

SonicWall Analytics

Verwandeln Sie Daten in aussagekräftige Informationen

Mit SonicWall Analytics lassen sich aus den Traffic-Daten Ihrer Firewall aussagekräftige Erkenntnisse zu Benutzern, Anwendungen und Netzwerken gewinnen. So können Sie über eine zentrale Oberfläche Sicherheitsrisiken präziser aufdecken und schneller mindern. Auf der Grundlage einer leistungsstarken cloudnativen Architektur entwickelt, reichert die Analyse-Engine eine gewaltige Menge von Rohdaten über Tausende Firewall-Nodes hinweg an, um Stakeholdern über ein Management-Dashboard einen transparenten Einblick in die Sicherheit und andere Bereiche zu bieten.

Mithilfe von Analytics lassen sich die Datenmodelle durch verschiedene Formen semantischer Graphen sowie Diagramme und Tabellen zur Zeitnutzung übersichtlich darstellen. Dies hilft, Zeit zu sparen und die Analysten zu entlasten. Zusätzliche Drill-down-Funktionen ermöglichen es Sicherheitsverantwortlichen, kritische Datenpunkte zu überprüfen und genauer unter die Lupe zu nehmen, um **verborgene Risiken aufzudecken und frühzeitig einzugreifen**. Wenn sie dabei riskante Benutzeraktivitäten identifizieren, können sie zudem evidenzbasierte Richtlinien durchsetzen.

Dank einer umfassenden Transparenz und Kontrolle können Sicherheitsanalysten sämtliche Aktivitäten in allen Bereichen einsehen, sodass sie Risiken besser im Griff haben. Gleichzeitig können Sicherheitsverantwortliche ihre wertvolle Zeit dazu nutzen, schnelle Maßnahmen für die wichtigsten Anwendungen und Benutzer zu orchestrieren, anstatt auf jedes einzelne Ereignis reagieren zu müssen. Analytics lässt sich mit der **Agilität und Elastizität** der Cloud nutzen und skalieren, um selbst anspruchsvollste Unternehmensanforderungen zu erfüllen.



HIGHLIGHTS

Geschäft

- Umfassender Einblick in die Sicherheit
- Echtzeitinformationen zum Sicherheitsstatus
- Erfüllung interner Compliance-Vorschriften
- Genaue Planung und Budgetierung für den Bereich Cybersicherheit
- Geringere Investitions- und Betriebskosten

Betrieb

- Einfache und übersichtliche Darstellung der Sicherheitskennzahlen
- Gewinnung von Erkenntnissen aus allen Netzwerk- und Benutzerereignissen sowie Warnmeldungen
- Definition präziser richtlinienbasierter Abwehrmaßnahmen
- Skalierbarkeit und Performance mit der Agilität und Elastizität der Cloud

Sicherheit

- Identifizierung verborgener Risiken
- Frühzeitiges Eingreifen
- Zeitnahe Reaktion auf unsichere Benutzeraktivitäten
- Aus Analysten bessere Risikomanager machen
- Aus Sicherheitsverantwortlichen bessere Problemlöser machen

Erfahren Sie mehr über SonicWall Analytics

www.sonicwall.com/analytics



Umfassende Einblicke

Analytics bietet Ihnen einen umfassenden Überblick über Ihre gesamte SonicWall-Sicherheitsumgebung auf Benutzer-, Gruppen- oder Geräteebene. Das Management-Dashboard stellt statische und echtzeitnahe Risikoberichte und Analysen des kompletten Netzwerkverkehrs und der gesamten Datenkommunikation im Firewall-Ökosystem bereit. Alle Protokolldaten werden erfasst, aggregiert, kontextualisiert und auf aussagekräftige und leicht nutzbare Weise präsentiert. So können Sie die Daten ermitteln, interpretieren und vorselektieren und auf Basis datengestützter Erkenntnisse die nötigen Abwehrmaßnahmen einleiten.

Analytics enthält eine große Bandbreite vordefinierter Berichte. Außerdem können Sie beliebige Verkehrsdaten kombinieren, um ganz flexibel benutzerdefinierte Reports je nach gewünschter Nutzung zu erstellen und nach einem regelmäßigen Zeitplan zu versenden. Es können historische Datensätze der letzten 365 Tage erfasst und für Verkehrsanalysen sowie die Erkennung von Sicherheitslücken und Anomalien eingesetzt werden. Diese Informationen helfen, Daten nachzuverfolgen und zu messen und ein Security-first-Netzwerk und Security-Operations-Center zu betreiben.



Abbildung 1: Management-Dashboard

Das Risiko verstehen

Mit den Drill-down- und Pivoting-Funktionen können Sie bestimmte Muster und Trends im Hinblick auf ein- und ausgehenden Verkehr, Anwendungsnutzung, Benutzer- und Gerätezugriff, Bedrohungsaktionen usw. genauer unter die Lupe nehmen. Verschiedene Berichte und Analysen zu Endpunkten, Netzwerken, Benutzern und Anwendungen ermöglichen es Ihnen, Warnmeldungen, Anomalien und riskante Benutzeraktivitäten proaktiv zu analysieren und darauf zu reagieren. Durch einen umfassenden Blick auf die Sicherheit lassen sich situationsbezogene Informationen

gewinnen, die es wiederum gestatten, Sicherheitsrisiken zu erkennen, richtlinienbasierte Maßnahmen zu orchestrieren, die Sicherheitsanforderungen konsequent umzusetzen und die Ergebnisse kontinuierlich in Ihrer gesamten Umgebung zu überwachen.

Flexible Implementierung mit SaaS-, virtuellen oder IaaS-Optionen

Analytics bietet Ihnen flexible Implementierungsoptionen, die optimal auf Ihre operativen Anforderungen abgestimmt sind.

Analytics ist als wartungsfreie SaaS-Lösung verfügbar, die von SonicWall gehostet wird und über das Internet aufrufbar ist. Dank der unbegrenzten Elastizität können Sie die Lösung bei Bedarf skalieren und gleichzeitig Ihre Betriebskosten senken. Die typischen Ausgaben für den Kauf von Hardware und Software, die benutzerdefinierte Installation, regelmäßige Wartung und Upgrades, Abschreibungen und Außerbetriebnahme entfallen und werden mit einer niedrigen, vorhersehbaren jährlichen Abogebühr ersetzt.

Die Funktionen im Überblick

Funktion	Beschreibung
Datenaggregation	Die Sicherheitsdaten, die durch alle Firewalls gehen, lassen sich automatisch aggregieren und normalisieren.
Datenkontextualisierung	Firewall-Daten lassen sich verarbeiten, anreichern und in einer strukturierten, aussagekräftigen und einfach zu nutzenden Weise darstellen. So können Sicherheitsexperten, Analysten und Stakeholder Erkenntnisse gewinnen und interpretieren, Prioritäten setzen, Entscheidungen treffen und angemessene Abwehrmaßnahmen ergreifen.
Streaming-Analyse	Streams aus Netzwerksicherheitsdaten werden kontinuierlich in Echtzeit verarbeitet und angezeigt. Die Ergebnisse werden in einem dynamischen, interaktiven Dashboard visualisiert.
Benutzeranalysen	Ein Management-Dashboard bietet einen umfassenden Überblick über die Webanwendungs- und Internetnutzung der Mitarbeiter. Werden riskante Webaktivitäten identifiziert, können Sie durch einen granulareren Drill-down auf historische Berichte evidenzbasierte und richtliniengesteuerte Maßnahmen einrichten.
Analyse des Anwendungsdatenverkehrs	Organisationen profitieren von aussagekräftigen Daten zum Anwendungsverkehr, zur Bandbreitennutzung und zu Sicherheitsbedrohungen. Gleichzeitig stehen leistungsstarke Troubleshooting- und forensische Funktionen zur Verfügung.
Sicherheitsanalysen	Nutzer profitieren von einem umfassenden Echtzeiteinblick und einer schnellen Bedrohungserkennung. Sicherheitsanalysten und Incident-Responder können Probleme ermitteln, identifizieren und untersuchen.
Dynamische Echtzeitvisualisierung	Eine zentrale Lösung ermöglicht es Sicherheitsanalysten, umfassende investigative und forensische Drill-down-Analysen von Sicherheitsdaten noch genauer und schneller durchzuführen.
Schnelle Erkennung und Behebung von Risiken	Investigative Funktionen erlauben die Ermittlung unsicherer Aktivitäten und die schnelle Erkennung und Minderung von Risiken durch angemessene Maßnahmen.
Produktivitätsberichte (erfordern eine aktivierte AGSS-/CGSS-Lizenz auf Firewalls der Generation 6/6.5 sowie eine Essential Protection-Lizenz auf Firewalls der Generation 7)	Leistungsstarke Snapshots und Drill-down-Berichte zum Internetverhalten der User bieten umfassende Einblicke in die Nutzung von Internetressourcen innerhalb der Organisation. Diese Reports erfassen Daten zur Website-Adresse sowie das Datum des Benutzerzugriffs und berechnen, wie viel Zeit die User auf jeder Site verbringen und ob diese Sites während oder außerhalb der Arbeitszeiten aufgerufen werden. Produktivitätsberichte unterteilen die Webaktivitäten der Nutzer in Produktivitätsgruppen wie „produktiv“, „unproduktiv“, „akzeptabel“, „inakzeptabel“ oder auch in benutzerdefinierte Gruppen. So können Organisationen Internetnutzungsmuster besser verstehen und die Mitarbeiterproduktivität optimieren. Zum Beispiel können Personalleiter mithilfe der Informationen zur Nutzung nicht arbeitsrelevanter Websites mögliche Verletzungen der Verhaltensrichtlinien durch Mitarbeiter prüfen und angemessen darauf reagieren. Ähnliche Use-Cases findet man auch in allen anderen Bereichen.

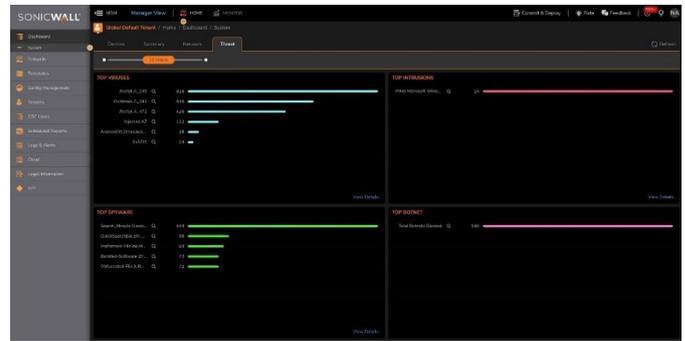


Abbildung 2: Bedrohungsübersicht

Für eine umfassende Systemkontrolle und Compliance können Sie Analytics vor Ort als Software auf Ihrer bevorzugten virtuellen Plattform installieren, wie zum Beispiel VMware und Microsoft Hyper-V. Dabei profitieren Sie von allen operativen und wirtschaftlichen Vorteilen der Virtualisierung, wie etwa einer hohen Systemskalierbarkeit, einer schnellen Systembereitstellung sowie niedrigeren Kosten.

Funktion	Beschreibung
VPN-Berichte	Diese Reports bieten einen Überblick darüber, welche Unternehmensressourcen im VPN-Tunnel genutzt werden, wie viel Bandbreite sie verbrauchen und von wem (Benutzername und IP-Adresse) dieser Datenverkehr ausgeht. Netzwerkadministratoren können diese Informationen nutzen, um geschäftskritische Anwendungen zu überwachen, den Datenverkehr zu steuern bzw. Traffic-Shaping durchzuführen und für Kapazitätssteigerungen zu planen.
Datenstromanalyse und -berichte	<p>Ein Flow-Reporting-Agent bietet Analyse- und Nutzungsdaten zum Anwendungsverkehr mittels IPFIX- oder NetFlow-Protokollen, um eine Echtzeitüberwachung bzw. historische Überwachung zu ermöglichen. Administratoren profitieren von einer effektiven und effizienten Oberfläche für die visuelle Echtzeitüberwachung ihres Netzwerks. So können sie Anwendungen und Websites mit hohem Bandbreitenbedarf identifizieren, die Anwendungsnutzung der jeweiligen User beobachten sowie Angriffe und Bedrohungen im Netzwerk antizipieren.</p> <ul style="list-style-type: none"> • Real-Time-Report-Bildschirm inklusive Filterung mit nur einem Klick • Top-Flows-Dashboard inklusive „Anzeige nach“-Schaltflächen mit nur einem Klick • Flow-Reports-Bildschirm mit zusätzlichen Tabs für Datenstromattribute • Flow-Analytics-Bildschirm mit leistungsstarken Funktionen für Korrelation und Pivoting • Session-Viewer für einen detaillierten Drill-down einzelner Sessions und Pakete
Umfassende grafische Reports	Diese Berichte ermöglichen einen umfassenden Überblick über Firewall-Bedrohungen, Bandbreitennutzung, Mitarbeiterproduktivität, verdächtige Netzwerkaktivitäten und Analysen zum Anwendungsverkehr.
Syslog-Reporting	Die optimierte Zusammenfassung von Daten ermöglicht echtzeitnahe Berichte zu ankommenden Syslog-Meldungen. Durch den direkten Zugriff auf die zugrunde liegenden Rohdaten werden zusätzlich umfassende granulare Kontrollmöglichkeiten und ein individuell anpassbares Reporting unterstützt.
Zeitgesteuerte Berichte	Von einem zentralen Zugangspunkt aus kann auf sämtliche zeitgesteuerte Berichte zugegriffen werden. Die einzelnen Berichte können dabei Diagramme und Tabellen für mehrere verschiedene Geräte enthalten. Die Berichte können zeitgesteuert erstellt und in unterschiedlichen Formaten an einen oder mehrere Analysten versendet werden.
360°-Reporting	Anpassbare Ansichten enthalten mehrere Übersichtsreports auf einer Seite. Benutzer können damit wichtige Kennzahlen zum Netzwerk leicht auffinden und in kürzester Zeit Daten aus verschiedenen Berichten analysieren.
Sammelreports zu verschiedenen Bedrohungsarten	Hierin werden Daten zu Angriffen erfasst. Bedrohungen, die von den SonicWall-Firewalls und den Sicherheitsservices SonicWall Capture ATP, Gateway Anti-Virus, Anti-Spyware, Intrusion-Prevention sowie Application Intelligence and Control erkannt wurden, können unmittelbar dargestellt werden.
Neue Erkenntnisse und Informationen zur Abwehr von Bedrohungen	Berichte zu bestimmten Arten von Angriffen oder Eindringversuchen sowie Angaben zur Ursprungsadresse ermöglichen es Administratoren, schnell auf aktuelle Bedrohungen zu reagieren.
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.
Capture ATP-Bericht	Capture bietet ein übersichtliches Bedrohungsanalyse-Dashboard und Berichte mit detaillierten Analyseergebnissen für die an den Service weitergeleiteten Dateien, z. B. Quelle, Ziel und eine Zusammenfassung mit genauen Angaben zu den eingeleiteten Anti-Malware-Maßnahmen.
Botnet-Bericht	Es stehen vier Berichtstypen zur Verfügung: 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	Der Report bietet Informationen zum blockierten Datenverkehr basierend auf dessen Herkunftsland oder Zielort. 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	<p>Hier wird die Media-Access-Control(MAC)-Adresse auf der Berichtsseite angezeigt. Gerätespezifische Informationen (Initiator-MAC und Responder-MAC) werden in fünf Berichtstypen dargestellt:</p> <ul style="list-style-type: none"> • Datennutzung > Initiatoren • Datennutzung > Responder • Datennutzung > Details • Benutzeraktivitäten > Details • Webaktivitäten > Initiatoren
Zentrales Logging	Security-Events und -Protokolle für alle verwalteten Appliances werden zentral konsolidiert. So können von einem einzigen Punkt aus forensische Netzwerkanalysen durchgeführt werden.
Cloudnative Architektur	Enorme Mengen abgefragter Daten lassen sich aus Zehntausenden Firewall-Nodes mit der Geschwindigkeit und Elastizität der Cloud erfassen, kombinieren, verarbeiten, wiederaufbereiten, extrahieren, korrelieren und laden.

Lizenzen und Pakete

	Funktionen	SaaS-Analytics	On-Premises-Analytics
Verwaltung	Back-up/Wiederherstellung – Firewall-System	Ja	Ja*
	Reporting (NetFlow-/IPFIX-basiert)	Ja	Ja*
	Analytics (NetFlow-/IPFIX-basiert)	Nur auf Grundlage lokaler Datei	Nur auf Grundlage lokaler Datei
Reporting	Zeitgesteuerte Berichte, Live-Monitor, zusammenfassende Dashboards	Ja	Ja
	Anzeige und Download von Berichten, etwa zu Anwendungen, Bedrohungen, CFS, Benutzern, Traffic, Quelle/Ziel (1 Jahr Flow-Reporting)	Ja	Ja
Analytics (NetFlow-/IPFIX-basiert)	Forensische Netzwerkanalysen und Threat-Hunting mittels Drill-down und Pivoting	Ja	Ja
	Cloud App Security – Aufspüren von Schatten-IT	Ja	Nein
	Aufbewahrung von Daten	30 Tage	1 Jahr
Technischer Support		24/7-Support	24/7-Support**

* Erfordert den AGSS-/CGSS-Service oder einen anderen bezahlten Capture Security Center-Service

** Erfordert eine Lizenz für 24/7-Support

Mindestanforderungen an das System

Für SonicWall Analytics im SaaS-Modus über den Network Security Manager:

Folgende SonicWall-Appliances werden unterstützt:

- SonicWall Network Security Appliances: NSA Series, NSa Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- SonicWall Network Security Virtual Appliances: NSv 10 bis NSv 400

Unterstützte SonicWall-Firmware

- SonicWall SonicOS 6.0 oder höher

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 On-Premises-Implementierung von SonicWall Analytics:

Virtual Appliance

- Hypervisor: VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V Win 2016
- Empfohlener Arbeitsspeicher: unbegrenzt (mindestens 8 GB)
- Festplatte: OVA-Image erfordert extern angeschlossene 65-GB-Festplatte
- vCPU: 4/unbegrenzt
- Netzwerkschnittstelle: 1
- VMware-Kompatibilitätsleitfaden

Folgende SonicWall-Appliances werden unterstützt:

- SonicWall Network Security Appliances: SuperMassive E10000 und 9000 Series, NSA Series, NSa Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- SonicWall Network Security Virtual Appliances: NSv Series



Erfahren Sie mehr über SonicWall Analytics

www.sonicwall.com/analytics

Über SonicWall

SonicWall bietet grenzenlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Besuchen Sie uns auf www.sonicwall.de oder folgen Sie uns auf [Twitter](#), [LinkedIn](#), [Facebook](#) und [Instagram](#), wenn Sie weitere Informationen wünschen.



SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA

Weitere Informationen erhalten Sie auf unserer Website.

www.sonicwall.com

SONICWALL®

© 2021 SonicWall Inc. ALLE RECHTE VORBEHALTEN.

SonicWall ist eine Marke oder eingetragene Marke von SonicWall Inc. und/oder deren Tochtergesellschaften in den USA und/oder anderen Ländern. Alle anderen Marken und eingetragenen Marken sind Eigentum der jeweiligen Inhaber. Die Informationen in diesem Dokument werden in Verbindung mit den Produkten von SonicWall Inc. und/oder deren Tochtergesellschaften bereitgestellt. Sie erhalten durch dieses Dokument oder in Verbindung mit dem Verkauf von SonicWall-Produkten keine Lizenz (weder ausdrücklich noch stillschweigend, durch Rechtsverwirkung oder anderweitig) für geistige Eigentumsrechte. SONICWALL UND/ODER DESSEN TOCHTERGESELLSCHAFTEN ÜBERNEHMEN KEINE HAFTUNG UND KEINERLEI AUSDRÜCKLICHE, STILLSCHWEIGENDE ODER GESETZLICHE GEWÄHRLEISTUNG FÜR DEREN PRODUKTE, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG FÜR DIE HANDELSÜBLICHKEIT, DIE VERWENDUNGSFÄHIGKEIT FÜR EINEN BESTIMMTEN ZWECK UND DIE NICHTVERLETZUNG VON RECHTEN DRITTER, SOWEIT SIE NICHT IN DEN BESTIMMUNGEN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT NIEDERGELEGT SIND. SONICWALL UND/ODER DESSEN TOCHTERGESELLSCHAFTEN HAFTEN NICHT FÜR IRGENDWELCHE UNMITTELBAREN, MITTELBAREN, STRAFRECHTLICHEN, SPEZIELLEN, ZUFÄLLIGEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN AUS ENTGANGENEM GEWINN, GESCHÄFTSUNTERBRECHUNG ODER VERLUST VON INFORMATION), DIE AUS DER VERWENDUNG ODER DER UNMÖGLICHKEIT DER VERWENDUNG DIESES DOKUMENTS ENTSTEHEN, SELBST WENN SONICWALL UND/ODER DESSEN TOCHTERGESELLSCHAFTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDEN. SonicWall und/oder dessen Tochtergesellschaften übernehmen keine Gewährleistungen in Bezug auf die Genauigkeit oder Vollständigkeit dieses Dokuments und behalten sich das Recht vor, Spezifikationen und Produktbeschreibungen jederzeit ohne Vorankündigung zu ändern. SonicWall Inc. und/oder deren Tochtergesellschaften übernehmen keinerlei Verpflichtung, die in diesem Dokument enthaltenen Informationen zu aktualisieren.