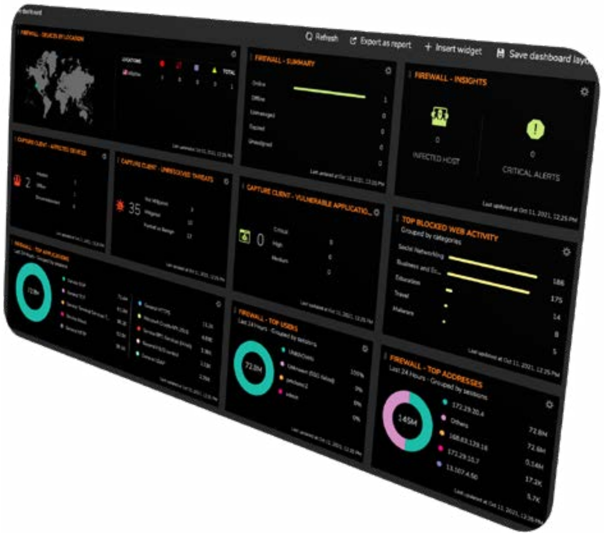
SonicWall Capture Client

An endpoint security solution that's powered by a dual engine for a layered security approach that protects endpoints whenever, wherever.

With the continued prevalence of distributed workforces and BYOD trends, the number of endpoints has exponentially increased, making the management and security of endpoints critical in today's business climate. From small- to medium-sized businesses (SMBs) to the largest enterprises, organizations need an easy-to-deploy endpoint security solution that provides air-tight, layered protection for the most persistent and advanced threats.

SonicWall's Capture Client is a unified endpoint security solution that is powered by a dual-engine and combines the best of SentinelOne's next-generation antivirus with SonicWall's ecosystem to help combat vendor sprawl and optimize security at the endpoint. In addition, in line with SonicWall's long heritage of supporting partners and Managed Service Provider's (MSPs), Capture Client is purpose-built to be able to scale and manage endpoints across diverse tenants to bring endpoint security to clients of different sizes and verticals.



BENEFITS

Improved Security

- High efficacy, actionable threat detection and protection through a powerful dual engine that contains the best of SentinelOne's NGAV and SonicWall's Capture Advanced Threat Protection (ATP) for multi-layered threat defense.

Reduced Complexity

- Granular and scalable policy management allows ease of management across global tenants. Actionable intelligence allows network admins to see through the noise, reduce alert fatigue and minimize monitoring silos - all in one unified client.

Reduced Vendor Spend/Sprawl

- Consolidate multiple management tools and utilize built in security tools like content filtering, application vulnerability intelligence and threat hunting with deep visibility.

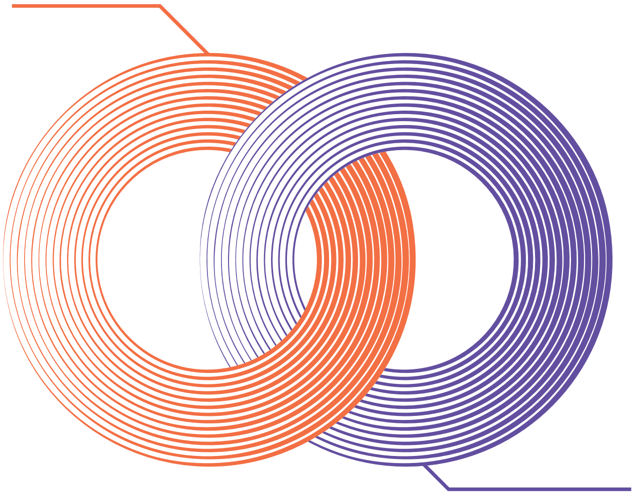
Seamless Integration with SonicWall's Ecosystem

- Deploys in a few clicks and effortlessly integrates with the SonicWall ecosystem across several points of synergy including SonicPlatform, NGFWs, Cloud Secure Edge, Managed Detection and Response, and more.

DATASHEET

ULTIMATE SYNERGY ACROSS SONICWALL ECOSYSTEM

- Unified Management and Reporting
- Capture ATP Integration
- DPI-SSL Certificate Management
- Firewall Enforcement
- Web Content Filtering



ENTERPRISE-GRADE NGAV

- High-accuracy Protection
- Endpoint Remediation and Rollback
- Best-in-Class for Macbooks
- Application Vulnerability Intelligence
- Deep Visibility
- Remote Shell

Features

Secure endpoints on three levels:

Prevention:

- **Next-Generation Antivirus (NGAV)**
  - » Built on the SentinelOne anti-malware engine, Capture Client requires no signatures, daily/ weekly updates or cloud lookups/ databases for detection.
- **Capture Advanced Threat Protection (ATP)**
  - » Includes patented Real-Time Deep Memory Inspection™ (RTDMI) component that act as an additional security feature to inspect and detect the most sophisticated malwares.
- **Web Content Filtering**
  - » Allows organizations to block malicious sites, as well as increase user productivity by throttling bandwidth or restricting access to objectionable or unproductive web content.
- **DPI-SSL Certificate Management**
  - » Enables enforcement of deep packet inspection of encrypted traffic (DPI-SSL) on endpoints and easily deploys trusted certifications to each endpoint.
- **Device Control**
  - » Prevent infected devices like USBs from connecting to endpoints, device control can lock out unknown devices.
- **Rogues**
  - » Helps identify unprotected endpoints to reduce the attack surface

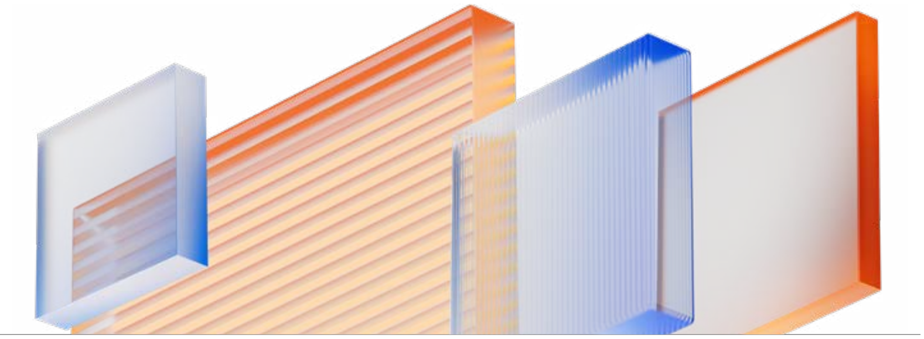
Detection:

- **Threat Hunting with Deep Visibility**
  - » Deep Visibility allows the security admins to easily find related IOCs, files, hashes, registry IDs, threat IDs and more using an intuitive UI. Queries can be customized as needed to allow for a quick, repeatable threat hunting process.
- **Application Vulnerability and Intelligence**
  - » Administrators can catalog every application on each protected endpoint with information on known vulnerabilities within them.
- **MDR***
  - » 24/7 cybersecurity experts that provide advanced behavioral analysis and autonomous defense for your endpoints. SOC monitoring reduces alert fatigue and operational inefficiencies.

**Available only with Capture Client MDR – SonicWall's managed service offering*

Remediation/Response:

- **Autonomous Remediation**
  - » Autonomously restore endpoints to a known good state before malicious activity was initiated.
- **One-Click Rollback Response**
  - » Resolve threats with one click and without scripting on one, several or all devices across the entire estate.
- **Remote Shell**
  - » Enables administrators to access an endpoint remotely without a third-party application to troubleshoot security and/or configuration issues. Administrators can use remote shell to gather forensics evidence and clean up an infected endpoint.
- **Endpoint Network Control**
  - » Allows for the transfer of firewall rules into the endpoint, therefore ensuring optimal security, regardless of a user's location. If an endpoint is discovered to be infected, it can be quarantined until an admin can remedy the issue.



Capture Client Features

Feature	Advanced	Premier	Capture Client MDR
Network Security Integrations			
Endpoint Visibility & Enforcement	✓	✓	✓
DPI-SSL Certificate Deployment	✓	✓	✓
Content Filtering	✓	✓	✓
Advanced Endpoint Protection			
Next-Generation Antivirus	✓	✓	✓
Capture Advanced Threat Protection (ATP) Sandboxing	✓	✓	✓
Endpoint Detection and Response (EDR)			
Attack Visualization	✓	✓	✓
Rollback & Remediation	✓	✓	✓
Device Control	✓	✓	✓
Application Vulnerability and Intelligence	✓	✓	✓
Rogues		✓	✓
Endpoint Network Control		✓	✓
Threat Hunting and Intelligence			
Threat Hunting with Deep Visibility		✓	✓
Remote Shell[1]		✓	✓
Exclusions Catalog		✓	✓
Managed Detection and Response (MDR)			
SIEM			✓
24/7 SOC			✓
2x/Month Audits			✓

[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

About SonicWall

SonicWall is a cybersecurity forerunner with more than 30 years of expertise and a relentless focus on its partners. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real time, SonicWall can quickly and economically provide purpose-built security solutions to any organization around the world. Based on data from its own threat research center, SonicWall delivers seamless protection against the most evasive cyberattacks and supplies actionable threat intelligence to partners, customers and the cybersecurity community.

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

SONICWALL