

# SonicWall Capture Client

Die konstant wachsende Bedrohung durch Ransomware und andere Malware-Angriffe zeigt deutlich, dass sich die Wirksamkeit von Lösungen zum Schutz der Clients nicht ausschließlich auf Basis der Endpunkt-Konformität messen lässt. Der bisher in der Antivirustechnologie eingesetzte signaturgestützte Ansatz ist seit Langem umstritten und kann mit den neuesten Malware- und Umgehungstechniken nicht Schritt halten. Auch die zunehmende Verbreitung von Telearbeit, Mobilität und BYOD macht die Verfügbarkeit eines konstanten Schutzes aller Endpunktstellen noch dringlicher.

SonicWall Capture Client ist ein optimal abgestimmtes Endpunktangebot und umfasst mehrere Schutzkapazitäten. Capture Client stützt sich auf die Next-Generation-Malwareschutz-Engine SentinelOne und setzt modernste Bedrohungsschutztechnologien ein, wie Machine-Learning, Netzwerk-Sandbox-Integration und System-Rollback. Darüber hinaus lässt sich durch die Installation und Verwaltung vertrauenswürdiger TLS-Zertifikate der verschlüsselte TLS-Verkehr mittels Deep Packet Inspection (DPI-SSL) auf SonicWall-Firewalls scannen.

Capture Client koexistiert mit SonicWall Global VPN Client und die Richtlinien für alle Produkte können über eine zentrale Cloud-basierte Verwaltungskonsole verwaltet werden. Durch Microsoft Active Directory Gruppenrichtlinien oder Implementierungstechniken von Drittanbietern kann Capture Client leicht jedem Client hinzugefügt werden. Dies kann auch durch Zustellung bedarfsspezifischer URLs erfolgen, sodass die Clients ohne weiteren Benutzereingriff selbst heruntergeladen und im Hintergrund installieren können. Bei einer Integration mit SonicWall-Firewalls liefert Capture Client eine Zero-Touch-Einbindung auf ungeschützten Clients.

## Leistungsmerkmale und Vorteile

**Kontinuierliche Verhaltensüberwachung** bei den Clients ermöglicht die Erstellung eines kompletten Profils der Aktivitäten auf Datei-, Anwendungs-, Prozess- und Netzwerkebene. Dies ermöglicht Schutz vor dateibasierter und auch dateiloser Malware und liefert eine 360-Grad-Sicht auf Angriffe und für die Ermittlungen umsetzbare Informationen.

**Mehrschichtige heuristische Techniken** für die Schutzfunktion umfassen Cloud-Intelligence, komplexe Analysen und dynamische Verhaltensüberwachung. Damit kann bekannte und unbekannte Malware abgewehrt und verhindert werden.

**Da keine regelmäßigen Scans oder Updates erforderlich sind**, wird das höchste Schutzniveau aller Zeiten ganz ohne Beeinträchtigung der Nutzerproduktivität ermöglicht.

**Durch die Integration von Advanced Threat Protection (ATP)** werden verdächtige Dateien automatisch für die erweiterte Analyse auf Codemanipulation, die von Endpunkten nicht durchgeführt werden kann, hochgeladen. So können mehr Bedrohungen noch vor der Ausführung gestoppt werden, wie z. B. Malware mit integrierten Zeitverzögerungen. Die Lösung erlaubt Administratoren zudem, Urteile über verdächtige Dateien aus der Capture ATP-Datenbank einzusehen, ohne die Dateien zur Analyse in die Cloud hochladen zu müssen.

**Einzigartige Rollback-Funktionen** unterstützen Richtlinien, die Bedrohungen nicht nur vollständig entfernen, sondern auch den angegriffenen Client in einen unversehrten Zustand vor Einleitung der Malware-Aktivität zurückversetzen. Somit ist im Fall von Ransomware- und ähnlichen Angriffen auf Windows keine manuelle Wiederherstellung erforderlich.

## Vorteile

- Unabhängige, Cloud-basierte Verwaltung
- Zusammenwirkung mit SonicWall-Firewalls
- Durchsetzung von Sicherheitsrichtlinien
- DPI-SSL-Zertifikatverwaltung
- Kontinuierliche Verhaltensüberwachung
- Hochpräzise Bestimmungen durch Machine-Learning
- Mehrschichtige heuristische Techniken
- Einzigartige Rollback-Funktionen
- Einfaches White-/Blacklisting
- Capture Advanced Threat Protection (ATP) Cloud-Sandbox für die automatische Malware-Analyse
- Threat-Intelligence-Austausch für die manuelle Inspektion ohne Uploads
- Schutz vor Bedrohungen aus dem Web
- Gerätekontrolle

Die Cloud-basierte Verwaltungskonsole reduziert den Platzbedarf und den Verwaltungsaufwand. Zugleich werden Einbindung und Durchsetzung des Endpunktschutzes, egal wo sich der Endpunkt befindet, optimiert.

Eine optionale Integration mit SonicWall-Firewalls Generation 6 und höher ermöglicht Zero-Touch-Deployment und bessere Endpunktkonformität. Zusätzlich wird die Durchsetzung einer Deep Packet Inspection des verschlüsselten Verkehrs (DPI-SSL) ermöglicht, indem an jeden Endpunkt vertrauenswürdige Zertifikate gesandt werden.

Schutz vor Bedrohungen aus dem Web und Gerätekontrolle ermöglichen Organisationen das Blockieren von böartigen Sites und IP-Adressen sowie das Verhindern der Verbindung von unbekanntem und potenziell infizierten Geräten mit dem Endpunkt.

Zentrale Verwaltung und Client Protection Reporting Die Cloud-basierte SonicWall-Verwaltungskonsole

dient als zentrale Benutzeroberfläche für die Verwaltung aller Client-Richtlinien, einschließlich Next-Generation-Malwareschutz, DPI-SSL-Zertifikatverwaltung, Content-Filtering und VPN.

Die Verwaltungskonsole ist eine Cloud-basierte, mandantenfähige Plattform, die ohne Aufpreis zur Verfügung gestellt wird. Sie ermöglicht Client Protection Reporting sowie Richtlinienverwaltung und unterstützt granulare Zugangskontrollen-Richtlinien. So können Managed-Service-Provider (MSPs) die Clients mehrerer Kunden verwalten und protokollieren. Zugleich kann jeder dieser Kunden auch seine eigenen Clients verwalten und protokollieren.

Die Konsole dient auch als Untersuchungsplattform und hilft bei der Identifizierung der Ursachen der erkannten Malwarebedrohungen. Sie liefert umsetzbare Informationen darüber, wie ein erneutes Auftreten dieser Bedrohungen verhindert werden kann. So kann ein Administrator

beispielsweise leicht beobachten, welche Anwendungen auf einem Client ausgeführt werden. Das hilft wiederum bei der Identifizierung von Rechnern, auf denen anfällige oder nicht genehmigte Software ausgeführt wird.

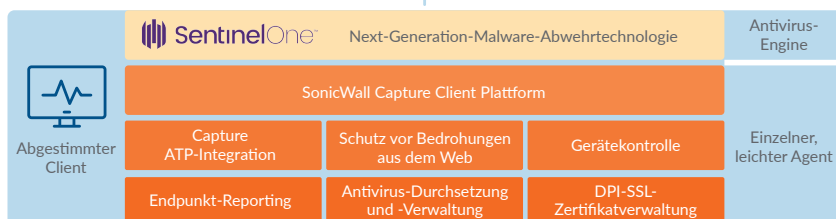
### Angebote und Plattform-Support

SonicWall Capture Client gibt es in zwei Ausführungen:

**SonicWall Capture Client Basic** bietet die neuesten Funktionen zum Schutz gegen Schadsoftware und zur Wiederherstellung sowie DPI-SSL-Support.

**SonicWall Capture Client Advanced** bietet alle oben aufgeführten Funktionsmerkmale der Basic-Funktion plus erweiterte Rollback-Fähigkeiten, Capture ATP-Integration, Angriffsvisualisierung und Schutz vor Bedrohungen aus dem Web.

Beide Angebote sind für Windows 7 und höher sowie für Mac OS X erhältlich.



### SYSTEMVORAUSSETZUNGEN

Betriebssystem	
Windows 7 und höher	
Windows Server 2008 R2 und höher	
Mac OS/OSX 10.10 und höher	
Hardware	
1 GHz Dual-Core CPU oder besser	
1 GB RAM oder höher, falls für das Betriebssystem erforderlich (2 GB werden empfohlen)	
2 GB freier Plattenspeicher	

### VERGLEICH DER FUNKTIONSMERKMALE

Funktion	Capture Client Basic	Capture Client Advanced
DPI-SSL-Zertifikateinbindung	✓	✓
Firewall-Durchsetzung	✓	✓
Antivirenschutz der nächsten Generation (NGAV)	✓	✓
Whitelisting/Blacklisting von Anwendungen	✓	✓
Automatische Analyse mit Capture Advanced Threat Protection (ATP)	–	✓
Austausch von Bedrohungsinformationen mit Capture ATP	–	✓
Abhilfe/Rollback	–	✓
Angriffsvisualisierung	–	✓
Schutz vor Bedrohungen aus dem Web	–	✓
Gerätekontrolle	–	✓

## CAPTURE CLIENT ARTIKELNUMMERN

Produkt	Gültigkeit	Artikelnummer
<b>ADVANCED</b>		
SONICWALL CAPTURE CLIENT ADVANCED 5-24 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1518
SONICWALL CAPTURE CLIENT ADVANCED 5-24 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1519
SONICWALL CAPTURE CLIENT ADVANCED 25-49 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1520
SONICWALL CAPTURE CLIENT ADVANCED 25-49 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1521
SONICWALL CAPTURE CLIENT ADVANCED 50-99 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1522
SONICWALL CAPTURE CLIENT ADVANCED 50-99 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1523
SONICWALL CAPTURE CLIENT ADVANCED 100-249 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1524
SONICWALL CAPTURE CLIENT ADVANCED 100-249 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1525
SONICWALL CAPTURE CLIENT ADVANCED 250-499 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1454
SONICWALL CAPTURE CLIENT ADVANCED 250-499 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1455
SONICWALL CAPTURE CLIENT ADVANCED 500-999 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1456
SONICWALL CAPTURE CLIENT ADVANCED 500-999 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1457
SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1458
SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1459
SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1460
SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1461
SONICWALL CAPTURE CLIENT ADVANCED 10000+ ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1462
SONICWALL CAPTURE CLIENT ADVANCED 10000+ ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1463
<b>BASIC</b>		
SONICWALL CAPTURE CLIENT BASIC 5-24 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1510
SONICWALL CAPTURE CLIENT BASIC 5-24 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1511
SONICWALL CAPTURE CLIENT BASIC 25-49 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1512
SONICWALL CAPTURE CLIENT BASIC 25-49 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1513
SONICWALL CAPTURE CLIENT BASIC 50-99 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1514
SONICWALL CAPTURE CLIENT BASIC 50-99 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1515
SONICWALL CAPTURE CLIENT BASIC 100-249 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1516
SONICWALL CAPTURE CLIENT BASIC 100-249 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1517
SONICWALL CAPTURE CLIENT BASIC 250-499 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1444
SONICWALL CAPTURE CLIENT BASIC 250-499 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1445
SONICWALL CAPTURE CLIENT BASIC 500-999 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1446
SONICWALL CAPTURE CLIENT BASIC 500-999 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1447
SONICWALL CAPTURE CLIENT BASIC 1000-4999 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1448
SONICWALL CAPTURE CLIENT BASIC 1000-4999 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1449
SONICWALL CAPTURE CLIENT BASIC 5000-9999 ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1450
SONICWALL CAPTURE CLIENT BASIC 5000-9999 ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1451
SONICWALL CAPTURE CLIENT BASIC 10000+ ENDPUNKTE mit 24x7 Support	3 JAHRE	02-SSC-1452
SONICWALL CAPTURE CLIENT BASIC 10000+ ENDPUNKTE mit 24x7 Support	1 JAHR	02-SSC-1453

## Über SonicWall

SonicWall kämpft seit über 27 Jahren gegen Cyberkriminalität und verteidigt kleine und mittelständische Betriebe, größere Unternehmen und Regierungsbehörden weltweit. Unsere preisgekrönten Lösungen zur Erkennung und Prävention von Datenschutzverletzungen in Echtzeit bauen auf der Forschung aus den SonicWall Capture Labs auf und sichern mehr als eine Million Netzwerke sowie E-Mails, Anwendungen und Daten in mehr als 215 Ländern und Gebieten. Die betreffenden Organisationen können sich besser auf ihr Geschäft konzentrieren und müssen sich weniger um ihre Sicherheit sorgen. Weitere Informationen finden Sie auf [www.sonicwall.com](http://www.sonicwall.com) oder folgen Sie uns auf [Twitter](#), [LinkedIn](#), [Facebook](#) und [Instagram](#).