

# SonicWall Capture Client

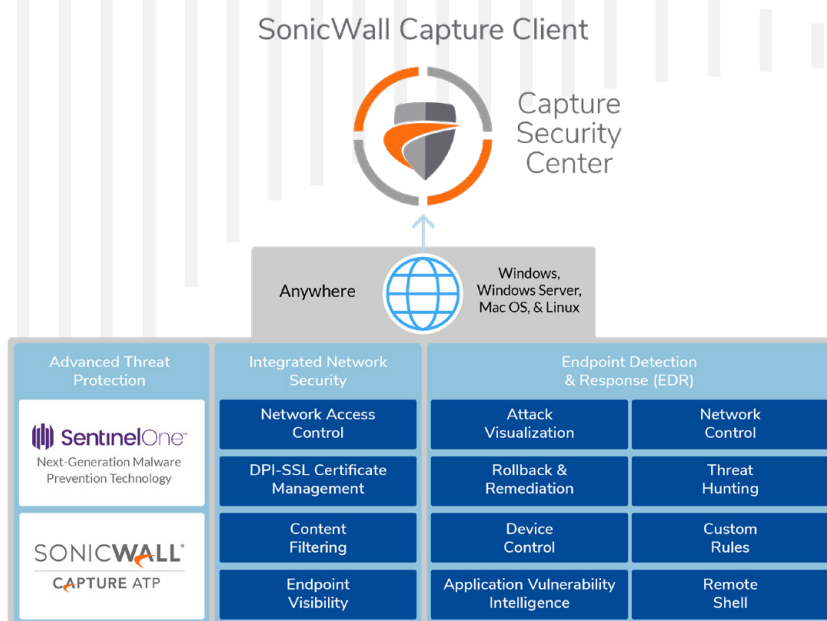
Modern Endpoint Protection for a Rapidly Evolving Threat Landscape

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

- Continuous behavioral monitoring
- Easy Threat Hunting
- Independent cloud-based management
- Security policy enforcement
- Multiple layered heuristic-based techniques for highly accurate determinations
- See all application vulnerabilities
- Single-click rollback capabilities
- Quickly view the global health of all tenants
- Fast global policy creation
- Easy Allow, Block and Exclusion creation
- Capture Advanced Threat Protection (ATP) cloud sandbox for automated malware analysis
- Upload-free threat intelligence sharing for manual file inspection
- Apply firewall policies through network control
- Enforce and view content filtering policy issues
- Block potentially malicious USB keys through Device Control
- Synergizes with SonicWall firewalls
- DPI-SSL certificate deployment



**Fitting Endpoint Security to Your Organization**

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

With a next-generation malware protection engine powered by SentinelOne, Capture Client applies behavior-based advanced threat protection techniques, such as machine learning, multi-engine sandbox integration, and single-click system rollback. Capture Client also enables the deep inspection of encrypted TLS traffic (DPI- SSL) on SonicWall firewalls by installing and managing trusted TLS certificates.

Capture Client policies for all features can be managed from a single cloud-based management console. Capture Client can be easily deployed either through Microsoft Active Directory group policies, any other third-party software deployment techniques, or through the delivery of customized URLs where clients can download and silently self-install without any additional intervention. Additionally when integrated with SonicWall firewalls, Capture Client delivers a zero-touch experience for deployment on unprotected clients with optional enforcement capabilities.

### Centralized Management and Client Protection Reporting

On the SonicWall cloud-based management console administrators can see the health of each tenant which is judged by the number of infections, vulnerabilities present, the version of Capture Client installed, and what and who is being blocked the most by the optional onboard Content Filtering. This dashboard can also tell you which devices are online and operating. From the management console, administrators can configure fine-grained policies for specific groups and even an entire tenant.

The Account Policy allows administrators to apply a single baseline policy to all tenants which makes it easier to spin up new tenants. This also allows for MSSPs to quickly create protections for new threats across all tenants on this policy. When the Inheritance option is activated, all new tenants will acquire the Account Policy, when turned off, unique policies can be created and modified for individual tenants for everything from content filtering to malware protection to DPI-SSL certificate management.

The Account scope allows managed service providers (MSSPs/MSPs) to manage and report on clients of multiple customers. At the same time, each of those customers can only manage and report on their own clients.

The management console also functions as an investigative platform to help identify the root cause of detected malware threats and provides actionable intelligence about how to prevent them from recurring. For example, Security Admins and Analysts can analyse convicted threats, determine what behaviour or attributes rendered a conviction and determine what additional response actions may be needed. Analysts can also search for indicators of compromise from emerging threats using storyline-based threat hunting.

---

## 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

### 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

### 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

## Features and Benefits Cont'd

### 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 (for Windows Devices)

- 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 (for Windows)

- Support policies that remove threats completely
- Restore endpoints to a state before malicious activity initiated

- Eliminate the need for manual restoration in the case of ransomware or similar attacks

### Application Vulnerability Intelligence (for Window and MacOS)

- 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

### Network Control

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

### Remote Shell

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

### 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 (for Windows and MacOS)

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

### Device Control (for Windows and MacOS)

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

## Capture Client Feature Comparison

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

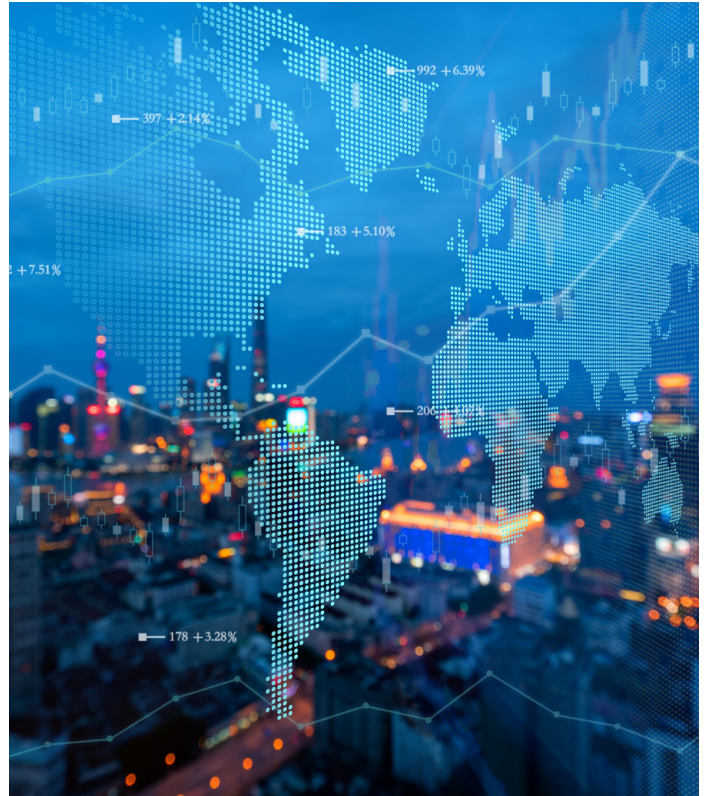
## System Requirements

### Operating System

- Windows 7 and upwards
- Windows Server 2008 R2 and upwards
- Mac OS/OSX 10.15.4 and upwards
- Amazon Linux AMI
- Red Hat Enterprise Linux RHEL v5.5-5.11, 6.5+, 7.0+
- Ubuntu 12.04, 14.04, 16.04, 16.10
- CentOS 6.5+, 7.0+
- Oracle Linux OL (formerly known as Oracle Enterprise Linux or OEL) v6.5-6.9 and v7.0+
- SUSE Linux Enterprise Server 12

### Hardware

- 1 GHz Dual-core CPU or better
- 1 GB RAM or higher if required by OS (recommended 2 GB)
- 2 GB free disk space



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

Read the Solution Brief: [www.sonicwall.com](http://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](http://www.sonicwall.com) or follow us on [Twitter](#), [LinkedIn](#), [Facebook](#) and [Instagram](#).



#### SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, CA 95035

Refer to our website for additional information.

[www.sonicwall.com](http://www.sonicwall.com)

SONICWALL®

© 2021 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.