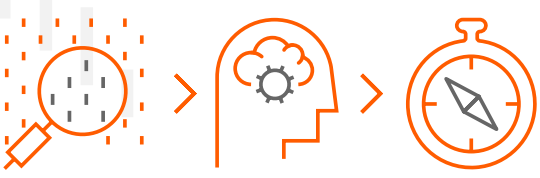
SonicWall Analytics

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 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 Datensätze durch verschiedene Formen semantischer Graphen sowie Diagramme und Tabellen zur Zeitnutzung übersichtlich darstellen. Dies hilft, Datensilos zu reduzieren und das Analystenteam 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

DATENBLATT

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.

Abbildung 1: Management-Dashboard

Analytics enthält eine große Bandbreite vordefinierter Berichte, die sich on demand oder in regelmäßigen Abständen bereitstellen lassen. Darüber hinaus lassen sich ganz flexibel benutzerdefinierte Berichte auf Basis von Parametern und Kennzahlen erstellen, die Sie aus einer umfangreichen Bibliothek von Firewalldatentypen wählen können. Dies ermöglicht es Ihnen, wertvolle Informationen von bestimmten Geräten über ausgewählte Gruppen oder Benutzer hinweg zusammenzuführen und relevante Erkenntnisse daraus zu extrahieren. Mithilfe benutzerdefinierter Berichte lassen sich Datentrichter entrümpeln bzw. vereinfachen. So erhalten Entscheider und Incident-Responder aussagekräftige Erkenntnisse aus einer geringeren Menge hochwertigerer Datensätze. Dieser bessere Überblick kommt ihnen wiederum bei der Traffic-Analyse sowie bei der Identifizierung von Sicherheitslücken und Anomalien zugute: Unter anderem können sie relevante Analysen genauer unter die Lupe nehmen, fundierte Entscheidungen treffen und zeitnahe regelbasierte Maßnahmen auf Grundlage verlässlicher Daten einleiten.

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.

Optimierung der Mitarbeiterproduktivität

Benutzeranalysen bieten Ihnen einen umfassenden und transparenten Überblick über die Webanwendungs- und Internetnutzung Ihrer Mitarbeiter. Analysten können durch Drill-down-Funktionen interessante Datenpunkte flexibel untersuchen. Werden dabei riskante Anwendungen bzw. auffällige Benutzer identifiziert, lassen sich hierfür evidenzbasierte und richtliniengesteuerte Maßnahmen einrichten. Darüber hinaus bieten Produktivitätsberichte einen Einblick in die Internetnutzung und das Verhalten von Mitarbeitern über einen bestimmten Zeitraum. Dank leistungsstarker Snapshots und detaillierter Berichte lassen sich die Webaktivitäten der Nutzer in Produktivitätsgruppen wie „produktiv“, „unproduktiv“, „akzeptabel“ und „inakzeptabel“ oder auch in benutzerdefinierte Gruppen einteilen. Auf diese Weise erhalten Organisationen einen besseren Einblick in die Internetnutzung und können diese effektiver überwachen.

Flexible Implementierung mit SaaS-, virtuellen oder IaaS-Optionen

Analytics bietet Ihnen flexible Implementierungsoptionen, die optimal auf Ihre operativen Anforderungen abgestimmt sind. Unter anderem ist Analytics als wartungsfreie Option verfügbar: Hier ist die Lösung in das von SonicWall gehostete SaaS-Angebot Network Security Manager (NSM) integriert und kann einfach über das Internet aufgerufen werden. Dank der unbegrenzten Elastizität können Sie die SaaS-Lösung bei Bedarf skalieren und gleichzeitig Ihre Betriebskosten senken. Die typischen Ausgaben für den Kauf von Hardware und Software sowie für die benutzerdefinierte Installation, regelmäßige Wartungsaktivitäten und Upgrades, Abschreibungen und Außerbetriebnahme entfallen; stattdessen fällt eine niedrige, vorhersehbare jährliche Abogebühr an.

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

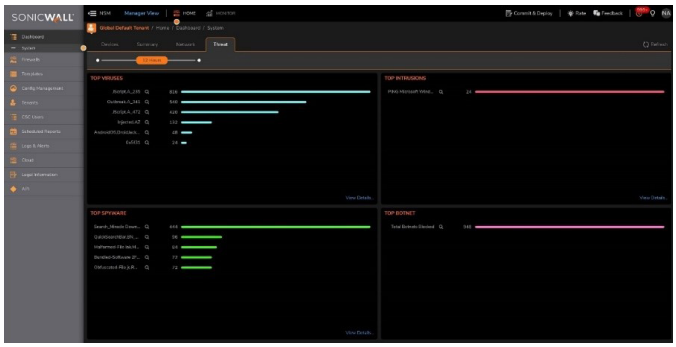


Abbildung 2: Bedrohungsübersicht

Die Funktionen im Überblick

Funktion	Beschreibung
Benutzeranalysen	Ein interaktives Dashboard bietet einen umfassenden Überblick über die Netzwerk- und Anwendungsnutzung der Mitarbeiter sowie über Bedrohungen. Werden riskante Webaktivitäten identifiziert, können Sie durch einen granularen 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	Leistungsstarke Snapshots und Drill-down-Berichte zum Internetverhalten der User bieten umfassende Einblicke in die Nutzung von Internetressourcen innerhalb der Organisation.

Funktion	Beschreibung
Benutzerdefinierte Berichte	Über einen selbstgesteuerten Workflow lassen sich benutzerdefinierte Berichte mit ausgewählten Parametern und Kennzahlen erstellen, die aus einer Bibliothek von Firewalldatentypen ausgewählt werden.
Berichte auf Nutzer- und Gruppenebene	Vordefinierte oder benutzerdefinierte Berichte lassen sich auf Ebene der Gerätegruppen oder Nutzer aufrufen.
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	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. • 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 (nur für Analytics 2.5)	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 SonicWall-Sicherheitsservices Capture ATP, Gateway-Anti-Virus, Anti-Spyware, Intrusion-Prevention sowie Application Intelligence and Control erkannt wurden, können unmittelbar dargestellt werden.
Aktuelle Informationen zu 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.
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

Reporting				
Feature	SaaS-Analytics für NSM Essential	SaaS-Analytics für NSM Advanced	On-Premises-Analytics	On-Premises-Analytics
Log/Protokoll	NetFlow-/IPFIX-basiert[1]	NetFlow-/IPFIX-basiert[1]	NetFlow-/IPFIX-basiert[1]	Syslog-basiert[1]
Dashboard auf Gruppen-/Nutzerebene	Ja	Ja	Nein	Nein
Capture ATP (Geräteebene)	Ja	Ja	Ja	Ja
Capture Threat Assessment (CTA) (Geräteebene)	Ja	Ja	Ja	Nein
Produktivitätsberichte[3]	Nein	Ja	Nein	Nein
VPN-Berichte	Nein	Ja	Nein	Ja
Benutzerdefinierte Berichte	Nein	Ja	Ja	Ja
Zeitgesteuerte Berichte (Flow, Syslog, CTA oder Management)	Ja (ausgenommen Flow)	Ja	Ja	Ja
Zeitraum der Berichtsdaten	7 Tage	365 Tage	365 Tage	365 Tage
Analysen				
Zeitraum der Analysedaten	-	30 Tage	90 Tage	90 Tage
Nutzerbasierte Analysen	Nein	Ja	Ja	Ja
Anwendungsanalysen	Nein	Ja	Ja	Ja
Forensische Netzwerkanalysen und Threat-Hunting mittels Drill-down und Pivoting	Nein	Ja	Ja	Ja
Technischer Support	24/7-Support	24/7-Support	24/7-Support[2]	24/7-Support[2]

[1] Erfordert den AGSS-/CGSS-Service oder einen anderen bezahlten Capture Security Center-Service.
[2] Erfordert eine Lizenz für 24/7-Support.
[3] Erfordert eine aktivierte AGSS-/CGSS-Lizenz auf Firewalls der Generation 6/6.5 sowie eine Essential-Protection-Lizenz auf Firewalls der Generation 7.

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, NS*a* Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- SonicWall Network Security Virtual Appliances: NS*v* 10 bis NS*v* 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

Unterstützte SonicWall-Firmware

- SonicWall SonicOS 6.0 oder höher

Folgende SonicWall-Appliances werden unterstützt:

- SonicWall Network Security Appliances: NS*sp*, SuperMassive E10000 und 9000 Series, NSA Series, NS*a* Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- SonicWall Network Security Virtual Appliances: NS*v* 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 großen Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Weitere Informationen erhalten Sie unter www.sonicwall.de.

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

Datasheet-Analytics-A4-JK-8806