

Capture Security appliance 1000

Fast and accurate on-premise, memory-based file analysis and malware detection

SonicWall Capture Security appliance™ (CSa) brings Capture Advanced Threat Protection™ (ATP) and sandboxing malware analysis to on-premise deployment scenarios. This offers 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, an ability to take advantage of the superior threat detection capabilities formerly offered only in the cloud.

HIGHLIGHTS

- Memory-based inspection with RTDMI
- Multi-Stage Analysis with reputation check, static analysis and dynamic analysis
- Management and File submission API
- Broad file type support
- Block Until Verdict support
- High security effectiveness
- Reporting and Role-Based Access
- Closed Network Support



SonicWall CSa Spec Preview. [View full specs »](#)

12,000 Files/Hr	2,500 Files/Hr	300 Files/Hr	100 MB	YES
Global Threat Lookup	Real-World File Mix Throughput	Dynamic Analysis Throughput	Max File Size	Closed Network Support

Find the right SonicWall solution for
your enterprise:

sonicwall.com/products

Equipped with Real-Time Deep Memory Inspection (RTDMI), CSa can detect and stop attacks using a wide range of file types by forcing malware to reveal its weaponry into memory.

The SonicWall Capture Security appliance™ (CSa) brings Capture Advanced Threat Protection™ (ATP) and sandboxing malware analysis to on-premise deployment scenarios. This offers 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, an ability to take advantage of the superior threat detection capabilities formerly offered only in the cloud. 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.

CSa analyzes a broad range of file types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, and multi-browser environments.

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. This ensures 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 patented 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 reputation and global intelligence checks, static analysis, and RTDMI technology operate in concert to deliver results quickly enough to enable technologies like Block Until Verdict in SonicWall products. This capability enables a file inspection policy on the firewall that prevents end users from downloading suspicious files until a full inspection is completed and a verdict is reached by Capture ATP or CSa. With Closed Network support enabled, cloud-based reputation and intelligence checks are disabled.



Directory scan

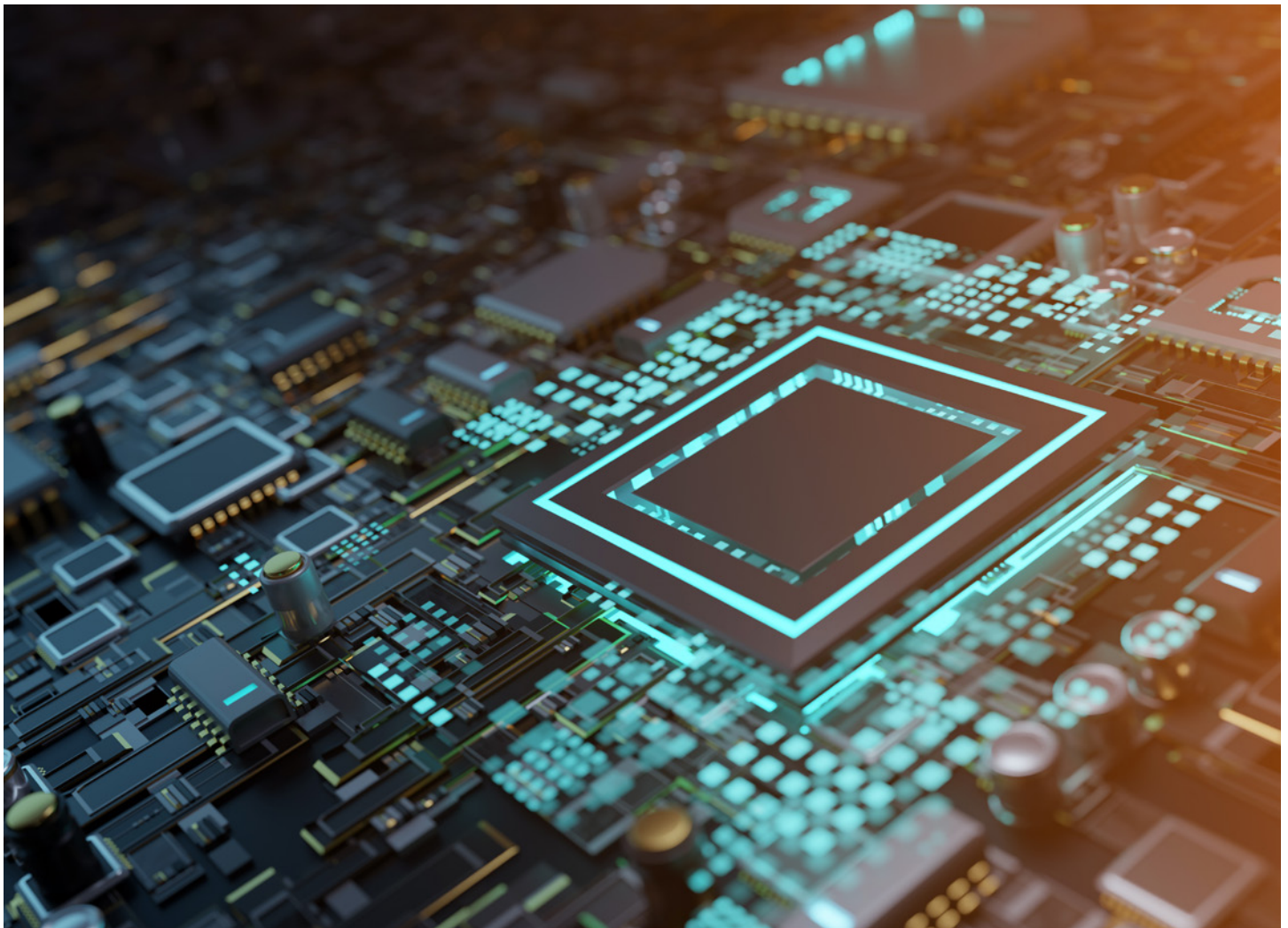
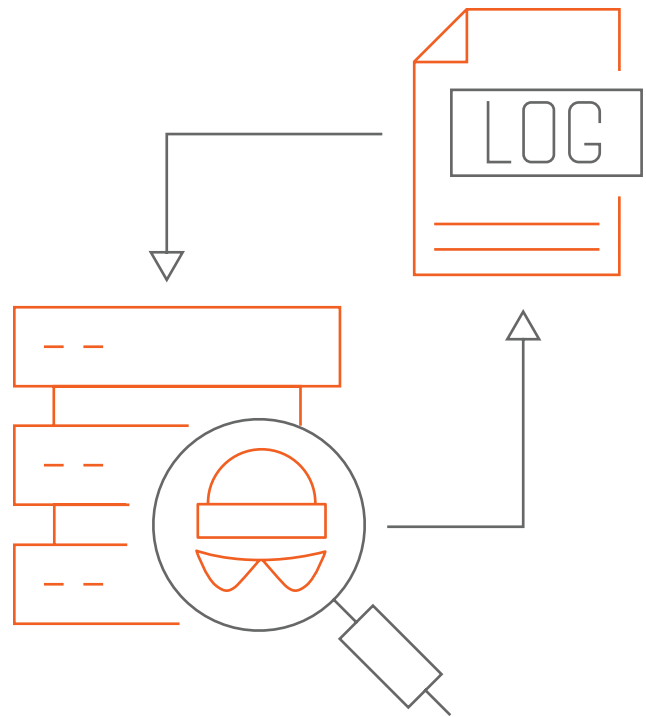
Directory Scan extends the threat analysis capability of CSa to file shares on-premise and in the cloud, supporting AzureFS, AWS S3, and SMBv3.

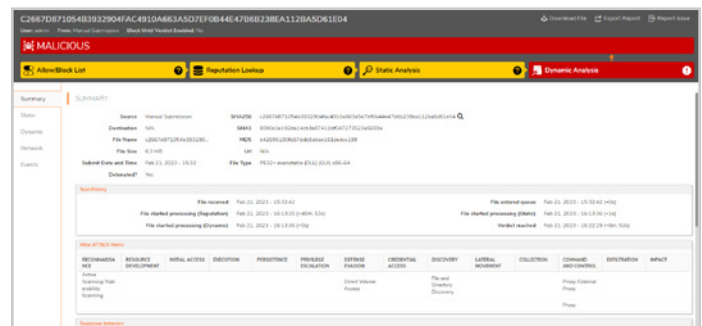
Deep reporting

Deep reporting enhances file analysis that is currently done in the sandbox in order to provide additional visibility - such as file information, scan history, suspicious behaviors, and mapping to the MITRE Attack Matrix - to the SOC administrator. The static analysis of files includes PE signatures, URL pre-filter information, and file version information.

Active/Passive High Availability support

Active/Passive High Availability support allows the administrator to add two CSa units in Active and Passive mode so the firewall will default to the standby mode if the active CSa fails for any reason.





DEPLOYMENT OPTIONS

- SonicWall CSa deployment is quick and straightforward, requiring only 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 it's reachable by devices that will submit files for analysis. The CSa can also be deployed in closed or air-gapped networks.

There are three primary deployment methods for the CSa 1000:

Single Office/Single Location

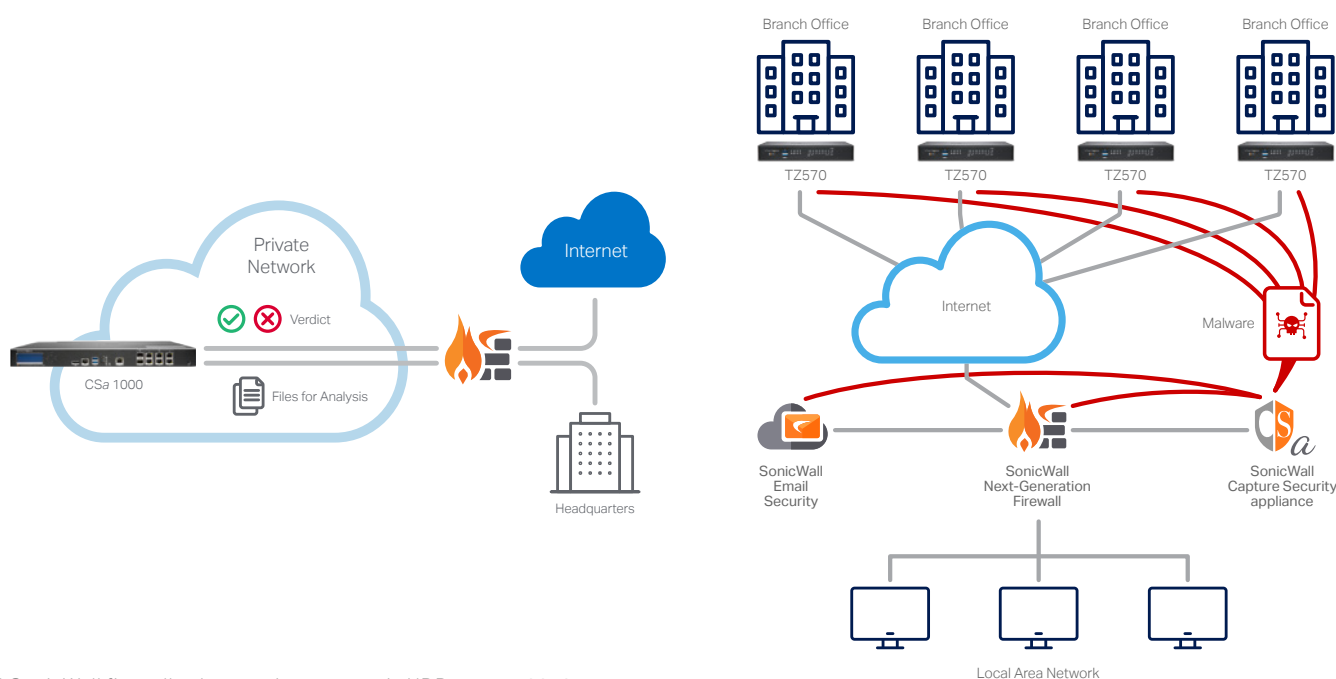
- The CSa can be deployed anywhere on the network as long as the submission sources that will use it can reach it via an IP*.
- Once the CSa is deployed, the firewalls and email security systems (other solutions pending) can be configured to redirect suspicious files to the CSa rather than the cloud 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.

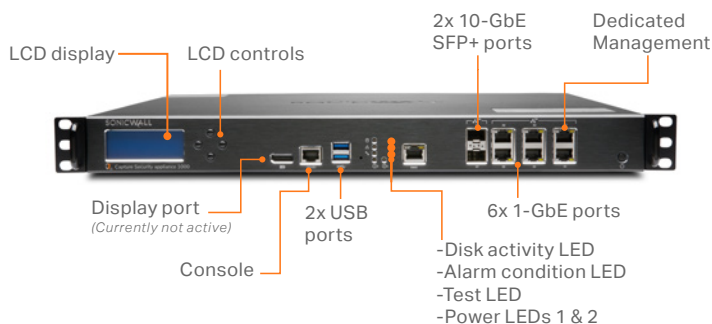
REST API Gateway

- The CSa series has 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.
- Code samples and instructions on how to get started with API scripting for the CSa are available at <https://github.com/sonicwall>.



* SonicWall firewalls also require access via UDP on port 2259

Capture Security appliance 1000



Features

CSa 1000

Reputation & Global Threat Lookup Throughput (Files per hour) ¹	12,000
Real-World File Mix Throughput (Files per hour) ¹	2,500
Dynamic Analysis (RTDMI) Throughput (Files per Hour) ¹	300
Max File Size	100 MB
Maximum Archive Scan Depth	3
REST API Support	Management and File Analysis
SonicWall devices supported	TZ, NSa & SuperMassive (running SonicOS 6.5.4.6/7.0.1 and above) ² Email Security 10.X NSsp 15700 Series NSv Series (7.X and Above)
File types supported	.cpl .dll .drv .exe .elf .ocx .scr .sys .doc .dot .wbk .docx .docm .dotx .dotm .docb .xls .xlt .xlm .xlsx .xslm .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
VMs Supported	Windows 7 32/64, Linux 64
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, ICSA

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 and compression levels and may vary from published figures.

2. 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.



PARTNER ENABLED SERVICES

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at:

www.sonicwall.com/PES

Leverage the power of Real-Time Deep Memory Inspection (RTDMI) in your environment, visit:

www.sonicwall.com/products/capture-security-appliance

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

SONICWALL®

© 2023 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non-infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profits, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.