SONICWALL

Durch unsere Fenster können Sie alles sehen

Seien Sie wachsamer. Eine ganzheitliche integrierte Lösung für ein allumfassendes Security-Management.

SONICWALL CAPTURE SECURITY CENTER IST BENUTZERFREUNDLICH

mit Single-Sign-On (SSO) und Single-Pane-of-Glass (SPOG)-Architektur. Eine zentrale skalierbare Management-Lösung mit Blick auf das gesamte Security-Ökosystem.

Das **Capture Security Center** (CSC) bietet eine zentrale funktionsreiche Benutzeroberfläche für den Zugriff auf alles, was Sie für ein allumfassendes Security-Management brauchen, einschließlich Analytics und Reporting für Netzwerk-, WLAN-, E-Mail-, Endpunkt- und Cloud-Sicherheit, Risk Meters und Asset Management.

Das CSC ist eine SaaS-Lösung, die 360° Sicht auf Ihr gesamtes SonicWall Security-Ökosystem und erhöhte Agilität ermöglicht. Aufgrund der funktionalen Integration sorgt diese Lösung für mehr Effizienz und betriebliche Elastizität und ist über eine zentrale Benutzeroberfläche verwaltbar. Anhand detaillierter Berichte und leistungsstarker Analysen können Sie überall und auf allen webfähigen Geräten schnell bzw. in Echtzeit informierte Entscheidungen in Bezug auf Bedrohungen treffen.

Das CSC unterstützt auch Ihre allgemeine Cyberabwehrstrategie, da es mit den Service-Level-Anforderungen von Security Operation Centers (SOCs) konform ist. Es sorgt für eine abgestimmte Security-Governance-Compliance und unterstützt viele andere Risikomanagementstrategien – alles von einer webfähigen Anwendung aus.

Capture Security Center ist eine wahre SPOG-Anwendung und ganzheitliche, integrierte Management-Lösung. Das CSC ist im Lieferumfang der meisten SonicWall Firewalls und Cloud-Dienste enthalten.

Erhöhen Sie Ihre Effizienz und betriebliche Flexibilität

Steigern Sie Ihre Effektivität. Arbeiten Sie schneller und intelligenter mit weniger Aufwand.

CAPTURE SECURITY CENTER IST EFFIZIENTER

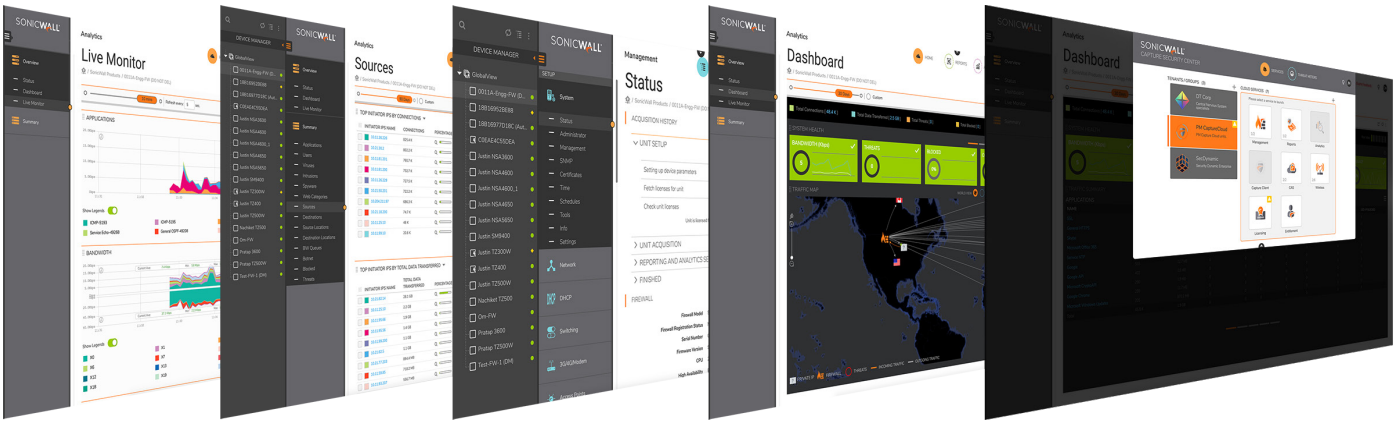
Erweiterte Sicht durch eine SPOG-Konsole. Sie erhalten totale Transparenz Ihrer Security-Infrastruktur und Ihres Netzwerkes und sehen alles, von der Architektur bis zu Cyberbedrohungen und Konformitätsproblemen.

CSC ist ein Management- und Produktivitätstool mit integrierter Skalierbarkeit und optimierter Koordination der Managementfunktionen

SSO gibt Einblick in jeden betrieblichen Aspekt Ihres Netzwerkes – von der Cloud-Security bis hin zu jedem Endpunkt. Die Cloud-native Benutzeroberfläche gibt Ihnen „ein Fenster“, durch das Sie alles sehen können. Alle Aufgaben lassen sich einfacher und effektiver durchführen.

Der Zeit- und Kostenaufwand für alltägliche Aufgaben wird reduziert. Unnötige Security-Silos werden eliminiert und bei allen wichtigen Arbeitsabläufen wird durch „Sehen-und-Klicken“-Funktionalität für erhöhte Effizienz gesorgt. Neue Fähigkeiten können sofort nach deren Einführung genutzt werden.

Der gesamte SonicWall Security-Stack lässt sich von einer zentralen Stelle aus verwalten. Sicherheitslücken und Risiken werden durch Risk Meters und präzise Analysen identifiziert. Durch die Verfügbarkeit zeitkritischer Bedrohungsdaten und sofortigen Einblick in die Situation kann schneller reagiert werden. Mittels Zero-Touch Deployment wird der Verwaltungsablauf vereinfacht, Konfigurationsfehler und menschliche Fehler werden vermieden und Remote-Firewalls, Switches und Access Points in Filialen können auf leichte Weise bereitgestellt werden.



Die Cloud-native Benutzeroberfläche sorgt für mehr Effizienz und betriebliche Flexibilität. Security-Silos werden reduziert und die Produktivität im gesamten Security-Umfeld wird gesteigert – alles von einer einzigen Anwendung aus.

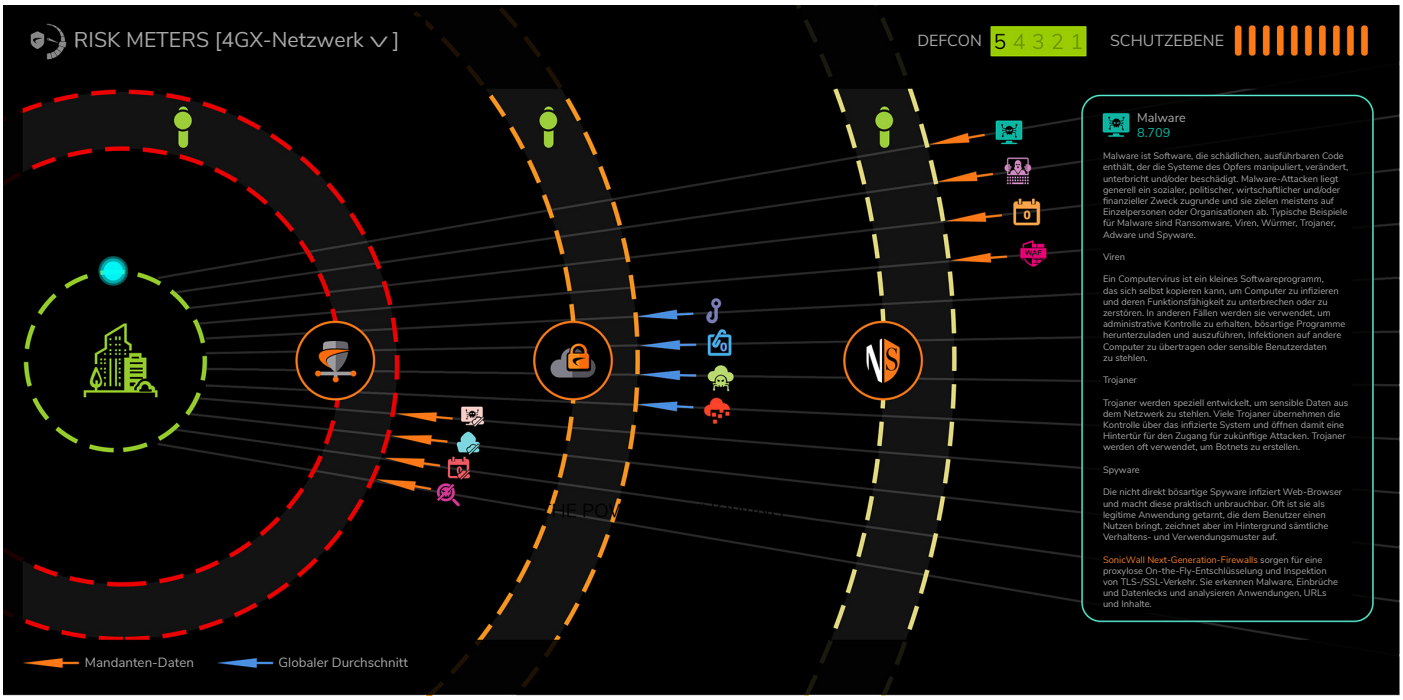
SONICWALL

Synchronisierte Cyberthreat-Daten für Ihr gesamtes Netzwerk

Sorgen Sie für Sicherheit. Untersuchen Sie Risiken und Bedrohungen in Echtzeit unter Verwendung von Daten aus der Praxis.

CAPTURE SECURITY CENTER BIETET MEHR THREAT-INTELLIGENCE

Durch aktuellste Cyber-Threat-Intelligence können bedarfsspezifische Daten auf Basis des vorliegenden Zustands Ihrer Security-Assets zusammengeführt werden. Verteidigen Sie Ihr Netzwerk unter Verwendung von Risikodaten aus der Praxis in Echtzeit.



Risk Meters zeigen automatisch Bedrohungsdaten und Risikoscores auf, die auf Live-Threat-Daten beruhen und mit dem vorliegenden Schutzgrad verglichen werden. Lücken in den Abwehrschichten werden aufgedeckt und Sie können Sicherheitsentscheidungen in Echtzeit treffen. Sicherheitsplanung, Richtlinien- und Budgetentscheidungen basieren auf logischen Bewertungen.

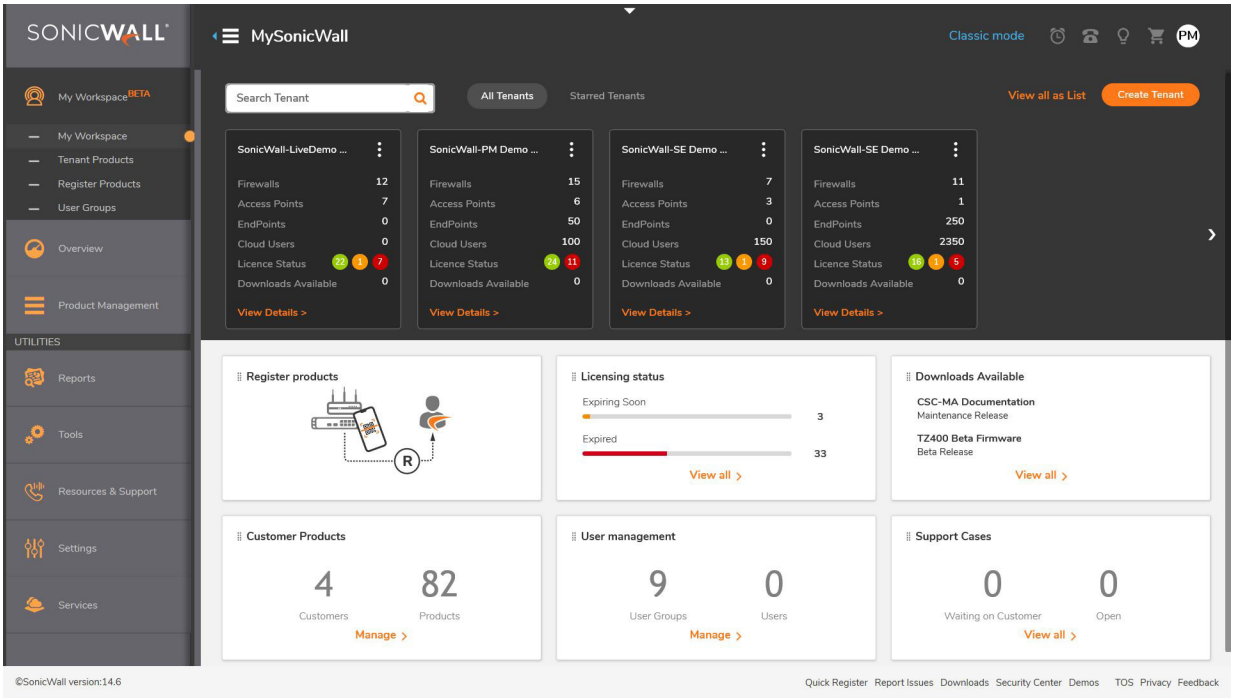
Mit **SonicWall Risk Meters** können Sie Ihre Security-Bewertung auf Basis der spezifischen Anforderungen Ihrer Netzwerkinfrastruktur anpassen. Alle Bedrohungen in Ihrem Netzwerk werden in einer grafikgestützten Echtzeit-Analyse dargestellt. Diese integrierte Funktion gibt Ihren Security-Teams Einblick in die Bedrohungsvektoren und ermöglicht die Identifizierung der besten Abwehrmethode zum Schutz des Netzwerks. Sie können genau beobachten, wie Bedrohungen vom Web, von der Cloud, aus Anwendungen, Endpunkten, Mobilgeräten, Datenbanken und IoT Ihr Netzwerk ansteuern. Sie können potenzielle Sicherheitslücken visualisieren, eingehende Attacken erkennen, alle potenziellen Quellen einschließlich Dienste von Dritten überwachen und Abwehrmaßnahmen ergreifen. Durch die Visualisierung des Geschehens in Echtzeit können unvorhergesehene Attacken eliminiert und die Netzwerksicherheit gestärkt werden.

Reibungslose Verwaltung von Sicherheitseinrichtungen

Behalten Sie die Kontrolle. Führen Sie alle Sicherheitsarbeiten von einer zentralen Stelle aus durch.

CAPTURE SECURITY CENTER FÜR EINE ALLUMFASSENDE KONTROLLE

Sie erhalten wertvolle Einsichten in Ihre Sicherheitsumfelder, die alle auf einen Blick überschaubar sind. Dadurch werden Verwaltungs- und Kundenabläufe vereinfacht, Entscheidungsfindungen beschleunigt, Supportleistungen optimiert und Sicherheitslücken geschlossen.



My Workspace ist über das Capture Security Center unter MySonicWall zugänglich und ermöglicht die Durchführung komplexer Sicherheitsoperationen auf eine einfachere und effizientere Weise. Der Arbeitsfluss wird systematisch optimiert für ein leichtes und schnelles Onboarding, Einrichten und Verwalten von mehreren Mandanten in verschiedenen Campus-Anlagen, Filialen oder Funktionsgruppen. Zugleich können große Mengen an Produktregistrierungen, Lizenzaktivierungen und Supportaktivitäten abgewickelt und Produktprobeversionen auf On-Demand-Basis aktiviert werden.

Mandanten-Workflows bieten sofortigen Zugang zu unternehmensübergreifenden Security-Operations-Teams und eine granulare, rollenbasierte Zugangskontrolle für alle im Capture Security Center verwalteten Produkte. Das intuitive Dashboard sorgt für sofortige Transparenz und macht auf Produkte aufmerksam, deren Lizenzen abgelaufen sind oder deren Software/Firmware aktualisiert werden muss. Das integrierte Self-Service-Portal ermöglicht die Kontaktaufnahme, Zusammenarbeit und Kommunikation mit Mandanten, um die Lösung und Verfolgung von Problemen zu erleichtern und bei Bedarf Unterstützung bereitzustellen.

Die CSC-Funktionen im Überblick

Verwaltung

- Zentraler Zugang zu den meisten Funktionen
- Mehrere gleichzeitige Benutzersitzungen
- Zentralisiertes Sicherheits- und Netzwerkmanagement
- Universelles Dashboard
- Firewall-Management
- SonicWall Switch-Management
- WLAN-Management
- Föderierte Richtlinienkonfiguration
- Festlegung von Richtlinien auf Gruppenebene
- Richtlinienreplikation von einem Gerät auf eine Gruppe von Geräten
- Management und Workflow von Änderungsanweisungen
- Zero-Touch-Deployment
- Mittels Zero-Touch bereitgestellte Gerätekonfigurationen
- VPN-Implementierung und -Konfiguration
- Active-Device-Überwachung mit Warnmeldungen
- Anwendungsvisualisierung und Intelligenz
- APIs, CLI und SNMP-Unterstützung
- Capture Client Management
- Cloud App Security Management
- Hosted Email Security Management
- MySonicWall und MyWorkspace
- Risk Meters
- Security Center
- Cloud App Security – Schatten-IT
- Lizenzverwaltung
- Rollenbasiertes Management (Benutzer, Gruppen)
- Sicherung der Einstellungsdateien für die Firewall-Appliance

Überwachung

- Device-Überwachung mit Warnmeldungen
- IPFIX-Datenfluss in Echtzeit
- Active-Device-Überwachung mit Warnmeldungen
- SNMP-Relay-Management
- VPN- und Firewallstatus-Überwachung
- Risk Meters

Reporting

- Zentrale Firewall-Protokollierung
- Syslog- oder IPFIX-basierte Berichte
- Personalisierte zeitlich gesteuerte PDF-Berichte
- Multi-Threat-Reporting
- Benutzerzentrisches Reporting
- Anwendungsnutzung-Reporting
- Botnet-Bericht
- Geo IP-Bericht
- MAC-Adressen-Bericht
- Capture ATP-Bericht
- Bericht über bösartige Wireless-Access-Points
- Cloud App Security (CAS) Reporting
- Capture Client-Reporting
- Bandbreiten- und Services-Bericht nach Schnittstelle

Analytics

- Benutzerbasierte Analysen
- Anwendungsnutzungs-Reporting
- Produktübergreifende Transparenz mit Capture Client
- Dynamische Visualisierung in Echtzeit
- Drilldown- und Pivoting-Funktionen

Lizenzierung und Pakete

Die Cloud-basierten Dienste sind in den folgenden Paketzusammenstellungen erhältlich.

1. CSC Basic Management (Lite)

Diese Version eignet sich ideal für Backup/Wiederherstellung des Firewall-Systems oder deren Einstellungen und für Firmware-Upgrades. Bei jeder Firewall mit AGSS- oder CGSS-Abo kann diese grundlegende Managmentfunktion aktiviert werden, um die Firewall-Verwaltung zu erleichtern.

2. CSC Management

Mit diesem bezahlten Abo werden alle Managementfunktionen aktiviert, einschließlich Workflow-Automatisierung und Zero-Touch-Deployment-Funktionen.

3. CSC Management und Reporting

Diese Lizenzoption eignet sich ideal für größere Einrichtungen mit vielen Firewalls an geografisch weit verstreuten Standorten, die unter Gruppenebenen- oder Mandanten-Management betrieben werden. Dazu gehören mittelgroße Betriebe, weit verbreitete Großunternehmen, Organisationen des öffentlichen Dienstes und Bildungseinrichtungen, Organisationen mit vielen Bezirken und Campusanlagen sowie Managed-Service-Providern (MSPs).

Neben den umfassenden Managementfunktionen bietet diese Abo-Option auch komplette Reportingfunktionen für periodische oder bei Bedarf durchgeführte Sicherheits- und Netzwerksleistungsprüfungen und Audits. Diese können über das interaktive universelle Dashboard online mittels Live-Diagrammen und Tabellen oder offline mittels terminierter exportierter Berichte durchgeführt werden.

4. CSC Analytics

Dieser leistungsstarker Add-On-Service ist in allen Capture Security Center-Abo-Optionen enthalten. Bei aktiviertem Service erhalten Sie vollen Zugang zu SonicWall Analytics und SonicWall Cloud App Security Tools und Services für die Durchführung von Netzwerk-Forensik und Threat-Hunting unter Verwendung umfassender Drilldown- und Pivoting-Funktionen. CSC Analytics beinhaltet auch eine 30-tägige Speicherung der Rollover-Protokolle und 365 Tage Reporting.

Unterstützte Firewall-Modelle

Capture Security Center ist verfügbar für Kunden mit SOHO-W, SOHO 250, SOHO 250W, TZ Series, NSA Series, NSa 2650-6650 und NSv Series Firewalls. Für SuperMassive 9000 Series, NSa Series und NSsp 12400 bis 12800 wird das CSC Management-Abo im Rahmen der entsprechenden AGSS-Abo-Aktivierung automatisch aktiviert.

CAPTURE SECURITY CENTER			
	Verwaltung	Reporting[4]	Analytics[4]
Einstiegslevel FW	SOHO-W, SOHO 250, SOHO 250W TZ Series, NSv 10-100	SOHO-W, SOHO 250, SOHO 250W, TZ Series, NSv 10-100	SOHO-W, SOHO 250, SOHO 250W, TZ Series, NSv 10-100
Mid-range FW	NSA Series, NSa Series, NSv 200-400	NSA Series, NSa Series, NSv 200-400	NSA Series, NSa Series, NSv 200-400
High-end FW	SuperMassive 9000 Series, NSsp 12000 Series, NSa 9250-9650, NSv 800-1600	SuperMassive 9000 Series, NSsp 12000 Series, NSa 9250-9650, NSv 800-1600	SuperMassive 9000 Series, NSsp 12000 Series, NSa 9250-9650, NSv 800-1600

[4] *Unterstützung von Reporting und Analytics für High-end FW ist nur bei On_prem Analytics verfügbar.*

	Funktionen	CSC Management Lite	CSC Management	CSC Management und Reporting	SaaS Analytics	On Premises Analytics
Verwaltung	Backup/Wiederherstellung – Firewallsystem	Ja	Ja	Ja	Ja	Ja[2]
	Backup/Wiederherstellung – Firewalleinstellungen	Ja	Ja	Ja	Ja	Ja[2]
	Firmware-Upgrade	Nur von einer lokalen Datei	Nur von einer lokalen Datei oder von MySonicWall	Ja	Nur von einer lokalen Datei	Nur von einer lokalen Datei[3]
	Aufgabenterminierung	-	Ja	Ja	-	-
	Gruppen-Firewall-Verwaltung	-	Ja	Ja	-	-
	Vererbung – vorwärts/ rückwärts gerichtet	-	Ja	Ja	-	-
	Zero-Touch-Deployment[1]	-	Ja	Ja	-	-
	Offline-Download der Firewall-Signatur	-	Ja	Ja	-	-
	Workflow	-	Ja	Ja	-	-
	Gepoolte Lizenzen – Suche, Freigabe, Bestandsaufnahme von gebrauchten Aktivierungscodes	-	Ja	Ja	-	-
Reporting (Netflow/ IPFIX-basiert)	Terminieren von Berichten, Live-Überwachung, Zusammenfassungs-Dashboards	-	-	Ja	Ja	Ja
	Herunterladen von Berichten: Anwendungen, Bedrohungen, CFS, Benutzer, Verkehr, Ursprung/ Ziel (1 Jahr Fluss-Reporting)	-	-	Ja	Ja	Ja
Analytics (Netflow/ IPFIX-basiert)	Netzwerk-Forensik und Threat-Hunting unter Verwendung von Drilldown und Pivots	-	-	-	Ja	Ja
	Cloud App Security – Schatten-IT	-	-	-	Ja	Nein
	Datenaufbewahrung	-	-	-	30 Tage Aufbewahrung der Verkehrsdaten	1 Jahr
Technischer Support		Nur Web-Fälle	24x7-Unterstützung	24x7-Unterstützung	24x7-Unterstützung	24x7-Unterstützung

[1] *Unterstützung für SOHO-W mit Firmware 6.5.2+; TZ, NSA Series und NSa 2650- 6650 mit Firmware 6.5.1.1+. Keine Unterstützung für SOHO oder NSv Series.*
[2] *Erfordert AGSS/CGSS Service oder einen bezahlten Capture Security Center Service.*
[3] *Erfordert eine 24/7 Support-Lizenz.*

Bestellinformationen

Produkt	Artikelnummer
SonicWall Capture Security Center Management für TZ Series, SOHO-W, SOHO 250, SOHO 250W, NSv 10 bis 100, 1 Jahr	01-SSC-3664
SonicWall Capture Security Center Management für TZ Series, SOHO-W, SOHO 250, SOHO 250W, NSv 10 bis 100, 2 Jahre	01-SSC-9151
SonicWall Capture Security Center Management für TZ Series, SOHO-W, SOHO 250, SOHO 250W, NSv 10 bis 100, 3 Jahre	01-SSC-9152
SonicWall Capture Security Center Management für NSA 2600 bis 6600, NSa 2650 bis 6650 und NSv 200 bis 400, 1 Jahr	01-SSC-3665
SonicWall Capture Security Center Management für NSA 2600 bis 6600, NSa 2650 bis 6650 und NSv 200 bis 400, 2 Jahre	01-SSC-9214
SonicWall Capture Security Center Management für NSA 2600 bis 6600, NSa 2650 bis 6650 und NSv 200 bis 400, 3 Jahre	01-SSC-9215
SonicWall Capture Security Center Management und Reporting für TZ Series, SOHO-W, SOHO 250, SOHO250W, NSv 10 bis 100, 1 Jahr	01-SSC-3435
SonicWall Capture Security Center Management und Reporting für TZ Series, SOHO-W, SOHO 250, SOHO250W, NSv 10 bis 100, 2 Jahre	01-SSC-9148
SonicWall Capture Security Center Management und Reporting für TZ Series, SOHO-W, SOHO 250, SOHO250W, NSv 10 bis 100, 3 Jahre	01-SSC-9149
SonicWall Capture Security Center Management und Reporting für NSA 2600 bis 6600, NSa 2650 bis 6650 und NSv 200 bis 400, 1 Jahr	01-SSC-3879
SonicWall Capture Security Center Management und Reporting für NSA 2600 bis 6600, NSa 2650 bis 6650 und NSv 200 bis 400, 2 Jahre	01-SSC-9154
SonicWall Capture Security Center Management und Reporting für NSA 2600 bis 6600, NSa 2650 bis 6650 und NSv 200 bis 400, 3 Jahre	01-SSC-9202
SonicWall Capture Security Center Analytics für SOHO-W, SOHO 250, SOHO250W, TZ Series, NSv 10 bis 100, 1 Jahr	02-SSC-0171
SonicWall Capture Security Center Analytics für NSA 2600 bis 6600, NSa 2650 bis 6650 und NSv 200 bis 400, 1 Jahr	02-SSC-0391

Internet Browser

- Microsoft® Internet Explorer 11.0 oder höher (nicht den Kompatibilitätsmodus verwenden)
- Mozilla Firefox 37.0 oder höher
- Google Chrome 42.0 oder höher
- Safari (neueste Version)

Im Capture Security Center verwaltete unterstützte SonicWall Appliances

- SonicWall Network Security Appliances: SuperMassive E10000 und 9000 Series, E-Class NSA, NSsp Series, NSa Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- SonicWall Network Security Virtual Appliances: NSv Series
- SonicWall Endpoint Security – Capture Client
- SonicWall Cloud Security – Cloud App Security (CAS)
- SonicWall Email Security
- SonicWall Web Application Firewall
- SonicWall Secure Mobile Access: SMA 100 Series

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, USA
Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com

Datasheet-CaptureSecurityCenter-US-COG-2315

SONICWALL®