SONICWALL

SonicWall Capture Client

Die konstant wachsende Bedrohung durch Ransomware und andere Malware-Attacken 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 und die Durchsetzung der Internetrichtlinien für Endpunkte 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, Multi-Engine-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 herunterladen und im Hintergrund installieren können. Bei der Integration mit SonicWall Firewalls ermöglicht Capture Client eine Zero-Touch-Einbindung auf ungeschützten Clients mit optionalen Enforcement-Funktionen.

Zentrale Verwaltung und Client Protection Reporting

Die Cloud-basierte SonicWall-Verwaltungskonsole und das globale Dashboard bieten MSSPs eine globale Ansicht mit einem Snapshot des Zustands ihrer Mandanten. Administratoren können den Zustand jedes Mandanten einsehen, wobei der Zustand auf Basis der Anzahl von Infektionen, vorhandener Schwachstellen, der installierten Capture Client-Version und der durch Content-Filtering am häufigsten blockierten Bedrohungen beurteilt wird. Zudem kann das Dashboard Auskunft darüber geben, welche Geräte online geschaltet und in Betrieb sind.

Die Globale Richtlinie ermöglicht Administratoren die Anwendung einer grundlegenden Richtlinie für alle Mandanten, wodurch die Integration neuer Mandanten wesentlich vereinfacht wird. Zugleich wird den MSSPs ermöglicht, bei neuen Bedrohungen schnell Schutzvorkehrungen für alle unter diese Richtlinie fallenden Mandanten einzurichten. Wenn die Option „Inheritance“ aktiviert ist, erhalten alle neuen Mandanten die Globale Richtlinie, auch wenn diese für sie deaktiviert ist. Zugleich können für einzelne Mandanten individuelle Richtlinien für Funktionen vom Content-Filtering über den Malware-Schutz bis hin zur DPI-SSL-Zertifikatsverwaltung erstellt und geändert werden.

Unterstützt granulare Zugriffskontrollen-Richtlinien und ermöglicht die Zuweisung von Richtlinien auf Basis der Microsoft Active Directory-Attribute, z. B. nach Benutzergruppe. So können Managed-Service-Provider (MSSPs/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

Vorteile

- Unabhängige, Cloud-basierte Verwaltung
- Zusammenwirkung mit SonicWall-Firewalls
- Durchsetzung von Sicherheitsrichtlinien
- DPI-SSL-Zertifikatverwaltung
- Kontinuierliche Verhaltensüberwachung
- Hochpräzise Bestimmungen dank maschinellem Lernen
- Mehrschichtige heuristische Techniken
- Informationen über Anwendungsschwachstellen
- Einzigartige Rollback-Funktionen
- Globales Health-Dashboard für alle Mandanten
- Einfache Erstellung von globalen Richtlinien
- Einfache Erstellung von Erlauben/Blockieren-Listen
- Capture Advanced Threat Protection (ATP) Cloud-Sandbox für die automatische Malware-Analyse
- Threat-Intelligence-Austausch für die manuelle Inspektion ohne Uploads
- Content-Filtering
- Device-Control

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.

Leistungsmerkmale und Vorteile

Kontinuierliche Verhaltensüberwachung

- Anzeige kompletter Profile von Dateien, Anwendungen, Prozessen und Netzwerkaktivitäten
- Schutz vor dateibasierter und dateiloser Malware
- 360-Grad-Ansicht von Angriffen mit umsetzbaren Informationen

Mehrschichtige heuristische Techniken

- Nutzung von Cloud-Intelligence-Daten, erweiterten statischen Analysen und dynamischer Verhaltensüberwachung
- Schutz vor bekannter und unbekannter Malware und Abhilfe vor, während oder nach einem Angriff

Keine regelmäßigen Scans oder periodische Updates erforderlich

- Jederzeit maximaler Schutz ohne Beeinträchtigung der Produktivität von Benutzern
- Umfassender Scan bei der Installation, gefolgt von kontinuierlicher Überwachung auf verdächtige Aktivitäten

Integration der Capture Advanced Threat Protection (ATP) (für Windows-Geräte)

- Verdächtige Dateien auf Windows-Geräten werden automatisch für eine erweiterte Sandbox-Analyse hochgeladen
- Erkennung schlummernder Bedrohungen noch vor deren Aktivierung, wie z. B. Malware mit integrierten Zeitverzögerungen
- Urteile über verdächtige Dateien können in der Capture ATP-Datenbank eingesehen werden, ohne die Dateien zur Analyse in die Cloud hochladen zu müssen

Einzigartige Rollback-Funktionen (für Windows)

- Support-Richtlinien für die vollständige Entfernung von Bedrohungen
- Wiederherstellung von Endpunkten auf einen Zustand vor Eintritt der bösartigen Aktivität
- Somit ist im Fall von Ransomware- und ähnlichen Attacken keine manuelle Wiederherstellung erforderlich

Informationen über Anwendungsschwachstellen (für Windows und MacOS)

- Katalogisierung aller installierten Anwendungen und aller damit verbundenen Risiken
- Untersuchung bekannter Schwachstellen mit Details zu den CVEs und den gemeldeten Schweregraden
- Diese Daten können für die Priorsierung von Patching und zur Reduzierung der Angriffsfläche verwendet werden

Optionale Integration mit SonicWall Firewalls

- Ermöglicht die Durchsetzung der Deep Packet Inspection von verschlüsseltem Datenverkehr (DPI-SSL) an Endpunkten
- Einfache Einbindung vertrauter Zertifikate für jeden Endpunkt
- Ungeschützte Benutzer werden vor dem Zugriff auf das Internet hinter einer Firewall auf eine Capture Client Download-Seite verwiesen

Content-Filtering (für Windows) und MacOS)

- Blockierung von IP-Adressen und Domänen bösartiger Websites
- Steigerung der Benutzerproduktivität durch Drosselung der Bandbreite oder Einschränkung des Zugriffs auf anstößige oder unproduktive Webinhalte

Gerätekontrolle (für Windows und MacOS)

- Blockierung potenziell infizierter Geräte vor deren Verbindung mit Endpunkten
- Verwendung granularer Richtlinien für die Zulassung von Listings

Angebote und Plattform-Support

SonicWall Capture Client gibt es in zwei Ausführungen:

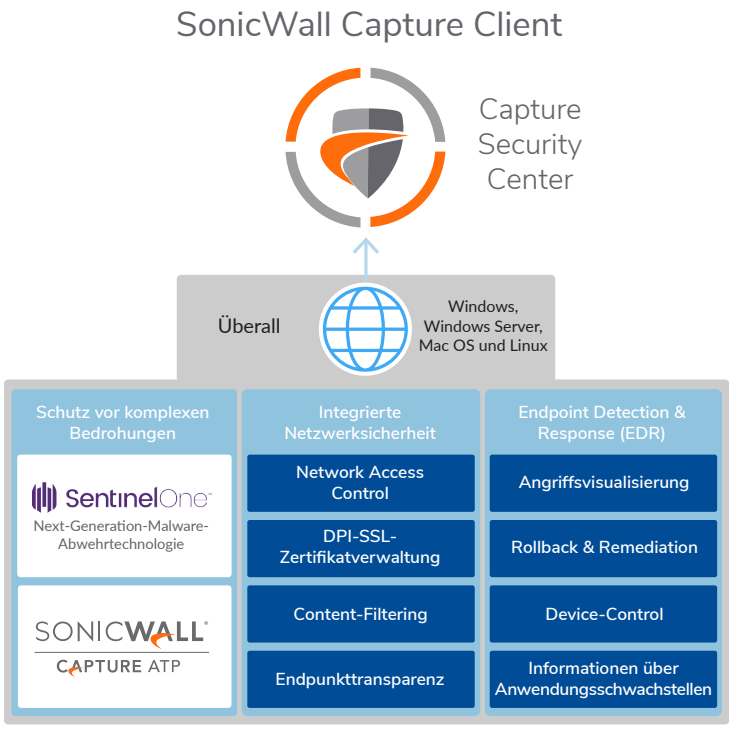
SonicWall Capture Client Basic bietet:

- Den neuesten Next-Generation-Malwareschutz von SonicWall
- Funktionen zur Wiederherstellung
- DPI-SSL-Support.

SonicWall Capture Client Advanced bietet:

- Alle oben aufgeführten Funktionsmerkmale der Basic-Ausführung
- Erweiterte Rollback-Funktionen
- Capture ATP-Integration
- Angriffsvisualisierung
- Informationen über Anwendungsschwachstellen
- Content-Filtering

Beide Angebote sind für Windows 7 und höher, Mac OSX sowie Linux erhältlich (weitere Informationen zu den Systemanforderungen finden Sie unten).



VERGLEICH DER FUNKTIONSMERKMALE		
Funktion	**Basic**	**Advanced**
Cloud Management, Reporting & Analytics (CSC)	✓	✓
Integrierte Netzwerksicherheit		
Endpunkttransparenz	✓	✓
DPI-SSL-Zertifikateinbindung	✓	✓
Content-Filtering	–	✓
Schutz vor komplexen Bedrohungen		
Malwareschutz der nächsten Generation	✓	✓
Capture Advanced Threat Protection Sandboxing	–	✓
Endpoint Detection and Response		
Angriffsvisualisierung	–	✓
Rollback & Remediation	–	✓
Device-Control	–	✓
Informationen über Anwendungsschwachstellen	–	✓

SYSTEMVORAUSSETZUNGEN
Betriebssystem
Windows 7 und höher
Windows Server 2008 R2 und höher
Mac OS/OSX 10.10 und höher
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 (vormals Oracle Enterprise Linux oder OEL) v6.5-6.9 und v7.0+
SUSE Linux Enterprise Server 12
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

CAPTURE CLIENT ARTIKELNUMMERN		
Produkt	Gültigkeit	Artikelnummer
ADVANCED		
SONICWALL CAPTURE CLIENT ADVANCED 5-24 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1518
SONICWALL CAPTURE CLIENT ADVANCED 5-24 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1519
SONICWALL CAPTURE CLIENT ADVANCED 25-49 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1520
SONICWALL CAPTURE CLIENT ADVANCED 25-49 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1521
SONICWALL CAPTURE CLIENT ADVANCED 50-99 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1522
SONICWALL CAPTURE CLIENT ADVANCED 50-99 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1523
SONICWALL CAPTURE CLIENT ADVANCED 100-249 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1524
SONICWALL CAPTURE CLIENT ADVANCED 100-249 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1525
SONICWALL CAPTURE CLIENT ADVANCED 250-499 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1454
SONICWALL CAPTURE CLIENT ADVANCED 250-499 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1455
SONICWALL CAPTURE CLIENT ADVANCED 500-999 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1456
SONICWALL CAPTURE CLIENT ADVANCED 500-999 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1457
SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1458
SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1459
SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1460
SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1461
SONICWALL CAPTURE CLIENT ADVANCED 10000+ ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1462
SONICWALL CAPTURE CLIENT ADVANCED 10000+ ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1463
BASIC		
SONICWALL CAPTURE CLIENT BASIC 5-24 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1510
SONICWALL CAPTURE CLIENT BASIC 5-24 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1511
SONICWALL CAPTURE CLIENT BASIC 25-49 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1512
SONICWALL CAPTURE CLIENT BASIC 25-49 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1513
SONICWALL CAPTURE CLIENT BASIC 50-99 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1514
SONICWALL CAPTURE CLIENT BASIC 50-99 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1515
SONICWALL CAPTURE CLIENT BASIC 100-249 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1516
SONICWALL CAPTURE CLIENT BASIC 100-249 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1517
SONICWALL CAPTURE CLIENT BASIC 250-499 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1444
SONICWALL CAPTURE CLIENT BASIC 250-499 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1445
SONICWALL CAPTURE CLIENT BASIC 500-999 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1446
SONICWALL CAPTURE CLIENT BASIC 500-999 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1447
SONICWALL CAPTURE CLIENT BASIC 1000-4999 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1448
SONICWALL CAPTURE CLIENT BASIC 1000-4999 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1449
SONICWALL CAPTURE CLIENT BASIC 5000-9999 ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1450
SONICWALL CAPTURE CLIENT BASIC 5000-9999 ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1451
SONICWALL CAPTURE CLIENT BASIC 10000+ ENDPUNKTE mit 24/7 Support	3 JAHRE	02-SSC-1452
SONICWALL CAPTURE CLIENT BASIC 10000+ ENDPUNKTE mit 24/7 Support	1 JAHR	02-SSC-1453

Über SonicWall

SonicWall bietet Boundless Cybersecurity für das hyperverteilte Umfeld einer neuen Arbeitsrealität, in der jeder remote, mobil und ungeschützt ist. Indem SonicWall das Unbekannte kennt, Echtzeit-Transparenz und skalierbare Ökonomien ermöglicht, werden Cybersicherheitslücken bei Unternehmen, Regierungen und KMU weltweit geschlossen. Weitere Informationen finden Sie auf www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

Datasheet-CaptureClient-US-VG-2889