# SonicWall Analytics

Machen Sie aus Daten Informationen, aus Informationen Wissen, aus Wissen Entscheidungen und aus Entscheidungen konkrete Handlungen

SonicWall Analytics bietet über eine zentrale Konsole einen genauen Überblick über sämtliche Aktivitäten in der SonicWall-Netzwerksicherheitsumgebung. Herzstück ist eine leistungsstarke, informationsgestützte Analyse-Engine, die Aggregation, Normalisierung, Korrelation und Kontextualisierung der Sicherheitsdaten, die durch alle SonicWall-Firewalls und Wireless-Access-Points fließen, automatisiert. Das interaktive Dashboard der Anwendung setzt verschiedene Diagramme und Tabellen zur Zeitnutzung ein, um die Datenmodelle darzustellen.

Analytics präsentiert die Ergebnisse in einer aussagekräftigen und leicht nutzbaren Form. So können Sicherheitsteams, Analysten, Auditoren, Vorstandsmitglieder und Führungskräfte Daten ermitteln, interpretieren und priorisieren, evidenzbasierte Entscheidungen treffen und angemessene Abwehr- und Korrekturmaßnahmen gegen identifizierte Risiken und Bedrohungen treffen.

Analytics bietet Stakeholdern alle Echtzeitinformationen auf einen Blick sowie die nötigen Berechtigungen und die Flexibilität, um umfassende investigative und forensische Drill-down-Analysen rund um Netzwerkverkehr, Benutzerzugriff, Konnektivität, Anwendungen und Nutzung, Zustand von Sicherheitsressourcen, Sicherheitsvorfälle, Bedrohungsprofile und andere firewallbezogene Daten durchzuführen.


## Vorteile:

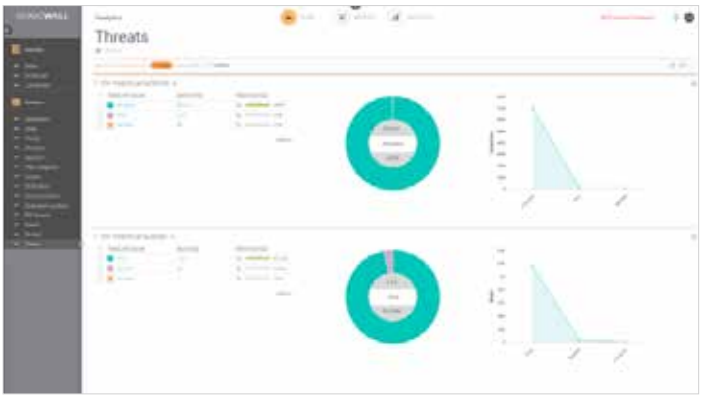
- Eine einzige Konsole für alle wichtigen Informationen und ein umfassender, situativ angepasster Überblick über alle Vorgänge in der Netzwerksicherheitsumgebung
- Umfassende Berechtigungen und Flexibilität, um tiefgehende investigative und forensische Analysen durchzuführen
- Ausführliche Informationen zu potenziellen und realen Risiken und Bedrohungen
- Schnellere, zuverlässigere und transparentere Behebung von Risiken
- Kürzere Reaktionszeit bei Vorfällen dank aussagekräftiger Echtzeitinformationen zu Bedrohungen

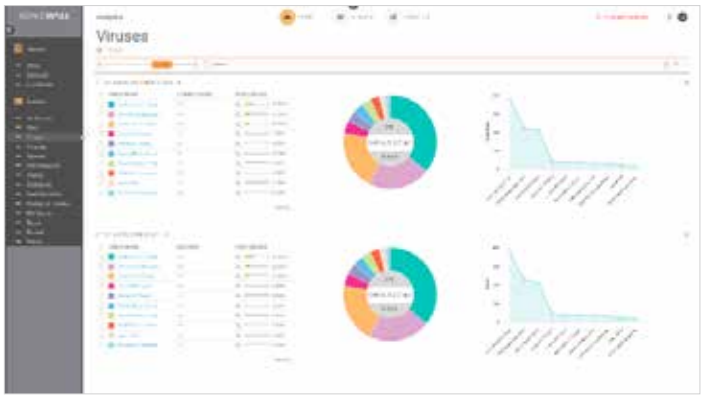
**Partner Enabled Services**
Brauchen Sie Hilfe bei der Planung, Implementierung oder Optimierung Ihrer SonicWall-Lösung? Unsere SonicWall Advanced Services Partner bieten Ihnen erstklassige Professional Services. Weitere Infos erhalten Sie unter www.sonicwall.com/PES.

Diese detaillierten Informationen und das tiefgehende Verständnis der Sicherheitsumgebung sorgen für die nötigen Erkenntnisse, um Sicherheitsrisiken zu identifizieren und gezielt zu beheben. Darüber hinaus lassen sich Ergebnisse schneller, zuverlässiger und genauer überwachen und nachverfolgen.

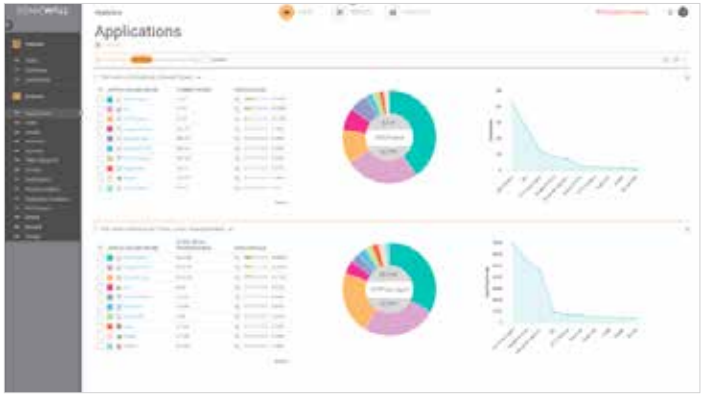
Durch die Integration von Analytics in den Geschäftsprozess lassen sich Analysen operationalisieren und so Daten in Informationen, Informationen in Wissen und Wissen in Entscheidungen zur Automatisierung der Sicherheitsprozesse umwandeln.









| 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 diese Funktion 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 allen Änderungen werden chronologisch gespeichert und helfen bei der Compliance, beim Audit-Trailing und bei der Fehlerbehebung. |
| Vollautomatische Implementierung | Durch diese Funktion lassen sich die Implementierung und Bereitstellung von SonicWall-Firewalls remote mithilfe der Cloud vereinfachen und beschleunigen. Es werden automatisch Richtlinien umgesetzt, Firmware-Upgrades durchgeführt und Lizenzen synchronisiert. |
| Effiziente VPN-Implementierung und -Konfiguration | Die Switches der Dell X-Series lassen sich jetzt ganz unkompliziert mit TZ-, NS*a*- und SuperMassive-Firewalls verwalten. Dabei erfolgt die Verwaltung für die gesamte Netzwerksicherheitsinfrastruktur über eine einzige Konsole. |
| Offline-Management | Durch diese Funktion lassen sich die Implementierung und Bereitstellung von SonicWall-Firewalls remote mithilfe der Cloud vereinfachen und beschleunigen. Es werden automatisch Richtlinien umgesetzt, Firmware-Upgrades durchgeführt und Lizenzen synchronisiert. |
| 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. |
| Überwachung aktiver Geräte und Alarmierung | Durch Echtzeitwarnmeldungen mit integrierten Überwachungsfunktionen und einfache Troubleshooting-Prozesse können Administratoren Präventivmaßnahmen einleiten und Probleme umgehend beheben. |
| 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 Application-Intelligence | Historische und Echtzeitberichte zeigen, welche Anwendungen von welchen Usern genutzt werden. Die Berichte bieten intuitive Filter- und Drill-down-Funktionen und sind komplett personalisierbar. |
| Vielfältige Integrationsmöglichkeiten | API(Application Programming Interface)-Schnittstelle für Webservices, CLI(Command Line Interface)-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-, NS*a*- und SuperMassive-Firewalls verwalten. Dabei erfolgt die Verwaltung für die gesamte Netzwerksicherheitsinfrastruktur über eine einzige Konsole. |
| HIPPA-, PCI- und SOX-Berichte | Vordefinierte PCI-, HIPAA- und SOX-Berichtsvorlagen für Security-Compliance-Audits. |
| **Analysen** | |
| Funktion | Beschreibung |
| Datenaggregation | Eine informationsgestützte Analyse-Engine automatisiert die Aggregation, Normalisierung, Korrelation und Kontextualisierung der Sicherheitsdaten, die durch alle SonicWall-Firewalls fließen. |
| Kontextualisierung von Daten | Mithilfe effizienter Analysen, die in einer strukturierten, aussagekräftigen und leicht nutzbaren Form präsentiert werden, können Sicherheitsteams, Analysten und Stakeholder Daten ermitteln, interpretieren und priorisieren, Entscheidungen treffen und angemessene Abwehrmaßnahmen einleiten. |
| Streaming-Analysen | Netzwerksicherheitsdatenströme werden kontinuierlich in Echtzeit verarbeitet, korreliert und analysiert. Die Ergebnisse werden in einem dynamischen, interaktiven visuellen Dashboard dargestellt. |
| Benutzeranalysen | Umfassende Analysen der Aktivitätsmuster von Usern ermöglichen tiefgehende Einblicke in ihr Nutzungsverhalten, ihre Zugriffe und ihre Verbindungen über das gesamte Netzwerk hinweg. |
| Dynamische Echtzeitvisualisierung | Über eine einzige Konsole können Sicherheitsteams tiefgehende investigative und forensische Drill-down-Analysen auf Basis von Sicherheitsdaten noch schneller, gezielter und genauer durchführen. |
| Schnelle Erkennung und Behebung von Risiken | Durch investigative Funktionen lassen sich unsichere Aktivitäten aufspüren und Risiken innerhalb kurzer Zeit steuern und beheben. |
| 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 User beobachten sowie Angriffe und Bedrohungen im Netzwerk antizipieren.<br>• Ein Real-Time-Viewer mit Personalisierung mittels Drag-and-drop<br>• Ein Real-Time-Report-Bildschirm inklusive Filterung mit nur einem Klick<br>• Ein Top-Flows-Dashboard inklusive „Anzeige nach"-Schaltflächen mit nur einem Klick<br>• Ein Flow-Reports-Bildschirm mit fünf zusätzlichen Tabs für Datenstromattribute<br>• Ein Flow-Analytics-Bildschirm mit leistungsstarken Funktionen für Korrelation und Pivoting<br>• Ein Session-Viewer für einen detaillierten Drill-down einzelner Sessions und Pakete |
| Analyse des Anwendungsverkehrs | Organisationen profitieren von aussagekräftigen Daten zum Anwendungsverkehr, zur Bandbreitennutzung und zu Sicherheitsbedrohungen. Gleichzeitig stehen leistungsstarke Troubleshooting- und Forensik-Funktionen zur Verfügung. |

## Die Funktionen im Überblick

### Zentrales Dashboard mit Visualisierungen und Diagrammen

- Bandbreite
- CPU-Nutzung
- Anzahl der Verbindungen
- Verbindungsgeschwindigkeit pro Sekunde
- Risikoindex (Skala von 1–10)
- Anzahl blockierter Bedrohungen
- Gesamtzahl der Verbindungen
- Gesamtmenge der übertragenen Daten
- Am meisten genutzte Anwendungen
- Häufigste Eindringversuche
- Gängigste URL-Kategorien
- Häufigste Viren
- Anzahl von Viren, Eindringversuchen, Spyware und Botnets

### Live Monitor-Streaming mit Flächen-/Balkendiagrammen

- Anwendungen
- Schnittstelle (eingehend/ausgehend), Durchschnitt, Minimum, Spitzen
  - Bandbreite
  - Paketrate
  - Paketgröße
  - Verbindungsgeschwindigkeit
- Nutzung
  - Anzahl der Verbindungen
  - Multicore-Monitor

### Hauptdashboards zu Top-Events mit Drill-down

- Anwendungen
- Benutzer
- Viren
- Eindringversuche
- Spyware
- Webkategorien
- Quellen
- Ziele
- Quellorte
- Zielorte
- Bandbreitenwarteschlangen
- Botnet

### Berichte mit Drill-down, Export nach PDF/CSV und zeitgesteuerte E-Mails

- Anwendungen/Benutzer/Quellen/Ziele
  - Verbindungen
  - Gesamtzahl der blockierten Verbindungen
  - Nach Anwendungsregel blockierte Verbindungen
  - Nach Bedrohung blockierte Verbindungen
  - Nach Botnet-Filter blockierte Verbindungen
  - Nach GeoIP-Filter blockierte Verbindungen
  - Nach Content-Filtering-Service blockierte Verbindungen
  - Virus
  - Eindringversuche
  - Spyware
  - Gesamtmenge der übertragenen Daten
  - Gesendete Daten
  - Erhaltene Daten
- Viren/Eindringversuche/Spyware/ Webkategorien/Quellorte/Zielorte/ Bandbreitenwarteschlangen
  - Verbindungen
  - Gesamtmenge der übertragenen Daten
  - Gesendete Daten
  - Erhaltene Daten
- Botnet
  - Verbindungen
- Export
  - .pdf
  - .csv
- Zeitgesteuerte Berichte
  - Flow-Reporting
  - Capture Threat Assessment (SWARM)
  - Täglich/Wöchentlich/Monatlich
  - Archive/E-Mail/PDF

### Analytics-Session-Viewer mit Drill-down, Filtering, Export einzelner Sitzungsdaten

- Datenverkehrsanalysen zu beliebigen Kombinationen folgender Elemente:
  - Anwendung
  - Anwendungskategorie
  - Anwendungsrisiko
  - Signatur
  - Handlung
  - Initiator-/Responder-IP
  - Initiator-/Responder-Land
  - Initiator-/Responder-Port
  - Initiator-/Responder-Bytes
  - Initiator-/Responder-Schnittstelle
  - Initiator-/Responder-Index
  - Initiator-/Responder-Gateway
  - Initiator-/Responder-MAC
  - Protokoll
  - Geschwindigkeit (KBit/s)
  - Flow-ID
  - Eindringversuch
  - Virus
  - Spyware
  - Botnet
- Analysen zu Bedrohungen / blockierten Bedrohungen zu beliebigen Kombinationen folgender Elemente:
  - Name der Bedrohung
  - Typ der Bedrohung
  - ID der Bedrohung
  - Anwendung
  - Anwendungskategorie
  - Anwendungsrisiko
  - Signatur
  - Handlung
  - Initiator-/Responder-IP
  - Initiator-/Responder-Land
  - Initiator-/Responder-Port
  - Initiator-/Responder-Bytes
  - Initiator-/Responder-Schnittstelle
  - Initiator-/Responder-Index
  - Initiator-/Responder-Gateway
  - Initiator-/Responder-MAC
  - Protokoll
  - Geschwindigkeit (KBit/s)
  - Flow-ID
  - Eindringversuch
  - Virus
  - Spyware
  - Botnet

### Analysen zu URL / blockierten Bedrohungen zu beliebigen Kombinationen folgender Elemente:

- URL
- URL-Kategorie
- URL-Domain
- Anwendung
- Anwendungskategorie
- Anwendungsrisiko
- Signatur
- Handlung
- Initiator-/Responder-IP
- Initiator-/Responder-Land
- Initiator-/Responder-Port
- Initiator-/Responder-Bytes
- Initiator-/Responder-Schnittstelle
- Initiator-/Responder-Index
- Initiator-/Responder-Gateway
- Initiator-/Responder-MAC
- Protokoll
  - Geschwindigkeit (KBit/s)
  - Flow-ID
  - Eindringversuch
  - Virus
  - Spyware
  - Botnet

### Analytics-Flow-Monitor – Drill-down- und Pivot-Funktionen für Datenstrom-Parameter

- Anwendungen
  - Namen
  - Kategorien
  - Signaturen
- User
  - Name
  - IP-Adresse
  - Domainnamen
  - Authentifizierungstypen
- Webaktivitäten
  - Websites
  - Webkategorien
  - URLs
- Quellen
  - IP-Adressen
  - Schnittstellen
  - Länder
- Ziele
  - IP-Adressen
  - Schnittstellen
  - Länder
- Bedrohungen
  - Eindringversuche
  - Viren
  - Spyware
  - Spam
  - Botnets
- VoIP
  - Medientypen
  - Anrufer-IDs
- Geräte
  - IP-Adressen
  - Schnittstellen
  - Namen
- Inhalte
  - E-Mail-Adressen
  - Dateitypen
- Bandbreitenverwaltung
  - Eingehend
  - Ausgehend
  - Alle
  - URL
  - Sitzungen
  - Gesamtzahl der Pakete
  - Gesamtzahl der Bytes
  - Bedrohungen

### Sterngraphen – Punkt-zu-Punkt-Visualisierungen, Drill-down und Pivoting

- Quellen/Benutzer/Standorte/Geräte
  - Von/An
    - » Ziele
    - » Anwendungen
    - » Webaktivitäten
    - » Bedrohungen
  - Gefiltert nach
    - » Anzahl der Verbindungen
    - » übertragenen Daten
    - » ausgetauschten Paketen
    - » Anzahl der Bedrohungen
  - Hervorhebung für
    - » Bedrohungen
    - » Daten > 1 MB
    - » Verbindungen > 1.000
    - » Pakete > 1.000

## Lizenzierung und Bündelung

| Capture Security Center (CSC) | | Lizenzstufe | | | |
|---|---|---|---|---|---|
| | | CSC Management Lite | CSC Management | CSC Management and Reporting | CSC Analytics |
| Lizenzierungs-anforderungen | Verfügbar für Kunden mit aktivem AGSS-/CGSS-Abo | AGSS/CGSS | AGSS/CGSS | AGSS/CGSS | AGSS/CGSS |
| Verwaltung | Eine einzige Konsole | ✓ | ✓ | ✓ | |
| | Back-up/Wiederherstellung | ✓ | ✓ | ✓ | |
| | Aufgabenplanung | | ✓ | ✓ | |
| | Verwaltung von Firewallgruppen | | ✓ | ✓ | |
| | Vererbung (Forward/Reverse) | | ✓ | ✓ | |
| | Vollautomatisch | | ✓ | ✓ | |
| | Offline-Downloads von Firewall-Signaturen | | ✓ | ✓ | |
| | Workflow | | ✓ | ✓ | |
| Reporting | Live Monitor, zentrale Dashboards | | | ✓ | |
| | Download von Berichten: Anwendungen, Bedrohungen, CFS, Benutzer, Datenverkehr etc. | | | ✓ | |
| | Zeitgesteuertes Reporting | | | ✓ | |
| Analysen | Analysen (30-Tage-Aufbewahrung) | | | | ✓ |
| | Cloud App Security (30-Tage-Aufbewahrung) | | | | ✓ |

## Capture Security Center – Bestellinformationen

| 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 and Reporting für TZ Series, NSv 10 bis 100, 1 Jahr | 01-SSC-3435 |
| SonicWall Capture Security Center Management and Reporting für TZ Series, NSv 10 bis 100, 2 Jahre | 01-SSC-9148 |
| SonicWall Capture Security Center Management and Reporting für TZ Series, NSv 10 bis 100, 3 Jahre | 01-SSC-9149 |
| SonicWall Capture Security Center Management and Reporting für NSA 2600 bis 6650 und NSv 200 bis 400, 1 Jahr | 01-SSC-3879 |
| SonicWall Capture Security Center Management and Reporting für NSA 2600 bis 6650 und NSv 200 bis 400, 2 Jahre | 01-SSC-9154 |
| SonicWall Capture Security Center Management and 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)

### Unterstützte SonicWall-Appliances, die von Capture Security Center verwaltet werden

- SonicWall-Netzwerksicherheits-appliances: NS*a* 2600 bis NS*a* 6650 und TZ Series-Appliances
- Virtuelle SonicWall-Netzwerksicherheits-appliances: NSv 10 bis NSv 400

### Über uns

Seit über 27 Jahren bekämpft SonicWall Cyberkriminalität, um kleinen, mittleren und großen Unternehmen weltweit Schutz zu bieten. Mit unseren Produkten und Partnern können wir eine automatisierte Echtzeitlösung zur Erkennung und Prävention von Sicherheitslücken für die individuellen Anforderungen von mehr als 500.000 Organisationen in über 215 Ländern und Regionen 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-Analytics-US-VG-MKTG4305

SONICWALL®