SonicWall Capture Client

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. Those demand a different approach to client protection. Furthermore, with the proliferation of telecommuting, mobility and BYOD, there is a dire need to deliver consistent protection for endpoints anywhere.

SonicWall Capture Client is a unified endpoint offering with multiple protection capabilities. With a next-generation malware protection engine powered by SentinelOne, Capture Client applies advanced threat protection techniques, such as machine learning, network sandbox integration, and system rollback. Capture Client also leverages the deep inspection of encrypted TLS traffic (DPI-SSL) on SonicWall firewalls by installing and managing trusted TLS certificates.

Capture Client co-exists with the SonicWall Content Filtering Client and the SonicWall Global VPN Client. Policies for all products can be managed from a single cloud-based management console. Capture Client can be easily added to any client deployed either through Microsoft Active Directory group policies or 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. And, when integrated with SonicWall firewalls, Capture Client delivers a zero-touch silent experience for deployment on unprotected clients.

Features and Benefits

Continuous behavioral monitoring of the client helps create a complete profile of file activity, application and process activity, and network activity. This allows for protection against both file-based and fileless malware and delivers a 360-degree attack view with actionable intelligence relevant for investigations.

Multiple layered, heuristic-based techniques for protection include cloud intelligence, advanced static analysis and dynamic behavioral protection. These help protect against and remediate known and unknown malware.

No need for regular scans or periodic updates enables the highest level of protection at all times without hampering user productivity.

Capture Advanced Threat Protection (ATP) integration automatically uploads suspicious files for advanced analysis through code manipulation that endpoints can't perform. Stop more threats before they execute such as malware with built-in timing delays. Administrators can also reference Capture ATP's database of file verdicts without the need to upload files to the cloud for analysis.

Unique rollback capabilities also support policies that not only remove the threat completely but also restore a targeted client to the state before the malware activity initiated. This eliminates the need for manual restoration in the case of ransomware and similar attacks on Windows.

Benefits:

- Independent cloud-based management
- Synergizes with SonicWall firewalls
- Security policy enforcement
- DPI-SSL certificate management
- Continuous behavioral monitoring
- Highly accurate determinations achieved through machine learning
- Multiple layered heuristic-based techniques
- Unique rollback capabilities
- Easy white/blacklisting
- Capture Advanced Threat Protection (ATP) cloud sandbox for automated malware analysis
- Upload-free threat intelligence sharing for manual file inspection

Cloud-based management console reduces the footprint and overhead of management. It also improves the ability to deploy and enforce endpoint protection, wherever the endpoint is.

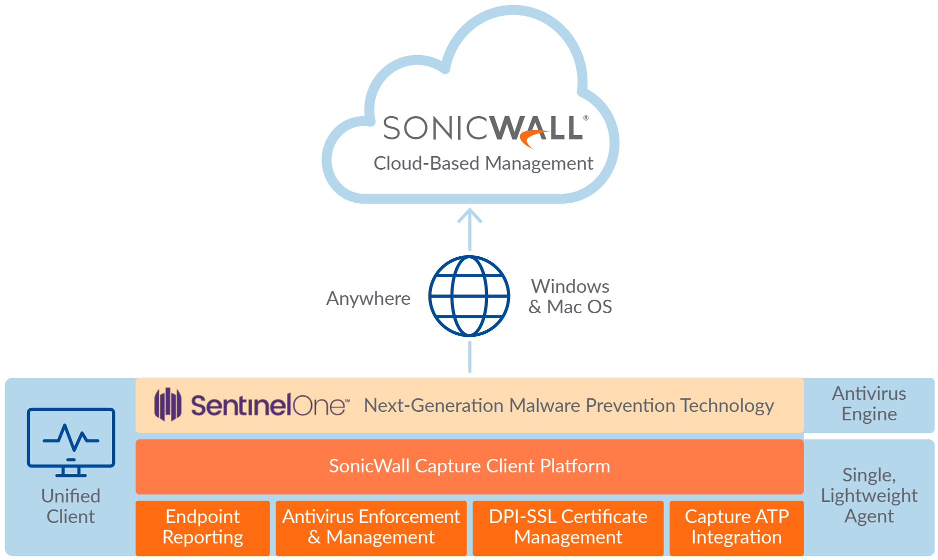
Integration with the SonicWall next-generation firewalls delivers zero-touch deployment and enhanced endpoint compliance. Plus it enables enforcement of deep packet inspection of encrypted traffic (DPI-SSL) by deploying trusted certificates to each endpoint.

Centralized Management and Client Protection Reporting

The SonicWall cloud-based management console functions as a single pane of glass to manage all client policies, including next-generation malware protection, DPI-SSL certificate management, content filtering and VPN.

The management console is a multi-tenant cloud-based platform offered at no additional cost. It provides client protection reporting and policy management, with support for fine-grain access control policies. These allow managed service providers (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.

It also functions as an investigative platform to help identify the root cause of detected malware threats and provide actionable intelligence about how to prevent these from recurring. For example, an administrator can easily view what applications are running on a client. That, in turn, can help identify machines that may be running vulnerable or unauthorized software.


SONICWALL
Cloud-Based Management
Anywhere
Windows & Mac OS
SentinelOne Next-Generation Malware Prevention Technology
Antivirus Engine
Unified Client
SonicWall Capture Client Platform
Single, Lightweight Agent
Endpoint Reporting
Antivirus Enforcement & Management
DPI-SSL Certificate Management
Capture ATP Integration

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.

Offerings and Platform Support

The SonicWall Capture Client is available in two offerings:

SonicWall Capture Client Basic delivers all SonicWall next-generation malware protection and remediation features, along with DPI-SSL support capabilities.

SonicWall Capture Client Advanced delivers everything listed above for Basic, plus advanced rollback capabilities and Capture ATP integration.

Both offerings are available for Windows 7 and higher, as well as for Mac OSX.

System Requirements
Operating Systems
Windows 7 and upwards
Windows Server 2008 R2 and upwards
Mac OS/OSX 10.10 and upwards
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

Features Comparison		
Feature	Capture Client Basic	Capture Client Advanced
DPI-SSL Certificate Deployment	✓	✓
Firewall Enforcement	✓	✓
Next-Generation Antivirus (NGAV) Protection	✓	✓
Application Whitelisting/Blacklisting	✓	✓
Capture Advanced Threat Protection (ATP) Automated Analysis	-	✓
Threat Intelligence Sharing with Capture ATP	-	✓
Remediation/Rollback	-	✓
Attack Visualization	-	✓