SONICWALL

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. Additionally, 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 SonicWall Global VPN Client and 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, 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.

Features and Benefits

Continuous behavioral monitoring of the endpoint 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 Client does a full scan on install and continuously monitors for suspicious activity continually afterward.

Capture Advanced Threat Protection (ATP) integration automatically uploads suspicious files for advanced sandboxing 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
- Application Vulnerability Intelligence
- 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
- Content Filtering
- Device Control

Application Vulnerability Intelligence gives administrators the ability to catalog every application on each protected endpoint and any risk associated with it. Risk is based on the presence of any known vulnerabilities with details of the CVEs and severity levels reported for that version, giving the administrator actionable intelligence to prioritize patching and reduce the attack surface of the endpoint.

Optional integration with SonicWall generation 6 and above 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.

Content Filtering allows organizations to block malicious sites IP addresses, and domains, as well as increase user productivity by throttling bandwidth or restricting access to objectionable or unproductive web content.

Device Control allows organizations to block potentially infected devices from connecting to the endpoint with granular whitelisting policies.

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, and content filtering.

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 including the ability to assign policies based on Microsoft Active Directory attributes. This allows 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.

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, 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.

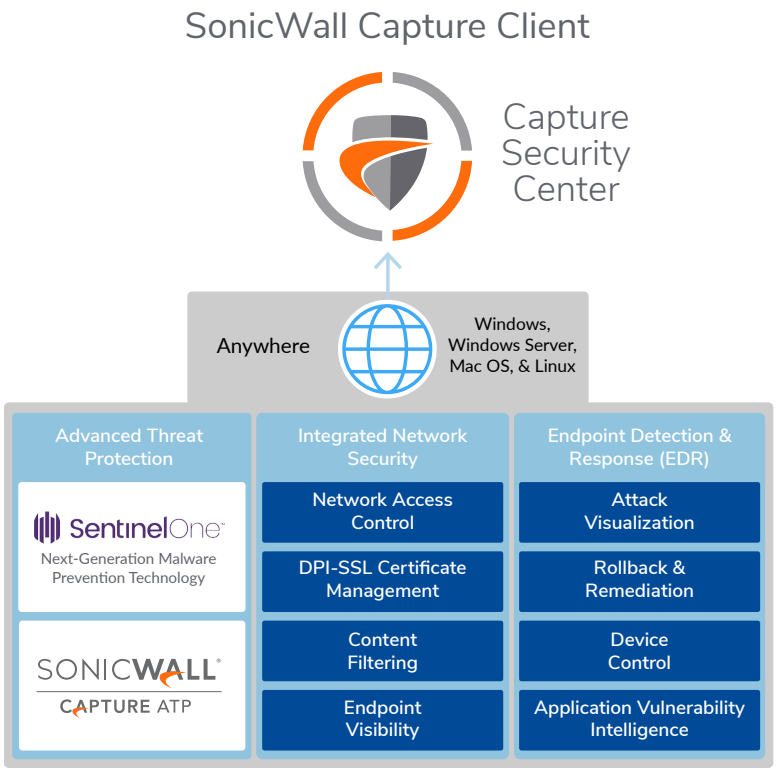
Offerings and Platform Support

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, Capture ATP integration, Attack Visualization, Application Vulnerability Intelligence, and Content Filtering.

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



FEATURES COMPARISON		
Feature	Basic	Advanced
Cloud Management, Reporting & Analytics (CSC)	✓	✓
Integrated Network Security		
Endpoint Visibility	✓	✓
DPI-SSL Certificate Deployment	✓	✓
Content Filtering	–	✓
Advanced Threat Protection		
Next-Generation Antimalware	✓	✓
Capture Advanced Threat Protection Sandboxing	–	✓
Endpoint Detection and Response		
Attack Visualization	–	✓
Rollback & Remediation	–	✓
Device Control	–	✓
Application Vulnerability and Intelligence	–	✓

SYSTEM REQUIREMENTS
Operating Systems
Windows 7 and upwards
Windows Server 2008 R2 and upwards
Mac OS/OSX 10.10 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

CAPTURE CLIENT SKUS		
Product	Validity	SKU
ADVANCED		
SONICWALL CAPTURE CLIENT ADVANCED 5-24 ENDPOINTS with 24X7 Support	3YR	02-SSC-1518
SONICWALL CAPTURE CLIENT ADVANCED 5-24 ENDPOINTS with 24X7 Support	1YR	02-SSC-1519
SONICWALL CAPTURE CLIENT ADVANCED 25-49 ENDPOINTS with 24X7 Support	3YR	02-SSC-1520
SONICWALL CAPTURE CLIENT ADVANCED 25-49 ENDPOINTS with 24X7 Support	1YR	02-SSC-1521
SONICWALL CAPTURE CLIENT ADVANCED 50-99 ENDPOINTS with 24X7 Support	3YR	02-SSC-1522
SONICWALL CAPTURE CLIENT ADVANCED 50-99 ENDPOINTS with 24X7 Support	1YR	02-SSC-1523
SONICWALL CAPTURE CLIENT ADVANCED 100-249 ENDPOINTS with 24X7 Support	3YR	02-SSC-1524
SONICWALL CAPTURE CLIENT ADVANCED 100-249 ENDPOINTS with 24X7 Support	1YR	02-SSC-1525
SONICWALL CAPTURE CLIENT ADVANCED 250-499 ENDPOINTS with 24X7 Support	3YR	02-SSC-1454
SONICWALL CAPTURE CLIENT ADVANCED 250-499 ENDPOINTS with 24X7 Support	1YR	02-SSC-1455
SONICWALL CAPTURE CLIENT ADVANCED 500-999 ENDPOINTS with 24X7 Support	3YR	02-SSC-1456
SONICWALL CAPTURE CLIENT ADVANCED 500-999 ENDPOINTS with 24X7 Support	1YR	02-SSC-1457
SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 ENDPOINTS with 24X7 Support	3YR	02-SSC-1458
SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 ENDPOINTS with 24X7 Support	1YR	02-SSC-1459
SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 ENDPOINTS with 24X7 Support	3YR	02-SSC-1460
SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 ENDPOINTS with 24X7 Support	1YR	02-SSC-1461
SONICWALL CAPTURE CLIENT ADVANCED 10000+ ENDPOINTS with 24X7 Support	3YR	02-SSC-1462
SONICWALL CAPTURE CLIENT ADVANCED 10000+ ENDPOINTS with 24X7 Support	1YR	02-SSC-1463
BASIC		
SONICWALL CAPTURE CLIENT BASIC 5-24 ENDPOINTS with 24X7 Support	3YR	02-SSC-1510
SONICWALL CAPTURE CLIENT BASIC 5-24 ENDPOINTS with 24X7 Support	1YR	02-SSC-1511
SONICWALL CAPTURE CLIENT BASIC 25-49 ENDPOINTS with 24X7 Support	3YR	02-SSC-1512
SONICWALL CAPTURE CLIENT BASIC 25-49 ENDPOINTS with 24X7 Support	1YR	02-SSC-1513
SONICWALL CAPTURE CLIENT BASIC 50-99 ENDPOINTS with 24X7 Support	3YR	02-SSC-1514
SONICWALL CAPTURE CLIENT BASIC 50-99 ENDPOINTS with 24X7 Support	1YR	02-SSC-1515
SONICWALL CAPTURE CLIENT BASIC 100-249 ENDPOINTS with 24X7 Support	3YR	02-SSC-1516
SONICWALL CAPTURE CLIENT BASIC 100-249 ENDPOINTS with 24X7 Support	1YR	02-SSC-1517
SONICWALL CAPTURE CLIENT BASIC 250-499 ENDPOINTS with 24X7 Support	3YR	02-SSC-1444
SONICWALL CAPTURE CLIENT BASIC 250-499 ENDPOINTS with 24X7 Support	1YR	02-SSC-1445
SONICWALL CAPTURE CLIENT BASIC 500-999 ENDPOINTS with 24X7 Support	3YR	02-SSC-1446
SONICWALL CAPTURE CLIENT BASIC 500-999 ENDPOINTS with 24X7 Support	1YR	02-SSC-1447
SONICWALL CAPTURE CLIENT BASIC 1000-4999 ENDPOINTS with 24X7 Support	3YR	02-SSC-1448
SONICWALL CAPTURE CLIENT BASIC 1000-4999 ENDPOINTS with 24X7 Support	1YR	02-SSC-1449
SONICWALL CAPTURE CLIENT BASIC 5000-9999 ENDPOINTS with 24X7 Support	3YR	02-SSC-1450
SONICWALL CAPTURE CLIENT BASIC 5000-9999 ENDPOINTS with 24X7 Support	1YR	02-SSC-1451
SONICWALL CAPTURE CLIENT BASIC 10000+ ENDPOINTS with 24X7 Support	3YR	02-SSC-1452
SONICWALL CAPTURE CLIENT BASIC 10000+ ENDPOINTS with 24X7 Support	1YR	02-SSC-1453

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

Datasheet-CaptureClient-US-COG-2413