SonicWall Capture Security Appliance 1000

Die SonicWall Capture Security Appliance™ (CSa) bringt Capture Advanced Threat Protection™ (ATP) und Sandbox-Malware-Analyse zu On-Premise-Implementierungen. Das ist besonders für Kunden von großem Wert, die strengen Compliance- und Richtlinienanforderungen unterliegen, bei denen das Senden von Dateien zur Analyse in die Cloud-Analyse nur begrenzt erlaubt ist oder die es vorziehen, dass alle ihre Daten innerhalb ihrer Organisation bleiben. Die CSa 1000 Appliance kann die von anderen SonicWall-Produkten als verdächtig befundenen Dateien analysieren, um eine schnelle, hochgenaue Erkennung von bisher unbekannten Bedrohungen zu ermöglichen, ohne dass der Kunde seine Dateien weiterleiten muss. Darüber hinaus werden die Vorteile dieser hocheffektiven Dateianalyse-Fähigkeiten durch die REST-API-Funktionalität der CSa auch für Threat Intelligence-Teams sowie für Drittanbieter von Sicherheitssystemen und für mit veröffentlichten APIs integrierbare Software-Stacks verfügbar gemacht.

Die CSa verwendet eine Kombination aus Reputation-basierten Prüfungen, statischer Dateianalyse und SonicWalls patentierter Real-Time Deep Memory Inspection™ (RTDMI) Engine für die Durchführung von dynamischen Analysen. Dadurch wird die bestmögliche Erkennungsrate für bösartige Dateien auf effizienteste und schnellstmögliche Weise sichergestellt. Das SonicWall-Ökosystem von Sicherheitsprodukten ist bereits vollständig in die Cloud-basierte Capture ATP-Analyse integriert und kann Inline-Sicherheit mit Funktionen wie Block Until Verdict durchsetzen.

Dieselben Funktionen werden unterstützt, wenn SonicWall-Produkte anstatt an die Cloud-basierte Capture ATP an die CSa-Serie angeschlossen werden.

RTDMI

SonicWalls zum Patent angemeldete Real-Time Deep Memory Inspection (RTDMI) Engine für die Dateianalyse ist eine neuartige Methode zur Analyse verdächtiger Dateien durch Überwachung des Verhaltens einer Anwendung im Arbeitsspeicher. RTDMI kann alle Verschleierungs- oder Verschlüsselungstechniken durchschauen, die von der neuesten Malware für das Umgehen von Netzwerk- und Sandbox-Analysen eingesetzt wird. Dadurch wird eine extrem genaue Erkennung der von Dokumenten, ausführbaren Dateien, Archivdateien und einer Vielzahl anderer Dateitypen eingeschleusten Angriffe ermöglicht.

Echtzeit-Schutz

Durch eine kombinierte Prüfung der Reputation und der globalen Bedrohungsinformationen arbeiten statische Analysen und RTDMI-Technologie effektiv zusammen, um die Resultate so schnell zu liefern, dass die in SonicWall-Produkte integrierten Technologien, wie Block Until Verdict, eingreifen können. Diese Fähigkeit ermöglicht die Einrichtung einer Dateiinspektionsregel in der Firewall, die ein Herunterladen verdächtiger Dateien durch den Endbenutzer verhindert, bis die die Inspektion vollständig abgeschlossen ist und Capture ATP oder CSa ein Urteil gefällt hat.

Vorteile:

- Arbeitsspeicherbasierte Inspektion mit RTDMI
- Mehrstufige Analyse mit Reputationsprüfung, statischer Analyse und dynamischer Analyse
- API-Zugriff für die Bedrohungsanalyse
- Unterstützung eines weiten Bereichs von Dateitypen
- Unterstützung für Block Until Verdict
- Höchste Sicherheit und Effektivität
- Reporting und rollenbasierter Zugriff

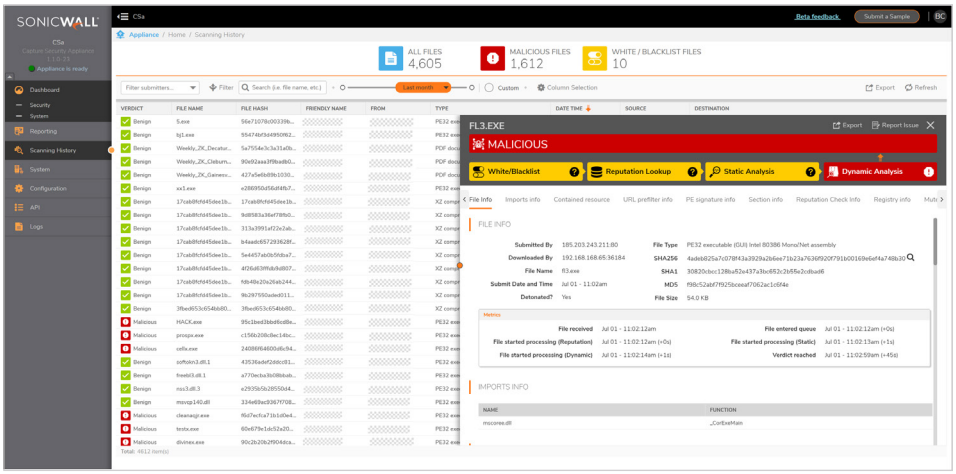
1. *Der Analysedurchsatz ist abhängig von Netzwerkkonnektivität, Dateitypen, Komprimierungsstufen und eventuell von veröffentlichten Zahlen.*
2. *Zwar gibt es keine feste Grenze, doch die Anzahl der Geräte wird durch die Anzahl der von jedem Gerät eingereichten Dateien bestimmt. Die empfohlene Reichweite bei der Veröffentlichung liegt bei etwa 250 Geräten.*
3. *Alle Appliances der TZ Series, NSa Series und SuperMassive Series, die SonicOS 6.5.4.6 oder höher ausführen können. Nicht unterstützt auf SuperMassive 9800 und NSsp 12000 Series.*

Bewährt und vertraut

- Die CSa bringt die Technologie von SonicWalls Cloud-basiertem Capture ATP Service, dem über 150.000 Kunden weltweit vertrauen, in einem Appliance-Formfaktor unter
- Durch regelmäßig aktualisierte Informationen wird die CSa mit den durch die SonicWall Capture ATP-Dateianalyse weltweit erfassten Threat-Intellicence-Daten synchronisiert

Reporting, Analyse und Verwaltung

- Über ein leicht zu navigierendes Dashboard und eine Dateianalyse-Historie bietet die CSa Appliance Einblick in die von allen Quellen eingereichten Dateien und zeigt auch die Häufigkeit, Ursprünge, Urteile und andere Erkenntnisse zu den für die Analyse eingereichten Dateien
- Reporting-Fähigkeiten liefern einen globalen Einblick in den ATP-Schutz der gesamten Organisation und bieten die Möglichkeit zur Planung regelmäßiger Berichte, die auf Basis verschiedener Rollen konfiguriert werden können
- Administratoren können verschiedenen Rollen granularen Zugang zur CSa 1000 gewähren und den Zugriff auf einen bestimmten Bereich der Benutzeroberfläche beschränken
- Sicherheitsexperten können Zugang zur Scanninghistorie erhalten sowie die Fähigkeit zum Ändern von Whitelists/Blacklists, zugelassenen Geräten und Melden von vermutlich falsch-positiven oder falsch-negativen Ergebnissen
- Netzwerk-Administratoren können Zugriff auf die betriebliche Konfiguration der Appliance erhalten, während sie aus Vertraulichkeitsgründen am Einsehen der eingereichten Dateien und ihres Ursprungs gehindert werden können



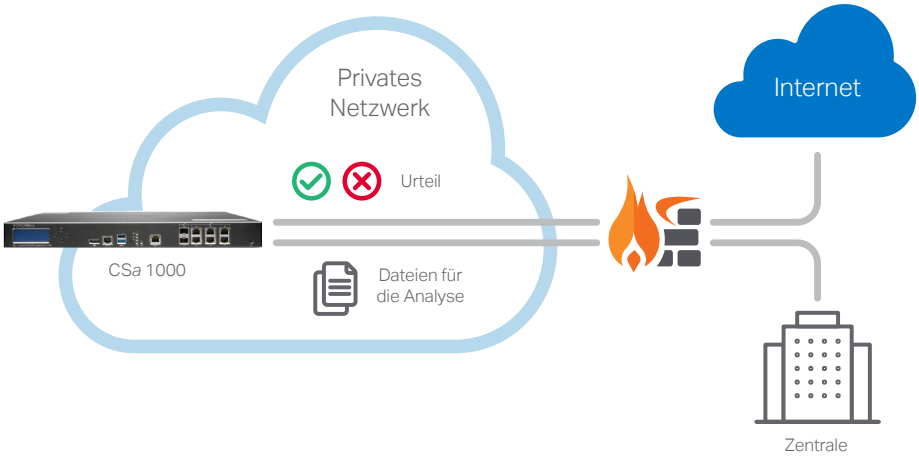
Funktionen

- Reputation- und Global-Verdict-Lookup (konfigurierbar)
- Statische Analyse und dynamische Analyse mit RTDMI
- Whitelist/Blacklist auf Hash/Domain
- Konfigurierbares terminiertes Reporting
- Rollenbasierte Administration (konfigurierbare Rollen)
- Management – HTTPS oder SSH über dedizierte Management-Schnittstelle oder reguläre Netzwerkschnittstelle
- Zugang zur SSH-Konsole
- Protokollierung und Alarmierung
- Reporting von falsch-positiven und falsch-negativen Ergebnissen mit automatischem Whitelisting/Blacklisting
- Direkte Verbindung oder über VPN (IP-adressierbar)
- Geschlossener Netzwerkbetrieb
- REST API-Unterstützung für die Einreichung und Analyse von Dateien
- Gehärtetes Betriebssystem mit Secure Boot und Chain-of-Trust zum Verhindern von unberechtigter Manipulation
- Lokale Protokollierung

1. *Der Analysedurchsatz ist abhängig von Netzwerkkonnektivität, Dateitypen, Komprimierungsstufen und eventuell von veröffentlichten Zahlen.*
2. *Zwar gibt es keine feste Grenze, doch die Anzahl der Geräte wird durch die Anzahl der von jedem Gerät eingereichten Dateien bestimmt. Die empfohlene Reichweite bei der Veröffentlichung liegt bei etwa 250 Geräten.*
3. *Alle Appliances der TZ Series, NSa Series und SuperMassive Series, die SonicOS 6.5.4.6 oder höher ausführen können. Nicht unterstützt auf SuperMassive 9800 und NSsp 12000 Series.*

Einbindungsoptionen

- Die Implementierung von SonicWall CSa ist schnell und unkompliziert. Sie erfordert lediglich die Konfiguration der Networking-, Reporting- und Gerätezugriffsanforderungen
- Die CSa ist IP-adressierbar und kann daher überall dort eingebunden werden, wo sie von Geräten erreichbar ist, die Dateien zur Analyse einreichen



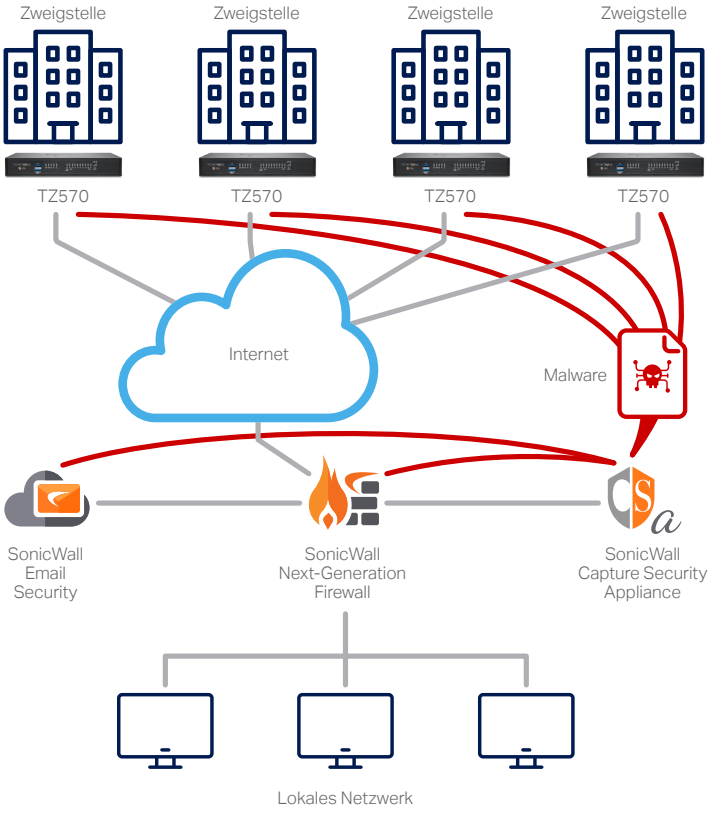
Es gibt drei primäre Implementierungsmethoden für die CSa 1000:

Einzelbüro/Einzelstandort

- Die CSa Appliance kann an jeder Stelle im Netzwerk eingebunden werden, an der sie von den bedienten Produkten über das IP erreicht werden kann[1]
- Nach Implementierung der CSa können die Firewalls und E-Mail-Sicherheitssysteme (weitere noch ausstehende Lösungen) so konfiguriert werden, dass verdächtige Dateien zur ATP-Analyse an die CSa anstatt an die Cloud weitergeleitet werden

Verteilte Unternehmen/Mehrere Zweigstellen

- Mehrere Niederlassungen/Zweigstellen können so konfiguriert werden, dass der Zugriff auf eine CSa Appliance entweder zentral im Rechenzentrum des Hauptsitzes oder in einem von allen Geräten erreichbaren dezentralen Rechenzentrum implementiert wird
- Der Zugriff kann direkt über das Internet oder per VPN erfolgen
- Eine Massenkonfiguration von SonicWall-Systemen, die auf das CSa ausgerichtet sind, kann entweder mittels GMS oder den Cloud-basierten zentralisierten NSM-Managementlösungen erfolgen, um eine schnelle Konfiguration und Implementierung zu ermöglichen



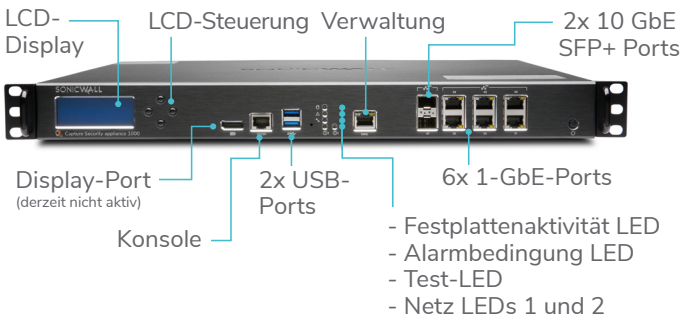
REST API Gateway

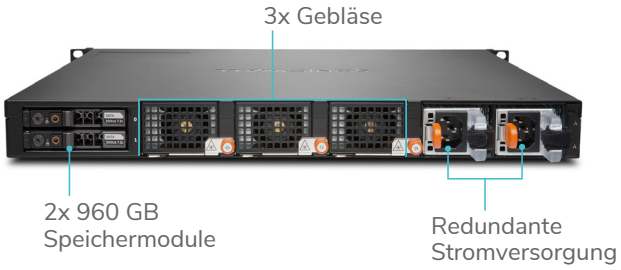
- Die CSa Series verfügt über eine REST API-Schnittstelle, über die Dateien für Analyse- und Abfrageergebnisse von Threat-Intelligence-Teams über eigene Scripts, Web-Portal-Integrationen und andere Sicherheitsprodukte eingereicht werden können
- Anleitungen zum Einstieg in das API-Scripting für die CSa und Codebeispiele finden Sie unter https://github.com/sonicwall

* [1]*SonicWall Firewalls benötigen auch Zugriff über UDP auf Port 2259*

1. *Der Analysedurchsatz ist abhängig von Netzwerkkonnektivität, Dateitypen, Komprimierungsstufen und eventuell von veröffentlichten Zahlen.*
2. *Zwar gibt es keine feste Grenze, doch die Anzahl der Geräte wird durch die Anzahl der von jedem Gerät eingereichten Dateien bestimmt. Die empfohlene Reichweite bei der Veröffentlichung liegt bei etwa 250 Geräten.*
3. *Alle Appliances der TZ Series, NSa Series und SuperMassive Series, die SonicOS 6.5.4.6 oder höher ausführen können. Nicht unterstützt auf SuperMassive 9800 und NSsp 12000 Series.*

CSa 1000





Technische Daten zur SonicWall CSa

FUNKTIONEN	
Durchsatz für Reputation- und Global-Threat-Lookup (Dateien pro Stunde)[1]	12.000
Durchsatz für Real World File Mix (Dateien pro Stunde)[1]	2500
Durchsatz für die dynamische Analyse (RTDMI) (Dateien pro Stunde)[1]	300
Maximale Dateigröße	100 MB
Maximal unterstützte Geräte[2]	Basierend auf der Leistung
Maximale Archiv-Scantiefe	3
REST API-Unterstützung	Ja
Unterstützte SonicWall Appliances	TZ, NSa und SuperMassive (mit SonicOS 6.5.4.6 und höher)[3] E-Mail Security 10.X NSsp 15000 Series - noch ausstehend NSv-Serie (7.X und höher) - noch ausstehend
Unterstützte Dateitypen	.cpl .dll .drv .exe .elf .ocx .scr .sys .doc .dot .wbk .docx .docm .dotx .dotm .docb .xls .xlt .xlm .xlsx .xlsm .xltx .xltm .xlsb .xla .xlam .xll .xlw .ppt .pot .pps .pptx .pptm .potx .potm .ppam .ppsx .ppsm .sldx .sldm .o .dylib .bundle .dmg .pdf .jar .apk .rar .bz2 .bzip2 .7z .xz .gz .zip
Aufbewahrungsfrist für Daten	Unbegrenzt, speicherplatzabhängig
Speicher	2 x 1TB SSD (RAID 1)
Schnittstellen	(6)-Port 1GE, (2)-Port 10Gb SFP+, (2) USB, (1) Konsole
Dediziertes Port-Management	Ja (X0)
Zertifizierungen	FIPS 140-2 ausstehend
PRODUKTMERKMALE	
Formfaktor	1U
Abmessungen	43 x 41,5 x 4,5 cm
Appliance-Gewicht	8,3 kg
Beschleunigung von Verschlüsselungsdaten (AES-NI)	Ja
MTBF (bei 25 °C) in Stunden	129.601
Stromversorgung	Duale Stromversorgung, hot-swappable
Eingangsnennwerte	100–240 V AC, 1,79 A
Leistungsaufnahme	114 W
Gesamtwärmeabgabe	389 BTU
Umweltvorschriften	WEEE, EU RoHS, China RoHS
Erschütterungen (außer Betrieb)	110 g, 2 ms
Emissionen	FCC, ICES, CE, C-Tick, VCCI; MIC
Sicherheit	TÜV/GS, UL, CE PSB, CCC, BSMI, CB Scheme
Betriebstemperatur	0 °C bis 40 °C
TPM	Ja

1. *Der Analysedurchsatz ist abhängig von Netzwerkkonnektivität, Dateitypen, Komprimierungsstufen und eventuell von veröffentlichten Zahlen.*
2. *Zwar gibt es keine feste Grenze, doch die Anzahl der Geräte wird durch die Anzahl der von jedem Gerät eingereichten Dateien bestimmt. Die empfohlene Reichweite bei der Veröffentlichung liegt bei etwa 250 Geräten.*
3. *Alle Appliances der TZ Series, NSa Series und SuperMassive Series, die SonicOS 6.5.4.6 oder höher ausführen können. Nicht unterstützt auf SuperMassive 9800 und NSsp 12000 Series.*

Produkt	Artikelnummer
Capture Security Appliance CSA 1000	02-SSC-2853
Capture Security Appliance CSA 1000 mit Intelligence Updates und Support-Bündel – 1 Jahr	02-SSC-5637
Capture Security Appliance CSA 1000 mit Intelligence Updates und Support-Bündel – 3 Jahre	02-SSC-5638
Capture Security Appliance CSA 1000 mit Intelligence Updates und Support-Bündel – 5 Jahre	02-SSC-5639

Services (Erforderlich für den CSa 1000-Betrieb. Alle Geräte, die Dateien an die CSa senden, müssen eine Capture ATP-Lizenz haben)	Artikelnummer
INTELLIGENCE UPDATES, AKTIVIERUNG UND UNTERSTÜTZUNG FÜR SONICWALL CSA 1000 1 JAHR	02-SSC-4712
INTELLIGENCE UPDATES, AKTIVIERUNG UND UNTERSTÜTZUNG FÜR SONICWALL CSA 1000 2 JAHRE	02-SSC-4713
INTELLIGENCE UPDATES, AKTIVIERUNG UND UNTERSTÜTZUNG FÜR SONICWALL CSA 1000 3 JAHRE	02-SSC-4714
INTELLIGENCE UPDATES, AKTIVIERUNG UND UNTERSTÜTZUNG FÜR SONICWALL CSA 1000 4 JAHRE	02-SSC-4715
INTELLIGENCE UPDATES, AKTIVIERUNG UND UNTERSTÜTZUNG FÜR SONICWALL CSA 1000 5 JAHRE	02-SSC-4716
INTELLIGENCE UPDATES, AKTIVIERUNG UND UNTERSTÜTZUNG FÜR SONICWALL CSA 1000 6 JAHRE	02-SSC-4717

REST API Aktivierung (Dieser Service ist nur für den REST API Betrieb erforderlich. Muss zusätzlich zum Service für Intelligence Update, Aktivierung und Unterstützung angewendet werden)	Artikelnummer
REST API AKTIVIERUNG FÜR SONICWALL CAPTURE APPLIANCE CSA 1000 1 JAHR	02-SSC-4706
REST API AKTIVIERUNG FÜR SONICWALL CAPTURE APPLIANCE CSA 1000 2 JAHRE	02-SSC-4707
REST API AKTIVIERUNG FÜR SONICWALL CAPTURE APPLIANCE CSA 1000 3 JAHRE	02-SSC-4708
REST API AKTIVIERUNG FÜR SONICWALL CAPTURE APPLIANCE CSA 1000 4 JAHRE	02-SSC-4709
REST API AKTIVIERUNG FÜR SONICWALL CAPTURE APPLIANCE CSA 1000 5 JAHRE	02-SSC-4710
REST API AKTIVIERUNG FÜR SONICWALL CAPTURE APPLIANCE CSA 1000 6 JAHRE	02-SSC-4711

1. *Der Analysedurchsatz ist abhängig von Netzwerkkonnektivität, Dateitypen, Komprimierungsstufen und eventuell von veröffentlichten Zahlen.*
2. *Zwar gibt es keine feste Grenze, doch die Anzahl der Geräte wird durch die Anzahl der von jedem Gerät eingereichten Dateien bestimmt. Die empfohlene Reichweite bei der Veröffentlichung liegt bei etwa 250 Geräten.*
3. *Alle Appliances der TZ Series, NSa Series und SuperMassive Series, die SonicOS 6.5.4.6 oder höher ausführen können. Nicht unterstützt auf SuperMassive 9800 und NSsp 12000 Series.*

Über SonicWall

SonicWall bietet Boundless Cybersecurity für das hyperverteilte Umfeld einer neuen Arbeitsrealität, in der jeder remote, mobil und ungeschützt ist. Indem SonicWall das Unbekannte kennt, Echtzeit-Transparenz und skalierbare Ökonomien ermöglicht, werden Cybersicherheitslücken bei Unternehmen, Regierungen und KMU weltweit geschlossen. Weitere Informationen finden Sie auf www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com

Datasheet-CSa-US-COG-2099