SONICWALL

SonicWall Capture Security appliance 1000

The SonicWall Capture Security appliance™ (CSa) brings Capture Advanced Threat Protection™ (ATP) and sandboxing malware analysis to on-premises deployment scenarios for customers with compliance and policy restrictions against sending files to cloud analysis, or who prefer for all of their data to remain inside their organization. The CSa 1000 can analyze suspicious files coming from other SonicWall products to provide rapid, high accuracy detection of previously unseen threats with the customer retaining custody of their files. Additionally, the REST API functionality on the CSa opens up the benefits of this highly effective file analysis capability to threat intelligence teams, third-party security systems and any software stack that can integrate with published APIs.

The CSa uses a combination of reputation-based checks, static file analysis and SonicWall's patented Real-Time Deep Memory Inspection™ (RTDMI) engine for dynamic analysis to ensure that it provides not only the best possible detection rate of malicious files, but also does this efficiently, in the shortest possible time. The SonicWall ecosystem of security products, already fully integrated with the cloud-delivered Capture ATP analysis, is able to enforce inline security with features such as Block Until Verdict.

The same capabilities are supported when the SonicWall products are connected to the CSa series instead of the cloud Capture ATP.

RTDMI

SonicWall's patent-pending Real-Time Deep Memory Inspection (RTDMI) file analysis engine is a novel method of analyzing suspicious files by monitoring the behavior of an application in memory. RTDMI can see through any obfuscation or encryption techniques that modern malware may deploy to evade network and sandbox analysis, yielding extremely high accuracy detection of attacks borne by documents, executables, archive files and a variety of other file types.

Real time protection

The combination of reputation and global intelligence checks, statics analysis and RTDMI technology operate in concert to deliver results quickly enough to enable technologies like Block Until Verdict in SonicWall products. This capability allows for a file inspection policy on the firewall to prevent suspicious files from being downloaded by the end-user until the full inspection is completed and a verdict is reached by Capture ATP or CSa.

Benefits:

- Memory-based inspection with RTDMI
- Multi-Stage analysis with reputation check, static analysis and dynamic analysis
- API Access for threat analysis
- Broad file type support
- Block until verdict support
- High-security effectiveness
- Reporting and Role-Based Access

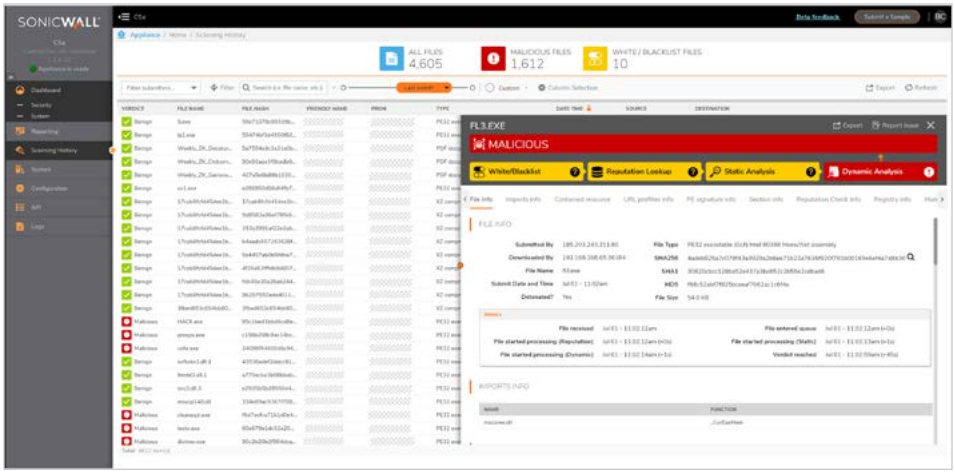
1. *Analysis throughput dependent on network connectivity, file types, compression levels and may vary from published figures.*
2. *While there is no hard limit, number of devices is going to be determined by the number of files submitted by each device. Recommended range at the of publication is around 250 devices*
3. *All TZ series, NSa series and SuperMassive series that can run SonicOS 6.5.4.6 or later. Not supported on SuperMassive 9800 and NSsp 12000 Series.*

Trusted by and benefits from the experience of many

- CSa combines the technology from SonicWall's Capture ATP, a cloud-based service trusted and used by over 150,000 customers across the globe, into an appliance form factor
- CSa also gets regular intelligence updates to synchronize with the threat intelligence gathered globally via SonicWall Capture ATP file analysis

Reporting, Analysis and Administration

- CSa provides an insight into files submitted from all sources with an easy to navigate dashboard and file analysis history, providing an insight into the frequency, sources, verdicts and other insights around files submitted for analysis
- Reporting capabilities provide a global view into the ATP protection across the organization, with ability to schedule regular reports configured based on different roles
- Administrators can grant granular access to the CSa 1000 to a variety of roles with the ability to restrict access to any part of the UI
- Security analysts can have access to the scanning history with ability to modify the whitelist/blacklist, allowed devices and report any suspected false positives or false negatives
- Network-level administrators can be granted access to the operational configuration of the appliance while being restricted, for confidentiality reasons, from seeing the submitted files and their sources



Features

- Reputation & Global Verdict lookup (configurable)
- Static analysis & dynamic analysis with RTDMI
- Whitelist/Blacklist on hash/domain
- Configurable scheduled reporting
- Role-based administration (configurable roles)
- Management – HTTPS or SSH via dedicated management interface or regular network interface
- SSH console access.
- Logging & alerting
- False positive & false negative reporting with automatic whitelist/blacklist
- Direct connectivity or via VPN (IP Addressable)
- Closed Network Operation
- REST API support for file submission and analysis
- Hardened OS with Secure Boot and chain of trust for anti-tampering
- Local logging

1. Analysis throughput dependent on network connectivity, file types, compression levels and may vary from published figures.
2. While there is no hard limit, number of devices is going to be determined by the number of files submitted by each device. Recommended range at the of publication is around 250 devices
3. All TZ series, NSa series and SuperMassive series that can run SonicOS 6.5.4.6 or later. Not supported on SuperMassive 9800 and NSsp 12000 Series.

Deployment Options

- SonicWall CSa deployment is quick and straightforward, requiring configuration of basic networking, reporting and allowed device access to get started
- The CSa is built to be IP-addressable and can therefore be deployed anywhere as long as its reachable by devices that will submit files for analysis

There are three primary deployment methods for the CSa 1000:

Single Office/Single Location

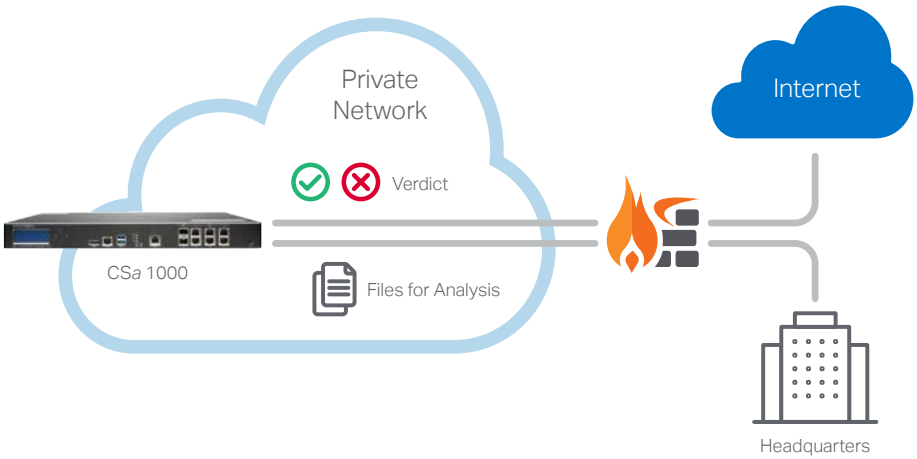
- The CSa can be deployed anywhere on the network as long as the products that will use it can reach it via an IP[1]
- Once the CSa is deployed, the Firewalls and Email Security systems (other solutions pending) can be configured to redirect suspicious files to the CSa rather than the cloud for ATP analysis

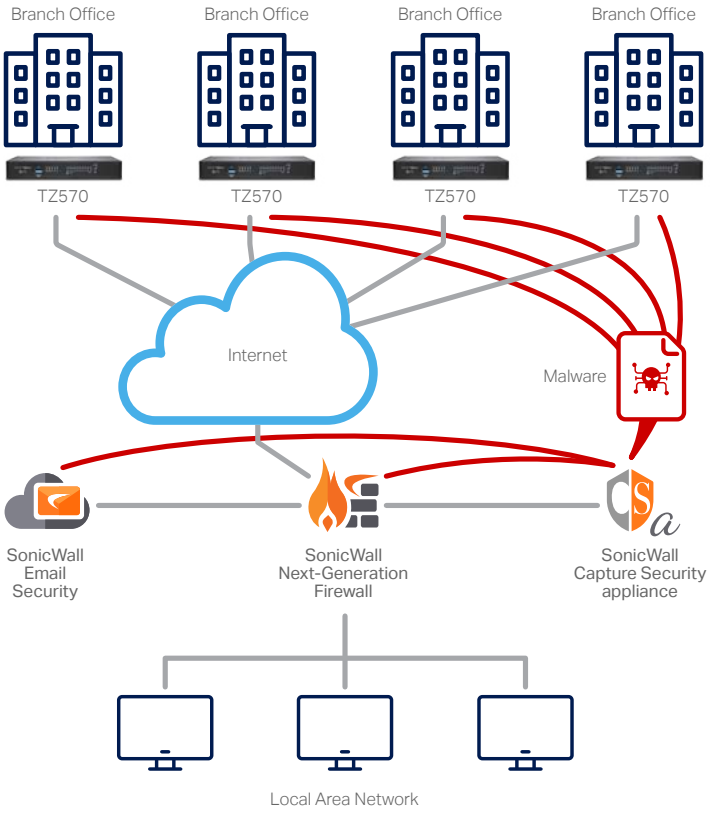
Distributed Enterprise/Multiple-Locations

- Multiple offices/branches can be configured to share access to a single CSa device, deployed either in the central HQ data center or in a remote datacenter reachable by all devices
- Access can be direct over the internet or via VPN
- Mass configuration of SonicWall systems to point to the CSa can be done with either GMS or the cloud-based NSM centralized management solutions for rapid configuration and deployment

REST API Gateway

- The CSa series have a REST API interface that can be used to submit files for analysis and query results by threat intelligence teams via their own scripts, web-portal integrations and other security products
- Instructions on how to get started with API scripting for the CSa and code samples are available at https://github.com/sonicwall

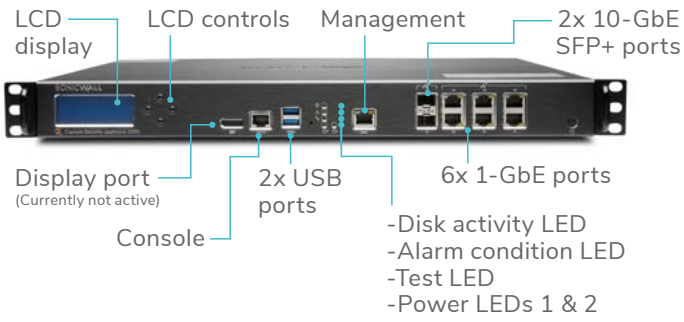


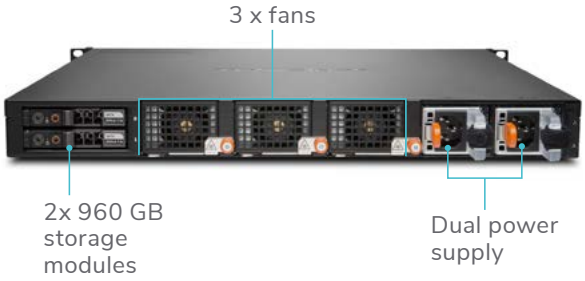


* [1]SonicWall firewalls also require access via UDP on port 2259

1. Analysis throughput dependent on network connectivity, file types, compression levels and may vary from published figures.
2. While there is no hard limit, number of devices is going to be determined by the number of files submitted by each device. Recommended range at the of publication is around 250 devices
3. All TZ series, NSa series and SuperMassive series that can run SonicOS 6.5.4.6 or later. Not supported on SuperMassive 9800 and NSsp 12000 Series.

CSa 1000





SonicWall CSa 1000 specifications

FEATURES	
Reputation & Global Threat Lookup Throughput (Files per hour)[1]	12,000
Real-World File Mix Throughput (Files per hour)[1]	2500
Dynamic Analysis (RTDMI) Throughput (Files per Hour)[1]	300
Max File Size	100 MB
Max Devices Supported[2]	Based on Performance
Maximum Archive Scan Depth	3
REST API Support	Yes
SonicWall devices supported	TZ, NSa & SuperMassive (running SonicOS 6.5.4.6 and above)[3] Email Security 10.X NSsp 15000 Series - Pending NSv Series (7.X and Above) - Pending
File types supported	.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
Data Retention Period	Unrestricted, limited by storage
Storage	2 x 1TB SSD (RAID 1)
Interfaces	(6)-port 1GE, (2)-port 10Gb SFP+, (2) USB, (1) console
Dedicated Port Management	Yes (X0)
Certifications	FIPS 140-2 Pending
PRODUCT CHARACTERISTICS	
Form factor	1U
Dimensions	17.0 x 16.5 x 1.75 in (43 x 41.5x 4.5 cm)
Appliance Weight	18.3 lbs (8.3 kgs)
Encryption data acceleration (AES-NI)	Yes
MTBF (@ 25°C or 77°F) in hours	129,601
Power	Dual power supply, hot swappable
Input rating	100-240 VAC, 1.79 A
Power consumption	114 W
Total heat dissipation	389 BTU
Environmental	WEEE, EU RoHS, China RoHS
Non-operating shock	110 g, 2 msec
Emissions	FCC, ICES, CE, C-Tick, VCCI; MIC
Safety	TUV/GS, UL, CE PSB, CCC, BSMI, CB scheme
Operating Temperature	0°C to 40°C (32°F to 104° F)
TPM	Yes

1. Analysis throughput dependent on network connectivity, file types, compression levels and may vary from published figures.
2. While there is no hard limit, number of devices is going to be determined by the number of files submitted by each device. Recommended range at the of publication is around 250 devices
3. All TZ series, NSa series and SuperMassive series that can run SonicOS 6.5.4.6 or later. Not supported on SuperMassive 9800 and NSsp 12000 Series.

Product	SKU
Capture Security Appliance CSA 1000	02-SSC-2853
Capture Security Appliance CSA 1000 with Intelligence Updates and Support Bundle – 1 Year	02-SSC-5637
Capture Security Appliance CSA 1000 with Intelligence Updates and Support Bundle – 3 Years	02-SSC-5638
Capture Security Appliance CSA 1000 with Intelligence Updates and Support Bundle – 5 Years	02-SSC-5639

Services (Required for CSa 1000 operation. All devices sending files to CSa must have Capture ATP licensed)	SKU
INTELLIGENCE UPDATES, ACTIVATION AND SUPPORT FOR SONICWALL CSA 1000 1YR	02-SSC-4712
INTELLIGENCE UPDATES, ACTIVATION AND SUPPORT FOR SONICWALL CSA 1000 2YR	02-SSC-4713
INTELLIGENCE UPDATES, ACTIVATION AND SUPPORT FOR SONICWALL CSA 1000 3YR	02-SSC-4714
INTELLIGENCE UPDATES, ACTIVATION AND SUPPORT FOR SONICWALL CSA 1000 4YR	02-SSC-4715
INTELLIGENCE UPDATES, ACTIVATION AND SUPPORT FOR SONICWALL CSA 1000 5YR	02-SSC-4716
INTELLIGENCE UPDATES, ACTIVATION AND SUPPORT FOR SONICWALL CSA 1000 6YR	02-SSC-4717

REST API Activation (This service is required only for REST API operation. It must be applied on top of the Intelligence Update, Activation and Support service)	SKU
REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 1YR	02-SSC-4706
REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 2YR	02-SSC-4707
REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 3YR	02-SSC-4708
REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 4YR	02-SSC-4709
REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 5YR	02-SSC-4710
REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 6YR	02-SSC-4711

1. Analysis throughput dependent on network connectivity, file types, compression levels and may vary from published figures.
2. While there is no hard limit, number of devices is going to be determined by the number of files submitted by each device. Recommended range at the of publication is around 250 devices
3. All TZ series, NSa series and SuperMassive series that can run SonicOS 6.5.4.6 or later. Not supported on SuperMassive 9800 and NSsp 12000 Series.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

Datasheet-CSa-US-COG-2099