichiers et des niveaux de compression, et il peut varier par rapport aux valeurs publiées.

2. Bien qu'il n'y ait pas de limite stricte, le nombre d'appareils sera déterminé par le nombre de fichiers soumis par chaque appareil. La plage recommandée à la publication est d'environ 250 appareils.

3. Toutes les séries TZ, NSa et SuperMassive qui peuvent exécuter SonicOS 6.5.4.6 ou une version ultérieure. Non pris en charge sur les séries SuperMassive 9800 et NSp 12000.

CSa 1000



Spécifications de SonicWall CSa 1000

FONCTIONNALITÉS	
Débit de recherche de réputation et des menaces globales (fichiers par heure) ¹	12 000
Débit du mix de fichiers réel (fichiers par heure) ¹	2500
Débit de l'analyse dynamique (RTDMI) (fichiers par heure) ¹	300
Taille maximale de fichier	100 Mo
Nombre maximal d'appareils pris en charge ²	Basé sur la performance
Profondeur maximale d'analyse des archives	3
Prise en charge de l'API REST	Oui
Appareils SonicWall pris en charge	TZ, NSa et SuperMassive (exécutant SonicOS 6.5.4.6 ou une version ultérieure) ³ Email Security 10.X Série NSsp 15000 - En attente Série NSv (7.X ou une version ultérieure) - En attente
Types de fichiers pris en charge	.cpl .dll .drv .exe .elf .ocx .scr .sys .doc .dot .wbk .docx .docm .dotx .dotm .docb .xls .xlt .xlm .xlsx .xism .xltm .xlsm .xlsb .xla .xlam .xll .xlw .ppt .pot .pps .pptm .potx .potm .ppam .ppsx .ppsm .sldx .sldm .o .dylib .bundle .dmg .pdf .jar .apk .rar .bz2 .bzp2 .7z .xz .gz .zip
Période de conservation des données	Aucune restriction ; dépend du stockage
Stockage	2 SSD de 1 To (RAID 1)
Interfaces	6 ports 1 GbE, 2 ports 10 Go SFP+, 2 ports USB, 1 port de console
Gestion des ports dédiés	Oui (X0)
Certifications	FIPS 140-2 en instance
CARACTÉRISTIQUES DU PRODUIT	
Format	1U
Dimensions	43 x 32,5 x 4,5 cm (17,0 x 16,5 x 1,75 po)
Poids de l'appareil	8,3 kg (18,3 lb)
Accélération des données de chiffrement (AES-NI)	Oui
Temps de fonctionnement entre deux pannes (à 25 °C ou 77 °F) en heures	129 601
Alimentation	Double système d'alimentation, échangeable à chaud
Classification entrante	100 à 240 V CA, 1,79 A
Consommation électrique	114 W
Dissipation thermique totale	389 BTU
Environnement	DEEE, RoHS UE, RoHS Chine
Choc hors fonctionnement	110 g, 2 ms
Émissions	FCC, ICES, CE, C-Tick, VCCI ; MIC
Sécurité	TÜV/GS, UL, CE PSB, CCC, BSMI, schéma CB
Température de fonctionnement	0 °C à 40 °C (32 °F à 104 °F)
TPM	Oui

1. Le débit d'analyse dépend de la connectivité réseau, des types de fichiers et des niveaux de compression, et il peut varier par rapport aux valeurs publiées.

2. Bien qu'il n'y ait pas de limite stricte, le nombre d'appareils sera déterminé par le nombre de fichiers soumis par chaque appareil. La plage recommandée à la publication est d'environ 250 appareils.

3. Toutes les séries TZ, NSa et SuperMassive qui peuvent exécuter SonicOS 6.5.4.6 ou une version ultérieure. Non pris en charge sur les séries SuperMassive 9800 et NSsp 12000.

Produit	Référence
Capture Security Appliance CSA 1000	02-SSC-2853
Capture Security Appliance CSA 1000 avec mises à jour des renseignements et assistance – 1 an	02-SSC-5637
Capture Security Appliance CSA 1000 avec mises à jour des renseignements et assistance – 3 ans	02-SSC-5638
Capture Security Appliance CSA 1000 avec mises à jour des renseignements et assistance – 5 ans	02-SSC-5639

Services (Requis pour le fonctionnement de CSa 1000.

Tous les appareils envoyant des fichiers à CSa doivent disposer d'une licence Capture ATP.)

	Référence
MISES À JOUR DES RENSEIGNEMENTS, ACTIVATION ET ASSISTANCE POUR SONICWALL CSA 1000 1 AN	02-SSC-4712
MISES À JOUR DES RENSEIGNEMENTS, ACTIVATION ET ASSISTANCE POUR SONICWALL CSA 1000 2 ANS	02-SSC-4713
MISES À JOUR DES RENSEIGNEMENTS, ACTIVATION ET ASSISTANCE POUR SONICWALL CSA 1000 3 ANS	02-SSC-4714
MISES À JOUR DES RENSEIGNEMENTS, ACTIVATION ET ASSISTANCE POUR SONICWALL CSA 1000 4 ANS	02-SSC-4715
MISES À JOUR DES RENSEIGNEMENTS, ACTIVATION ET ASSISTANCE POUR SONICWALL CSA 1000 5 ANS	02-SSC-4716
MISES À JOUR DES RENSEIGNEMENTS, ACTIVATION ET ASSISTANCE POUR SONICWALL CSA 1000 6 ANS	02-SSC-4717

Activation de l'API REST (Ce service est requis uniquement pour le fonctionnement de l'API REST. Il doit être appliqué en plus des services de mise à jour des renseignements, d'activation et d'assistance.)

	Référence
ACTIVATION DE L'API REST POUR SONICWALL CAPTURE APPLIANCE CSA 1000 1 AN	02-SSC-4706
ACTIVATION DE L'API REST POUR SONICWALL CAPTURE APPLIANCE CSA 1000 2 ANS	02-SSC-4707
ACTIVATION DE L'API REST POUR SONICWALL CAPTURE APPLIANCE CSA 1000 3 ANS	02-SSC-4708
ACTIVATION DE L'API REST POUR SONICWALL CAPTURE APPLIANCE CSA 1000 4 ANS	02-SSC-4709
ACTIVATION DE L'API REST POUR SONICWALL CAPTURE APPLIANCE CSA 1000 5 ANS	02-SSC-4710
ACTIVATION DE L'API REST POUR SONICWALL CAPTURE APPLIANCE CSA 1000 6 ANS	02-SSC-4711

1. Le débit d'analyse dépend de la connectivité réseau, des types de fichiers et des niveaux de compression, et il peut varier par rapport aux valeurs publiées.

2. Bien qu'il n'y ait pas de limite stricte, le nombre d'appareils sera déterminé par le nombre de fichiers soumis par chaque appareil. La plage recommandée à la publication est d'environ 250 appareils.

3. Toutes les séries TZ, NSa et SuperMassive qui peuvent exécuter SonicOS 6.5.4.6 ou une version ultérieure. Non pris en charge sur les séries SuperMassive 9800 et NSsp 12000.

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.