

SonicWall Capture Client

Stop Breaches Faster Than Humanly Possible...Autonomously

The ever-growing threat of ransomware and other malicious malware-based attacks has proven that client protection solutions cannot be measured based only on endpoint compliance. Traditional antivirus technology uses a long-embattled signature-based approach, which has failed to match the pace of emerging malware and evasion techniques.

Additionally, with the proliferation of telecommuting, mobility and BYOD, there is a dire need to deliver consistent protection, application vulnerability intelligence, and web policy enforcement and more for endpoints anywhere. SonicWall Capture Client is a unified endpoint offering with multiple EPP and EDR capabilities.

HIGHLIGHTS

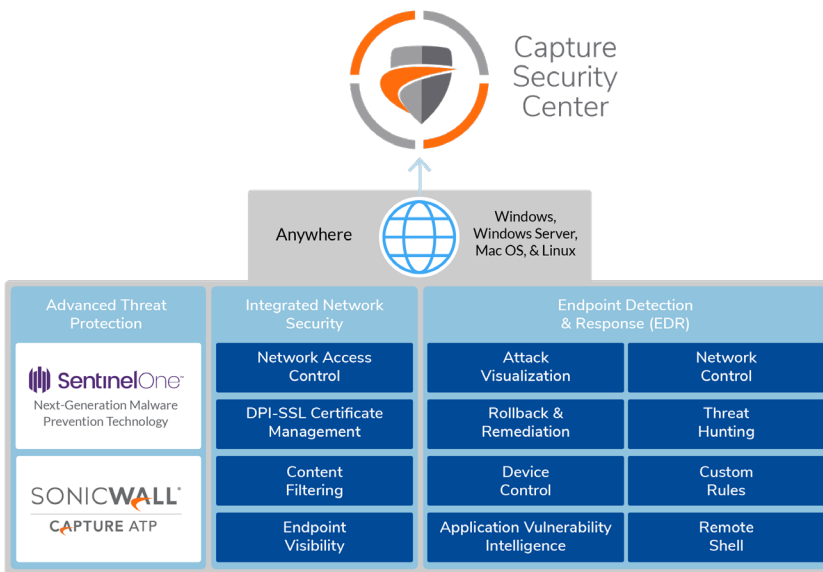
- Get high efficacy, actionable threat detection without the noise
- Centralized and cloud-delivered management with true multi-tenant capabilities to fortify network and endpoint security
- Empower and up-level security and IT teams with an easy-to-use, intuitive solution that stops modern adversaries

**Fitting Endpoint Security to
Your Organization**

[Read the Brief: sonicwall.com](https://sonicwall.com)



SonicWall Capture Client



Capture Client applies behavior-based advanced threat protection, powered by NGAV SentinelOne.

Capture ATP Integration for higher security effectiveness, faster response times and a lower total cost of ownership.

Features and Benefits

Continuous behavioral monitoring

- See complete profiles of file, application, process, and network activity
- Protect against both file-based and fileless malware
- Deliver a 360-degree attack view with actionable intelligence

Threat Hunting with Deep Visibility

- Utilize Deep Visibility to search for threats based on behavior indicators as well as Indicators of Compromise (IOC) across covered Windows, MacOS, and Linux devices
- Automate Threat Hunting and Response with Custom Rules and Alerts

Capture Advanced Threat Protection (ATP) integration

- Automatically upload suspicious files on Windows devices for advanced sandboxing analysis
- Find dormant threats before execution such as malware with built-in timing delays
- Reference Capture ATP's database of file verdicts without the need to upload files to the cloud

Unique rollback capabilities

- Support policies that remove threats completely
- Autonomously restore endpoints to a known good state, before malicious activity initiated

Multiple layered, heuristic-based techniques

- Leverage cloud intelligence, advanced static analysis and dynamic behavioral protection
- Protect against and remediate known and unknown malware before, during, or after an attack

Application Vulnerability Intelligence

- Catalog every installed application and any associated risk
- Examine known vulnerabilities with details of the CVEs and severity levels reported
- Use this data to prioritize patching and reduce the attack surface

Endpoint Network Control

- Add firewall-like controls to the endpoint
- Use an additional quarantine rulebase to handle infected devices

Remote Shell¹

- Eliminate the need to have physical contact with devices for troubleshooting, changing local configurations, as well as conducting forensic investigations

No need for regular scans or periodic updates

- Enable the highest level of protection at all times without hampering user productivity
- Receive a full scan on install and continuously monitors for suspicious activity continually afterward

Optional integration with SonicWall firewalls

- Enable enforcement of deep packet inspection of encrypted traffic (DPI-SSL) on endpoints
- Easily deploy trusted certificates to each endpoint
- Direct unprotected users to a Capture Client download page before accessing the Internet when behind a firewall

Content Filtering

- Block malicious sites IP addresses, and domains
- Increase user productivity by throttling bandwidth or restricting access to objectionable or unproductive web content

Device Control

- Block potentially infected devices from connecting to endpoints
- Use granular allow listing policies

Capture Client Features

Feature	Advanced	Premier
Cloud Management, Reporting & Analytics (CSC)	✓	✓
Network Security Integrations		
Endpoint Visibility & Enforcement	✓	✓
DPI-SSL Certificate Deployment	✓	✓
Content Filtering	✓	✓
Advanced Endpoint Protection		
Next-Generation Antimalware	✓	✓
Capture Advanced Threat Protection Sandboxing	✓	✓
ActiveEDR (Endpoint Detection and Response)		
Attack Visualization	✓	✓
Rollback & Remediation	✓	✓
Device Control	✓	✓
Application Vulnerability and Intelligence	✓	✓
Rogues		✓
Endpoint Network Control		✓
ActiveEDR Threat Hunting and Intelligence		
Threat Hunting with Deep Visibility		✓
Remote Shell ¹		✓
Exclusions Catalog		✓

¹ Remote shell will be made available on demand in a new account (with 2FA enabled) directly on S1 console.

Capture Client - System Requirements | SonicWall

Best Practices for Global Endpoint Security Operations For MSSPs and Distributed Enterprises

Read the Solution Brief: www.sonicwall.com

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®

© 2022 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.



SONICWALL®

SonicWall Capture Client

Modern Endpoint Protection for a Rapidly Evolving Threat Landscape

