SONICWALL CAPTURE SECURITY CENTER

Cloudbasierte Management-, Reporting- und Analyselösung für die Netzwerk-, Endgeräte- und Cloudsicherheit

SonicWall Capture Security Center ist eine offene und skalierbare cloudbasierte Sicherheitsmanagementsoftware, die als kostengünstiger Service bereitgestellt wird. Unternehmen und Serviceprovider unterschiedlicher Größen und Anwendungsszenarien können damit das gesamte Security-Ökosystem von SonicWall zentral steuern. Sie erhalten Einblick in alle sicherheitsrelevanten Aspekte und profitieren von einer flexiblen, leistungsstarken Lösung, die sich einfach, präzise und schnell bedienen lässt. Alle Security-Services und Managementtools von SonicWall sind in dieser cloud- und serviceorientierten Architektur zusammengefasst. Das verbessert nicht nur die Effizienz und Flexibilität, sondern ermöglicht auch eine breiter angelegte Cyber-Abwehrstrategie.

Capture Security Center nutzt Geschäftsprozesse und Service-Level-Definitionen, um in Security Operation Centers (SOCs) die Grundlage für eine einheitliche Security-Governance-, Compliance- und Risikomanagementstrategie zu legen. Dabei setzt es auf eine ganzheitliche Orchestrierung der Sicherheitsinfrastruktur und führt alle operativen Aspekte der Netzwerk-, Endgeräte- und Cloudsicherheit in einem einfachen, allgemeingültigen Management-Framework zusammen. Aufgaben lassen sich einfacher erledigen und in vielen Fällen automatisieren, um die Komplexität, den Zeitaufwand und die Kosten für Sicherheitsprozesse und deren Administration zu reduzieren. Neben Firewall- und Endgeräte-Provisioning gehören dazu auch Konfiguration, Monitoring, Reporting, Patching, Auditing sowie die Datenverkehrs- und Datenanalyse, die für die vorbeugende Identifizierung und Reaktion auf Sicherheitsprobleme unerlässlich ist.

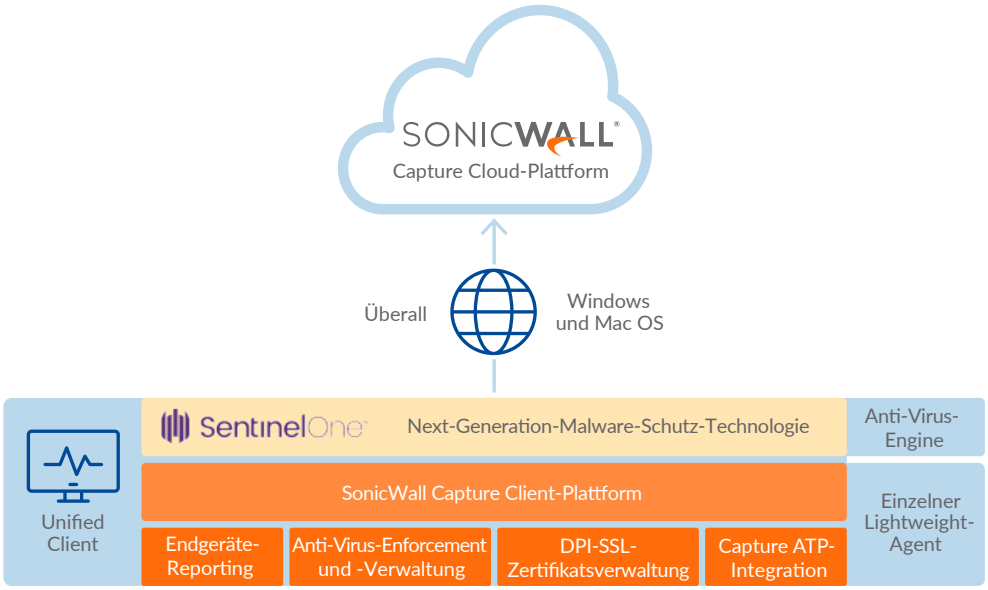
Vorteile:

- Einheitliches Sicherheitsprogramm für Security-Governance, Compliance und Risikomanagement
- Integrationsfähige Managementkonsole für all Ihre SonicWall-Lösungen
- Sicherheits-Compliance und fehlerfreies Richtlinienmanagement durch automatisierte Workflows
- Einfache und vollautomatische Remote-Implementierung und -Bereitstellung von SonicWall-Firewalls
- Zentrale Übersicht und situativ angepasste Informationen zur Sicherheitsumgebung des Netzwerks
- Umfassende investigative und forensische Analyse angereicherter Sicherheitsdaten
- Verkürzte Reaktionszeiten bei Vorfällen durch aussagekräftige Echtzeitdaten zu Bedrohungen

Capture Security Center unterstützt eine Single-Sign-on-Anmeldung zur Lizenzierung, Bereitstellung und Verwaltung aller Netzwerk-, Endgeräte- und Cloud-Security-Services, wie Firewall Management, Analytics, Capture Client and Cloud Application Security. Unser Ziel ist es, das gesamte SonicWall Security-Portfolio unter einem Managementdach zusammenzufassen, das einfache Integrationsmöglichkeiten und Sicherheitsservices für Web, Wireless, E-Mail, Mobilgeräte und IoT bietet.[1] All diese Cloudservices greifen ineinander und ergeben eine mehrstufige Sicherheitslösung, die aus Cyber Defense, Threat Intelligence, Kollaboration sowie einheitlichen Management-, Reporting- und Analysefunktionen besteht. Ein Aboservice mit Software-Updates und Support sorgt dafür, dass immer die neuesten Innovationen und Verbesserungen bereitstehen. So ist es einfacher, Sicherheitsrisiken abzubauen, aufsichtsbehördliche Auflagen zu erfüllen und sich gegen aktuelle Sicherheitsschwachstellen und Bedrohungen zu wappnen. Capture Security Center bietet aber auch uneingeschränkte Skalierbarkeit und Flexibilität. Zudem lassen sich Leistung und Kapazität jederzeit gemäß den geschäftlichen Anforderungen anpassen.

Capture Client

Der Capture Security Center umfasst unter anderem den SonicWall Capture Client, eine einheitliche Clientplattform, die verschiedene Funktionen zum Schutz von Endgeräten bereitstellt. Capture Client setzt mit seiner Next-Generation Malware-Engine von SentinelOne auf hochentwickelte Technologien wie maschinelles Lernen und System-Rollback zum Schutz vor raffinierten Bedrohungen. Dies bietet Schutz vor dateibasierten oder dateilosen Malware-Attacken und gewährleistet eine 360-Grad-Sicht auf Angriffe sowie Echtzeitinformationen, die für Untersuchungszwecke eingesetzt werden können. Durch das Management von vertrauenswürdigen SSL-Zertifikaten, die zur Deep Packet Inspection von SSL-/TLS-Datenverkehr herangezogen werden, liefert Capture Client in Verbindung mit den SonicWall Firewalls Informationen zum verschlüsseltem Datenverkehr.



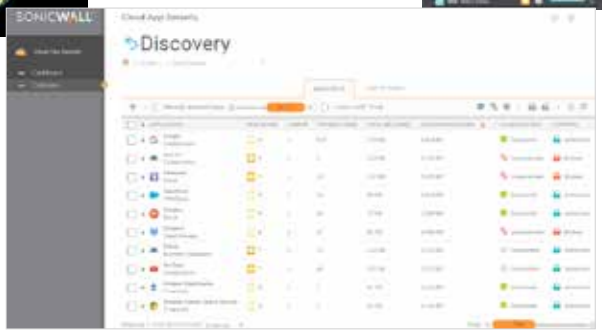
[1] *Sicherheitsservices für Web, Wireless, E-Mail, Mobilgeräte und IoT werden in zukünftigen Produktankündigungen in diese Plattform integriert.*

Cloud App Security

Das SonicWall Capture Security Center Analytics-Abopaket verschafft Kunden Einblicke in ihre Schatten-IT und erleichtert die Kontrolle ihrer Cloudanwendungen. SonicWall Cloud App Security stellt CASB-ähnliche Funktionalität bereit. Administratoren erhalten Einblick in die Nutzung risikoreicher Anwendungen, können Benutzeraktivitäten überwachen und auf verwalteten Firewalls Richtlinien zur Blockierung und Freigabe von IT-Anwendungen festlegen, um sensible Daten zu schützen.

Zu den wesentlichen Aufgaben des Cloud App Security-Service gehört die Ermittlung von Schatten-IT, die Bereitstellung von Echtzeitinformationen und die Klassifizierung und Steuerung von Anwendungen. Der Service ermöglicht die sichere Einführung von SaaS-Anwendungen bei voller Mitarbeiterproduktivität und zu geringen TCO.

1. **Aufspüren von Schatten-IT:** Anhand vorhandener Firewall-Protokolldateien wird die Cloud-Discovery automatisiert, um die verwendeten Anwendungen und deren Risikoprofil zu identifizieren.
2. **Anwendungstransparenz in Echtzeit:** Ein intuitives Dashboard liefert Echtzeitinformationen zur Anwendungsnutzung mit Angaben zu Datenverkehrsvolumen, Nutzeraktivität und Nutzungsort.
3. **Klassifizierung und Steuerung von Anwendungen:** Unverwaltete Cloudanwendungen werden als "zugelassene Apps" (durch die IT genehmigt) oder "nicht zugelassene Apps" (nicht von der IT genehmigt) klassifiziert. Abhängig von der Risikobewertung der Anwendung werden Blockierungs- und Freigaberegeln erstellt.



SONICWALL

Workflow-Automatisierung

Durch die native Workflow-Automatisierung hilft das Capture Security Center SOCs dabei, die Anforderungen verschiedener gesetzlicher Vorgaben wie PCI, HIPPA und DSGVO an das Auditing und die Verwaltung von Regeländerungen an der Firewall einzuhalten. Es ermöglicht Regeländerungen durch den Einsatz konsequenter Verfahren beim Konfigurieren, Abgleichen, Validieren, Prüfen und Freigeben von Firewall-Regeln vor der Implementierung. Die Freigabegruppen sind flexibel und erlauben die Einhaltung verschiedener Autorisierungs- und Auditverfahren in unterschiedlichen Organisationen. Bei der Workflow-Automatisierung werden freigegebene Sicherheitsregeln programmseitig implementiert, um die operative Effizienz zu verbessern, Risiken zu mindern und Fehler zu vermeiden.

Capture Security Center bietet einen ganzheitlichen Ansatz für Security-Governance, Compliance und Risikomanagement.

1. KONFIGURATION UND VERGLEICH

Capture Security Center konfiguriert **Aufträge für Regeländerungen** und **markiert Abweichungen farblich** für einen klaren Vergleich.

2. VALIDIERUNG

Capture Security Center prüft **die Integrität der Regellogik**.

3. PRÜFUNG UND GENEHMIGUNG

Capture Security Center sendet eine E-Mail an Reviewer und **protokolliert den Audit-Trail (Genehmigung/Ablehnung)** der Regel.

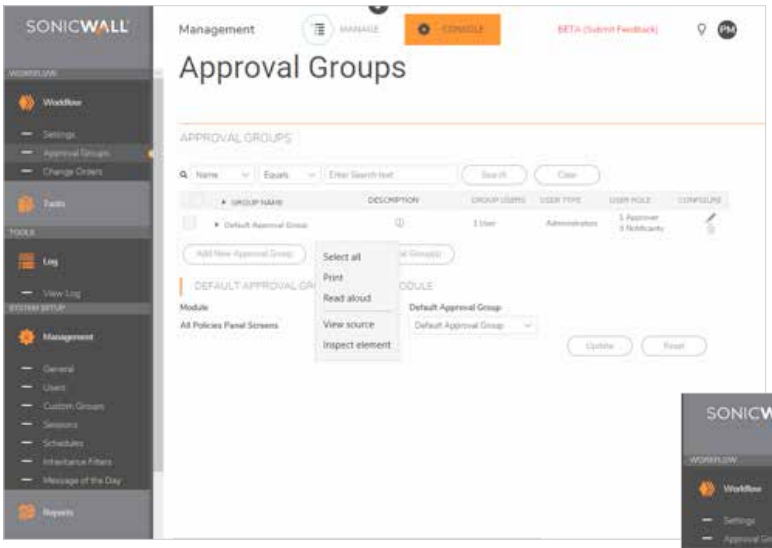
4. IMPLEMENTIERUNG

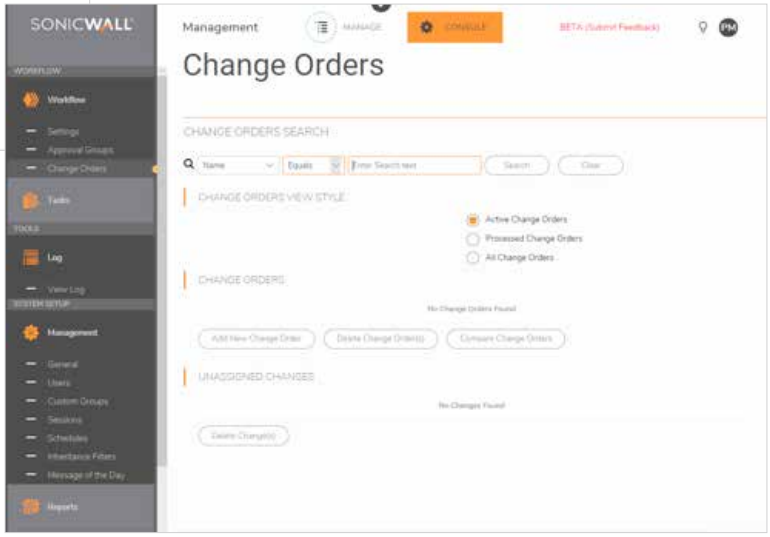
Capture Security Center implementiert die Regeländerungen sofort oder **nach einem festen Zeitplan**.

5. AUDIT

Die Änderungsprotokolle ermöglichen eine genaue **Prüfung** der Regeln und akkurate **Compliance**-Daten.

Workflow-Automatisierung: Vier Schritte für einen fehlerfreies Regelmanagement





SONICWALL®

Vollautomatische Bereitstellung

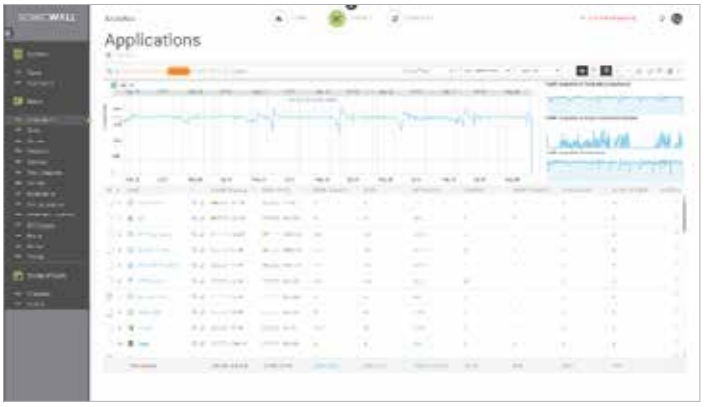
Die vollautomatische Bereitstellung ist als Service in Capture Security Center integriert und vereinfacht und beschleunigt den Bereitstellungsprozess für SonicWall-Firewalls in Niederlassungen und Remote-Standorten. Der Prozess erfordert minimalen Benutzereingriff und ist vollständig automatisiert, sodass eine große Anzahl von Firewalls in vier einfachen Bereitstellungsschritten in Betrieb genommen werden können. Dadurch werden Zeitaufwand, Kosten und Komplexität der Installation und Konfiguration erheblich reduziert, während die Sicherheit und die Konnektivität umgehend und automatisch zur Verfügung stehen.

SCHRITT 1	**FIREWALL REGISTRIEREN** Die neue Firewall wird mit der zugewiesenen Seriennummer und dem Authentifizierungscode in MySonicWall registriert.
SCHRITT 2	**FIREWALL VERBINDEN** Die Firewall wird über das mitgelieferte Ethernetkabel mit dem Netzwerk verbunden.
SCHRITT 3	**FIREWALL EINSCHALTEN** Die Firewall wird mit dem Netzkabel an das Stromnetz angeschlossen und eingeschaltet. Das Gerät erhält eine vom DHCP-Server automatisch zugewiesene WAN-IP. Sobald die Verbindung hergestellt wurde, wird das Gerät automatisch erkannt, authentifiziert und im Capture Security Center hinzugefügt. Alle Lizenzen und Konfigurationen werden mit MySonicWall und License Manager synchronisiert.
SCHRITT 4	**FIREWALL VERWALTEN** Das Gerät ist jetzt betriebsbereit und kann über die cloudbasierte zentrale Managementkonsole von Capture Security Center verwaltet werden. Dies umfasst Firmware-Upgrades, Sicherheitspatches und Konfigurationsänderungen auf Gruppenebene.

Vollautomatische Bereitstellung: Inbetriebnahme der Firewall in vier einfachen Schritten

Reporting

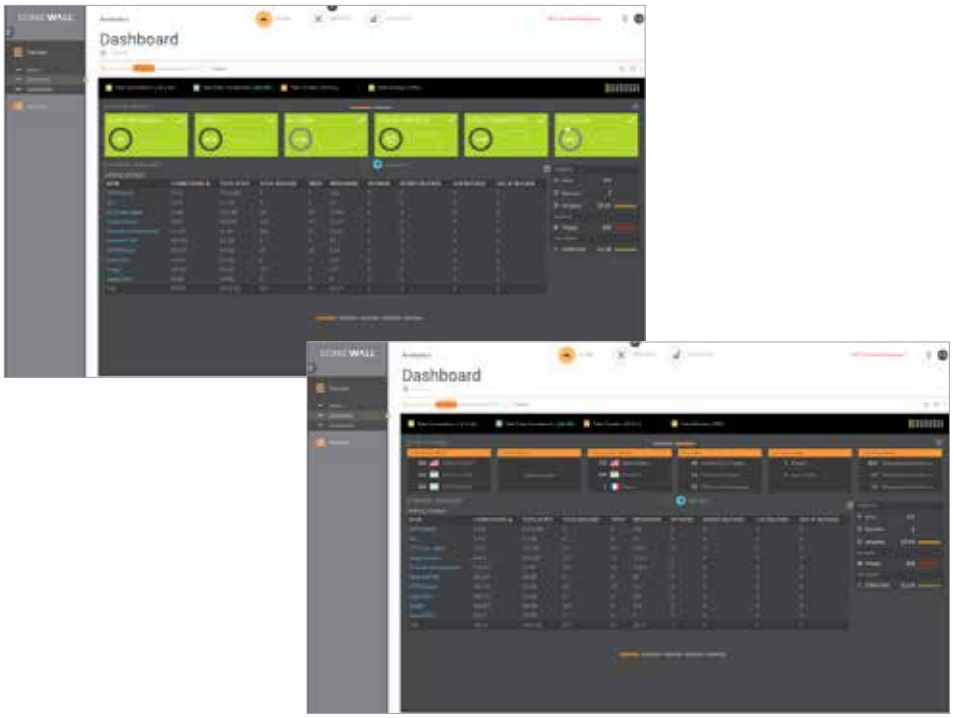
Das Capture Security Center bietet neben mehr als 140 vordefinierten Berichten auch die Möglichkeit, individuelle Berichte zu erstellen und dabei die auditierbaren Daten beliebig zu kombinieren. So können die gewünschten Anwendungsfälle durchgespielt werden. Die Ergebnisse umfassen einen Gesamt- und Detailüberblick über Netzwerkereignisse, Benutzeraktivitäten, Bedrohungen, Prozess- und Performanceprobleme, Sicherheitseffektivität, Risiken und Sicherheitslücken, Compliance Readiness und sogar Post-mortem-Analysen. In sämtliche Berichte fließt der kollektive Input aus vielen Jahren Zusammenarbeit zwischen SonicWall und seinen Kunden und Partnern ein. Dies liefert Organisationen äußerst detaillierte Einblicke, Anwendungsmöglichkeiten und Kenntnisse zu den Syslog- und IPFIX/NetFlow-Daten, die SOCs zum Nachverfolgen, Messen und Durchführen effektiver Netzwerk- und Sicherheitsprozesse benötigen.

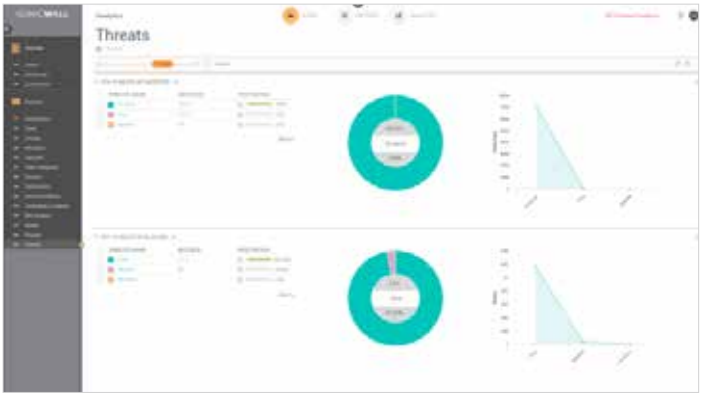


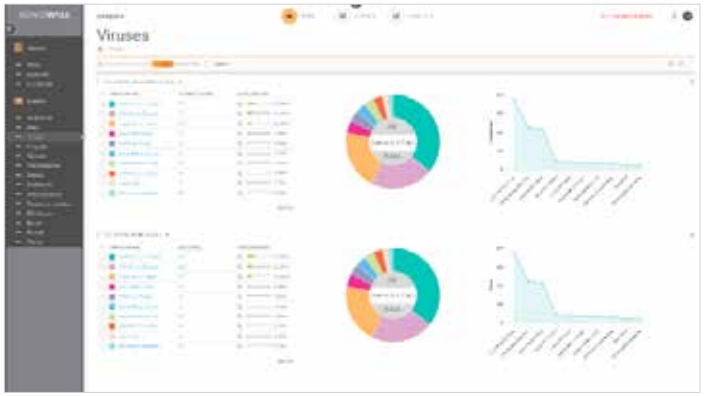
Analytics

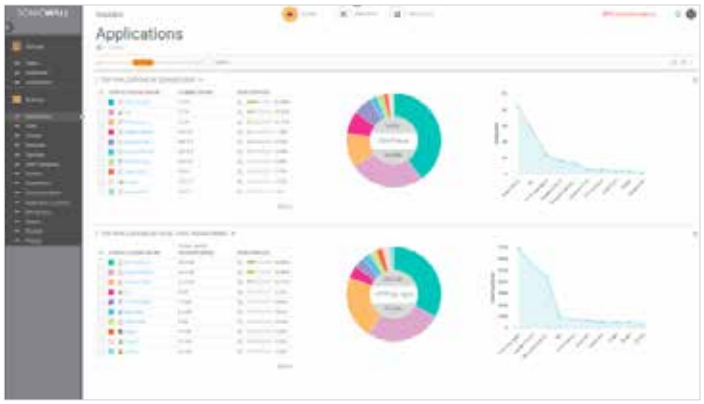
Als informationsgestützte Big Data-Analyse-Engine automatisiert SonicWall Analytics die Aggregierung, Normalisierung, Korrelation und Kontextualisierung der Sicherheitsdaten über alle verwalteten Firewalls hinweg. Dadurch erhalten Unternehmen Echtzeiteinblicke in sämtliche Netzwerkvorgänge. Anhand der Ergebnisse, die in einer strukturierten, sinnvollen, verwertbaren und einfach zu nutzenden Weise dargestellt werden, können Sicherheitsexperten, Analysten, Auditoren, Führungskräfte, Vorstandsmitglieder und Stakeholder Erkenntnisse gewinnen und interpretieren, Prioritäten setzen, Entscheidungen treffen und angemessene Schutz- und Korrekturmaßnahmen ergreifen.

Analytics bietet Echtzeitvisualisierung, Überwachung und Warnmeldungen zu angereicherten Sicherheitsdaten in einer einzigen Lösung. Mit den leistungsstarken Tools der Engine erhalten Kunden die vollständige Kontrolle, Agilität und Flexibilität, um umfassende investigative Drill-down-Analysen des Netzwerkverkehrs sowie der Benutzeraktivitäten, Sicherheitsereignisse, Bedrohungsprofile, Anwendungsnutzung und einer Reihe weiterer kontextbasierter Firewall-Daten durchzuführen. Diese tiefgehenden Informationen zur Sicherheitsumgebung sorgen für eine umfassende Transparenz und bieten Kunden die Möglichkeit, Sicherheitsrisiken nicht nur zu erkennen, sondern entsprechende Korrekturmaßnahmen einzuleiten und die Ergebnisse gezielt und schnell zu überwachen und nachzuverfolgen. Mit Analytics können Kunden Sicherheitsanalysefunktionen implementieren und in Geschäftsprozesse integrieren, um Daten in Informationen, Informationen in Wissen und Wissen in Entscheidungen umzuwandeln, die eine vollständige Automatisierung der Sicherheitsfunktionen ermöglichen.







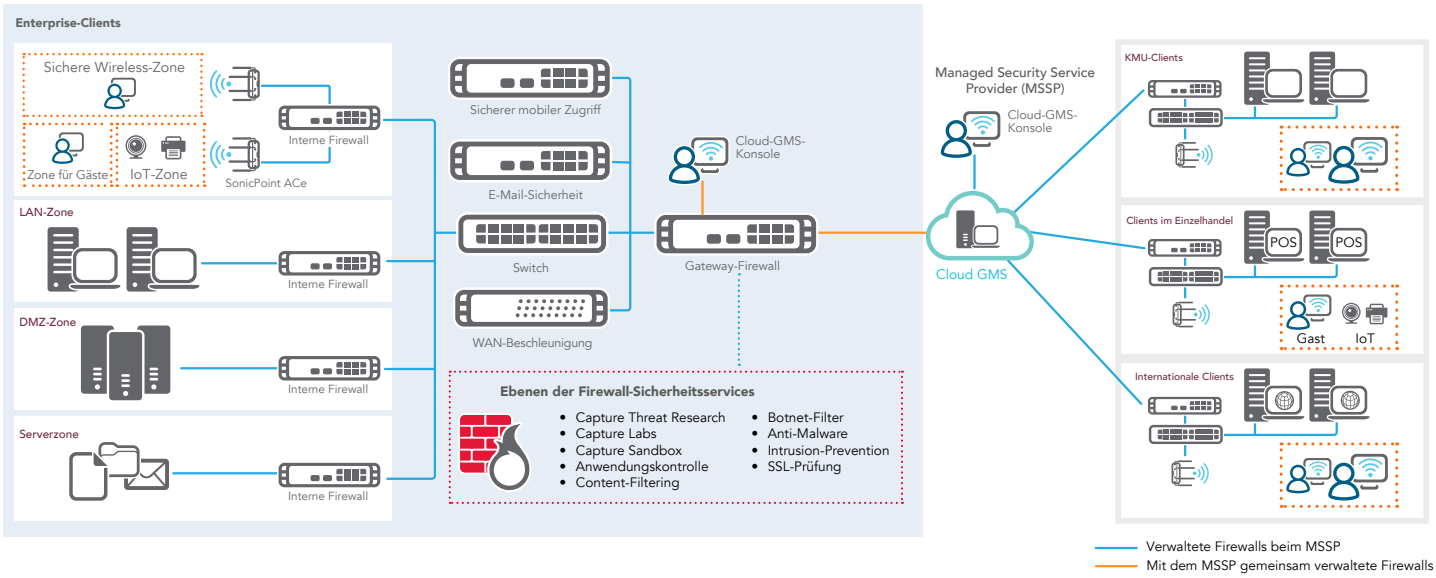


SONICWALL®

Skalierbare Cloud-Architektur

Die verteilte Architektur von Capture Security Center sorgt für uneingeschränkte Systemverfügbarkeit und Skalierbarkeit. Die Lösung eignet sich für kleine und große Unternehmen, Telekommunikationsanbieter, Netzbetreiber und Serviceprovider mit einem umfassenden mehrmandantenfähigen Ökosystem und kann je nach Bedarf auf Tausende SonicWall-Sicherheitsgeräte erweitert werden – unabhängig von deren Standort. Kunden profitieren mit Capture Security Center von hoch interaktiven, einheitlichen Dashboards mit Echtzeit-Überwachung, Reporting und Analysedaten, die intelligente Entscheidungen zu Sicherheitsregeln sowie Zusammenarbeit, Kommunikation und Wissen innerhalb des gemeinsamen Sicherheitsframeworks unterstützen. Mit einer unternehmensweiten Sicht auf die Sicherheitsumgebung und Echtzeit-Sicherheitsdaten für die zuständigen Mitarbeiter können Organisationen geeignete Aktionen für Sicherheitsregeln und -kontrollen durchführen, um ein stärkeres adaptives Sicherheitskonzept zu erhalten.

Capture Security Center bietet eine ganzheitliche und skalierbare Plattform mit Sicherheitsmanagement, Analysen und Reporting für verteilte Unternehmen wie Netzbetreiber, Telekommunikationsanbieter und MSPs.



Cloudbasierte Management-, Reporting- und Analyselösung für die Netzwerk-, Endgeräte- und Cloudsicherheit

Sicherheitsmanagement- und Überwachungsfeatures	
Funktion	Beschreibung
Zentrales Sicherheits- und Netzwerkmanagement	Unterstützt Administratoren bei der Implementierung, Verwaltung und Überwachung einer verteilten Netzwerksicherheitsumgebung.
Föderierte Regelkonfiguration	Einfache, zentrale Regeldefinition für Tausende SonicWall-Firewalls, drahtlose Access-Points, E-Mail-Sicherheitsfunktionen, Secure-Remote-Access-Geräte und Switches.
Change-Order-Management und -Workflow	Durch dieses Feature lässt sich ein Prozess für die Konfiguration, den Vergleich, die Validierung, die Prüfung und die Genehmigung von Regeln vor der Implementierung durchsetzen. Auf diese Weise werden die Richtigkeit und Einhaltung von Regeländerungen sichergestellt. Die Freigabegruppen lassen sich benutzerdefiniert konfigurieren, um die Einhaltung unternehmenseigener Sicherheitsregeln zu gewährleisten. Alle Regeländerungen sind in einer nachprüfbaren Form protokolliert, um sicherzustellen, dass die Firewall gesetzliche Vorgaben erfüllt. Sämtliche granularen Details zu vorgenommenen Änderungen werden chronologisch gespeichert und unterstützen dadurch die Compliance, das Audit-Trailing und die Fehlerbehebung.
Vollautomatische Bereitstellung	Vereinfacht und beschleunigt die Remote-Implementierung und -Bereitstellung von SonicWall-Firewalls über die Cloud. Sorgt für die automatische Durchsetzung von Regeln, führt Firmware-Upgrades durch und synchronisiert Lizenzen.
Effiziente VPN-Implementierung und -Konfiguration	Die Switches der Dell X-Series lassen sich jetzt ganz unkompliziert mit TZ-, NSA- und SuperMassive-Firewalls verwalten. Dabei erfolgt die Verwaltung für die gesamte Netzwerksicherheitsinfrastruktur über eine einzige Konsole.
Offline-Management	Vereinfacht und beschleunigt die Remote-Implementierung und -Bereitstellung von SonicWall-Firewalls über die Cloud. Sorgt für die automatische Durchsetzung von Regeln, führt Firmware-Upgrades durch und synchronisiert Lizenzen.
Effiziente Lizenzverwaltung	Vereinfacht die Bereitstellung von VPN-Konnektivität und konsolidiert Tausende von Sicherheitsregeln.
Umfassendes Dashboard	Das Dashboard umfasst personalisierbare Widgets, geografische Karten und benutzerorientierte Reporting-Funktionen.
Aktive Überwachung von Geräten und Warnmeldungen	Echtzeit-Alarme mit integrierten Überwachungsfunktionen und einfache Troubleshooting-Prozesse ermöglichen es Administratoren, Präventivmaßnahmen zu ergreifen und eine umgehende Problembehebung zu veranlassen.
SNMP-Unterstützung	Bietet leistungsstarke Echtzeit-Traps für alle Transmission Control Protocol/Internet Protocol (TCP/IP)- und SNMP-fähigen Geräte und -Anwendungen. Damit lassen sich Fehler bei kritischen Ereignissen im Netzwerk schnell lokalisieren und beheben.
Anwendungsvisualisierung und -informationen	Historische und Echtzeitberichte zeigen, welche Anwendungen von welchen Benutzern verwendet werden. Die Berichte bieten intuitive Filter- und Drill-down-Funktionen und sind komplett personalisierbar.
Vielfältige Integrationsmöglichkeiten	API-Schnittstelle für Webservices, CLI-Unterstützung für die meisten Funktionen und SNMP-Trap-Unterstützung für Serviceprovider und Unternehmen.
Verwaltung von Switches der Dell Networking X-Series	Die Switches der Dell X-Series lassen sich jetzt ganz unkompliziert mit TZ-, NSA- und SuperMassive-Firewalls verwalten. Dabei erfolgt die Verwaltung für die gesamte Netzwerksicherheitsinfrastruktur über eine einzige Konsole.
Reporting	
Funktion	Beschreibung
Botnet-Bericht	Vier Berichtstypen: Versuche, Ziele, Initiatoren und Zeitverlauf. Sie enthalten Informationen zum Angriffsvektor wie etwa Botnet-ID, IP-Adressen, Länder, Hosts, Ports, Schnittstellen, Initiator/Ziel, Quelle/Ziel und Benutzer.
Geo-IP-Bericht	Bietet Informationen zum blockierten Datenverkehr basierend auf dem Herkunftsland oder dem Zielort des Datenverkehrs. Vier Berichtstypen: Versuche, Ziele, Initiatoren und Zeitverlauf. Sie enthalten Informationen zum Angriffsvektor wie etwa Botnet-ID, IP-Adressen, Länder, Hosts, Ports, Schnittstellen, Initiator/Ziel, Quelle/Ziel und Benutzer.
Bericht zur MAC-Adresse	Hier wird die Media Access Control (MAC)-Adresse auf der Berichtsseite angezeigt. Gerätespezifische Informationen (Initiator MAC und Responder MAC) werden in fünf Berichtstypen dargestellt: • Datennutzung > Initiatoren • Datennutzung > Responder • Datennutzung > Details • Benutzeraktivitäten > Details • Webaktivitäten > Initiatoren
Capture ATP-Bericht	Dank detaillierter Bedrohungsinformationen kann gezielt auf eine Bedrohung oder Infizierung reagiert werden.
HIPPA-, PCI- und SOX-Berichte	Vordefinierte PCI-, HIPAA- und SOX-Berichtsvorlagen für Security-Compliance-Audits.

Reporting (Fortsetzung)	
Funktion	Beschreibung
Berichte zu unberechtigten drahtlosen Access-Points	Die Berichte enthalten Informationen zu allen genutzten Drahtlosgeräten sowie zu unautorisiertem Verhalten aus Ad-hoc- oder Peer-to-Peer-Networking zwischen Hosts und zufälligen Verbindungen für Benutzer, die sich mit benachbarten unautorisierten Netzwerken verbinden.
Intelligentes Reporting und Visualisierung der Benutzeraktivitäten	Umfassende Berichte mit grafischen Elementen für SonicWall-Firewalls, E-Mail-Sicherheit und Mobilgeräte mit sicherem Zugriff. Detaillierter Einblick in Nutzungstrends und Security-Events. Serviceprovider profitieren von einem einheitlichen Corporate Branding.
Zentrales Logging	Zentrale Konsolidierung von Security-Events und -Protokollen für Tausende von Appliances. So können von einem zentralen Punkt aus forensische Netzwerkanalysen durchgeführt werden.
Echtzeit- und historisches Syslog-Reporting der nächsten Generation	Bahnbrechende Verbesserungen der Architektur verkürzen die zeitaufwendige Zusammenfassung, sodass Berichte über eingehende Syslog-Nachrichten nahezu in Echtzeit erstellt werden können. Außerdem lassen sich Daten per Drill-down aufschlüsseln und Berichte umfassend personalisieren.
Übergreifende zeitgesteuerte Berichte	Zeitliche Steuerung von Berichten, die automatisch erstellt und über mehrere Appliances unterschiedlichen Typs hinweg an autorisierte Empfänger per E-Mail versendet werden.
Analytics	
Funktion	Beschreibung
Datenaggregierung	Die informationsgestützte Analyse-Engine automatisiert die Aggregierung, Normalisierung, Korrelation und Kontextualisierung der Sicherheitsdaten über alle Firewalls hinweg.
Datenkontextualisierung	Verwertbare Analysedaten, die in einer strukturierten, sinnvollen und einfach zu nutzenden Weise dargestellt werden, ermöglichen Sicherheitsexperten, Analysten und Stakeholdern, Erkenntnisse zu gewinnen und zu interpretieren, Prioritäten zu setzen, Entscheidungen zu treffen und angemessene Korrekturmaßnahmen zu ergreifen.
Streamanalyse	Streams aus Netzwerksicherheitsdaten werden kontinuierlich in Echtzeit verarbeitet, korreliert und analysiert. Die Ergebnisse werden in einem dynamischen, interaktiven Dashboard visualisiert.
Benutzeranalysen	Umfassende Analysen von Benutzeraktivitätstrends zur Gewinnung vollständiger Einblicke in die Nutzung, Zugriffe und Verbindungen im gesamten Netzwerk.
Dynamische Echtzeitvisualisierung	Eine zentrale Lösung ermöglicht Sicherheitsexperten, umfassende investigative und forensische Drill-down-Analysen von Sicherheitsdaten noch genauer, transparenter und schneller durchzuführen.
Schnelle Erkennung und Behebung	Investigative Funktionen zur Ermittlung unsicherer Aktivitäten und zur schnellen Erkennung und Minderung von Risiken.
Datenstromanalyse und -berichte	Datenstromberichts-Agent für Analyse- und Nutzungsdaten zum Anwendungsverkehr mittels IPFIX- oder NetFlow-Protokolle, um die Echtzeitüberwachung bzw. historische Überwachung zu ermöglichen. Bietet eine wirksame und effiziente Oberfläche für die visuelle Echtzeitüberwachung des Netzwerks. Administratoren können so Anwendungen und Websites mit hohem Bandbreitenbedarf identifizieren, die Anwendungsnutzung der jeweiligen Benutzer beobachten sowie Angriffe und Bedrohungen im Netzwerk antizipieren. • Ein Real-Time-Viewer mit Personalisierung mittels Drag-and-drop • Ein Real-Time-Report-Bildschirm inklusive Filterung mit nur einem Klick • Ein Top-Flows-Dashboard inklusive „Anzeige nach“-Schaltflächen mit nur einem Klick • Ein Flow-Reports-Bildschirm mit fünf zusätzlichen Tabs für Datenstromattribute • Ein Flow-Analytics-Bildschirm mit leistungsstarken Funktionen für Korrelation und Pivoting • Ein Session-Viewer für einen detaillierten Drill-down einzelner Sessions und Pakete
Analyse des Anwendungsdatenverkehrs	Organisationen profitieren von aussagekräftigen Daten zum Anwendungsverkehr, zur Bandbreitennutzung und zu Sicherheitsbedrohungen. Gleichzeitig stehen leistungsstarke Fehlerbehebungs- und forensische Funktionen zur Verfügung.
Cloud App Security	
Funktion	Beschreibung
Echtzeit-Dashboard	Visuelle Echtzeitdarstellung von Anwendungen, Datenverkehrsvolumen, Benutzeraktivität und Nutzungsstandort.
Anwendungserkennung	Automatisierung der Cloud-Anwendungserkennung durch Nutzung der Protokolldateien Ihrer SonicWall-Firewall, um Schatten-IT-Aktivitäten im Netzwerk zu ermitteln.
Bewertung des Anwendungsrisikos	Ermöglicht fundierte Entscheidungen zum Sperren/Entsperren von Anwendungen basierend auf der Risikobewertung.
Anwendungsklassifizierung und -kontrolle	Klassifizierung von Anwendungen als zugelassene oder nicht zugelassene Apps und Einrichtung von Regeln zum Sperren risikobehafteter Anwendungen.

Die Funktionen im Überblick

Verwaltung

- Ortsunabhängiger Zugriff
- Warnmeldungen und Benachrichtigungen
- Diagnosetools
- Mehrere gleichzeitige Benutzersitzungen
- Offline-Management und Scheduling
- Verwaltung von Firewall-Sicherheitsregeln
- Verwaltung von VPN-Sicherheitsregeln
- Verwaltung von E-Mail-Sicherheitsregeln
- Verwaltung von SSL-VPN-Regeln und Regeln für einen sicheren Remote-Zugriff
- Verwaltung der Security-Mehrwertdienste
- Definition von Regelvorlagen auf Gruppenebene
- Regelreplikation von einem Gerät auf eine Gerätegruppe
- Regelreplikation von der Gruppenebene auf ein einzelnes Gerät
- Redundanz und Hochverfügbarkeit
- Bereitstellungsmanagement
- Skalierbare und verteilte Architektur
- Dynamische Verwaltungsansichten
- Einheitlicher Lizenzmanager
- Befehlszeilenschnittstelle (CLI)
- API-Schnittstelle für Webservices
- Rollenbasierte Verwaltung (Benutzer, Gruppen)
- Umfassendes Dashboard
- Sicherung von Einstellungsdateien für Firewall-Appliances

Überwachung

- IPFIX-Datenströme in Echtzeit
- SNMP-Unterstützung
- Aktive Überwachung von Geräten und Warnmeldungen
- SNMP-Relay-Verwaltung
- Überwachung des VPN- und Firewall-Status
- Live-Syslog-Überwachung und Warnmeldungen

Reporting

- Große Auswahl an grafischen Berichten
- Compliance-Reporting
- Personalisierbares Reporting mit Drill-down-Funktionen
- Zentrales Logging
- Sammelberichte zu verschiedenen Bedrohungen
- Reporting zu Benutzern
- Berichte zur Anwendungsnutzung
- Detaillierte Serviceberichte
- Neues Abwehrkonzept gegen Angriffe
- Bandbreiten- und Serviceberichte pro Schnittstelle
- Reporting für SonicWall-UTM-Firewall-Appliances
- Reporting für SonicWall-SRA-SSL-VPN-Appliances
- Universelle zeitgesteuerte Berichte
- Syslog- und IPFIX-Reporting der nächsten Generation
- Flexibles und granulares Reporting nahezu in Echtzeit
- Reporting zur genutzten Bandbreite pro Benutzer
- Reporting zu Client-VPN-Aktivitäten
- Detaillierter Zusammenfassungsbericht der Services über VPN
- Berichte zu unberechtigten drahtlosen Access-Points
- Reporting zur SRA SMB Web Application Firewall (WAF)
- Reporting zu Cloud App Security (CAS)
- Reporting zu Capture Client

Analytics

- Datenaggregierung
- Datenkontextualisierung
- Streamanalyse
- Benutzeranalysen
- Dynamische Echtzeitvisualisierung
- Schnelle Erkennung und Behebung

Lizenzen und Pakete

Capture Security Center (CSC)		Lizenzstufe			
		CSC Management Lite	CSC Management	CSC Management and Reporting	CSC Analytics
Lizenzanforderung	Verfügbar für Kunden mit aktivem AGSS/CGSS-Abo	AGSS/CGSS	AGSS/CGSS	AGSS/CGSS	AGSS/CGSS
Verwaltung	Zentrale Verwaltung	✓	✓	✓	
	Sicherung/Wiederherstellung	✓	✓	✓	
	Aufgabenplanung		✓	✓	
	Verwaltung mehrerer Firewalls		✓	✓	
	Vererbung – Forward/Reverse		✓	✓	
	Automatische Bereitstellung		✓	✓	
	Downloads von Firewall-Offline-Signaturen		✓	✓	
	Workflow		✓	✓	
Reporting	Live-Überwachung, Übersichts-Dashboards			✓	
	Berichte herunterladen: Anwendungen, Bedrohungen, CFS, Benutzer, Datenverkehr usw.			✓	
	Zeitgesteuertes Reporting			✓	
Analytics	Analytics (30-tägige Speicherung)				✓
	Cloud App Security (30-tägige Speicherung)				✓

Bestellinformationen für Capture Security Center

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

Internet-Browser

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

Für die Verwaltung mit Capture Security Center unterstützte SonicWall-Appliances

- SonicWall Netzwerksicherheits-Appliances: NSa 2600 bis NSa 6650 und Appliances der TZ Series
- Virtuelle SonicWall Netzwerksicherheits-Appliances: NSv 10 bis NSv 400
- SonicWall Endpunktsicherheit – Capture Client
- SonicWall Cloud-Sicherheit – Cloud App Security (CAS)

Über uns

Seit über 26 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

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

DataSheet-CaptureSecurityCenter-US-VG-MKTG2657