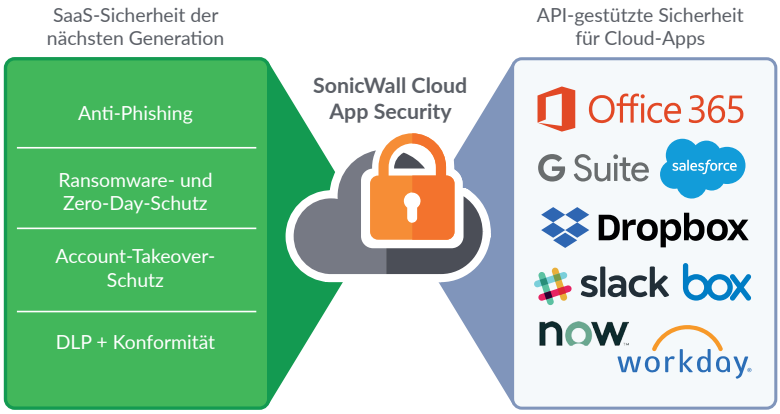
SONICWALL

SonicWall Cloud App Security

SonicWall Cloud App Security liefert Sicherheit der nächsten Generation für SaaS-Anwendungen wie Office 365 und G Suite. Damit werden E-Mail, Daten und Anmeldedaten vor komplexen Bedrohungen geschützt, während gleichzeitig für Konformität in der Cloud gesorgt wird. Für Ihren Umzug in die Cloud bietet SonicWall die Best-in-Class API-basierte Sicherheit, verbunden mit einem niedrigen TCO-Aufwand, minimalen Allgemeinkosten für die Implementierung und den Vorteil einer nahtlosen Benutzererfahrung.



Visualisierung: Erkennung aller (genehmigten und nicht genehmigten) Cloud-Dienste, die von den Mitarbeitern einer Organisation genutzt werden. Hierbei wird auch der Ost-West-Verkehr (Cloud zu Cloud) untersucht, weil Nutzer anhand von zulässiger IT wie Office 365 auf nicht genehmigte Apps authentisieren können.

E-Mail-Sicherheit der nächsten Generation. Da E-Mail zu den gefragtesten SaaS-Anwendungen gehört, ist der Schutz des beliebten Bedrohungsvektors maßgebend für die SaaS-Sicherheit. Die Lösung umfasst das Sandboxing von Anhängen, erweiterte URL-Analysen und Schutz vor Beeinträchtigung des geschäftlichen E-Mail-Verkehrs.

Schutz vor komplexen Bedrohungen: Verhindert die Verbreitung von Malware über Cloud-Anwendungen wie OneDrive, Box und Dropbox durch einen Echtzeit-Antivirus-Scan auf bekannte Bedrohungen und Capture ATP-Sandboxing zur Identifizierung von Zero-Day- und unbekannten Bedrohungen.

Datensicherheit: Setzen Sie datenzentrierte Sicherheitsrichtlinien mit engmaschigen Zugangskontrollen und mit der Vorbeugung gegen das Hochladen sensibler oder vertraulicher Dateien durch. Die Lösung enthält rollenbasierte Richtlinien-Tools, Datenklassifizierung und Technologien zur Vorbeugung gegen Datenverlust, die die Bewegungen der Nutzer überwachen und ihren Zugang sperren oder einschränken.

Konformität: Die Lösung sieht eine sorgfältige Prüfung sämtlicher Bewegungen in Echtzeit sowie bereits erfolgter Ereignisse vor und bietet einfache Vorlagen zur Vorbeugung gegen Datenverlust, damit Sie Richtlinienkontrollen und die Einhaltung behördlicher Vorschriften in Echtzeit durchsetzen können.

Vorteile:

E-Mail-Sicherheit der nächsten Generation

- Stoppt Ransomware, Zero-Day-Attacken und gezielte Phishing-E-Mails, bevor diese den Posteingang der Benutzer erreichen
- Schützt vor komplexen Bedrohungen durch Sandboxing von Anhängen und erweiterten URL-Analysen
- Scannt die ein- und abgehenden sowie alle internen E-Mails in Office 365 und G Suite
- Nutzt Machine Learning und künstliche Intelligenz (KI), um Identitätsfälschungen abzuwehren
- Entfernt schädliche E-Mails auch nach Ankunft im Posteingang der Benutzer

SaaS-Sicherheit der nächsten Generation (CASB)

- Sorgt für granuläre Visualisierung und Kontrolle von genehmigten IT-Systemen und Schatten-IT-Systemen
- Bietet umfassenden Schutz für den Verkehr vom Benutzer zur Cloud und von Cloud zu Cloud
- Verhindert das Hochladen sensibler Daten und den unberechtigten Austausch von Dateien
- Legt einheitliche Datensicherheits-richt-linien für alle genehmigten Anwendungen fest
- Schützt vor Account-Takeovers (ATO), Insiderbedrohungen und Gefahren durch kompromittierte Zugangsdaten
- Stoppt die Verbreitung von Ransomware und Zero-Day-Malware in der Cloud
- Sorgt durch einfache DLP-Vorlagen für die Durchsetzung behördlicher Konformitätsrichtlinien
- Identifiziert Sicherheitsverletzungen und Sicherheitslücken durch eine Analyse historischer und Echtzeitvorfälle

Sicherheit – unkompliziert und erschwinglich

- Liefert ein nahtloses Benutzererlebnis beim Zugriff von jedem Gerät und von jedem beliebigen Standort aus
- Eliminiert Schwachstellen, Latenzprobleme und die Notwendigkeit von Verkehrsumlei-tungen mittels Proxy
- Automatisiert die automatische Erkennung von Cloud-Anwendungen, wenn zusammen mit SonicWall NGFW implementiert
- Reduziert die Total Cost of Ownership (TCO) auf ein Minimum, lässt sich schnell implementieren und leicht verwenden

Lösungsüberblick

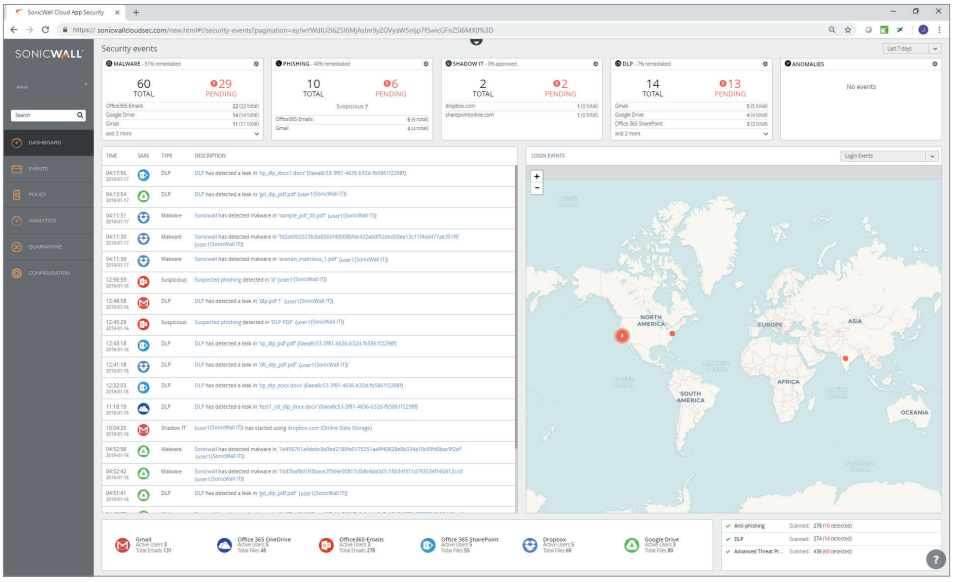
SonicWall Lösungsbeschreibung

SonicWall Cloud App Security sorgt für Out-of-Band-Scanning des an genehmigte und nicht genehmigte SaaS-Anwendungen gehenden Verkehrs durch Verwendung von APIs und Analysen der Verkehrsprotokolle.

Die Lösung bietet eine nahtlose Integration mit den genehmigten SaaS-Anwendungen durch Einsatz nativer APIs und bietet CASB-Funktionalitäten, wie Visualisierung, Schutz vor komplexen Bedrohungen, Schutz vor Datenlecks (DLP) und Konformität. Bei Einsatz mit einer Firewall der nächsten Generation (NGFW) von SonicWall bietet Cloud App Security auch Visualisierung und Kontrolle von Schatten-IT für die Cloud-Nutzung im Netzwerk.

Mit dieser Lösung können IT-Abteilungen SaaS-Anwendungen einführen, ohne irgendwelche Beeinträchtigung der Sicherheit und Konformität befürchten zu müssen. Administratoren können von einer zentralen Stelle aus für alle unternehmensweiten SaaS-Anwendungen einheitliche Richtlinien festlegen. Durch Verwendung der verfügbaren DLP- und Compliance-Reporting-Vorlagen können Sicherheitslücken schnell geschlossen und für den geschäftlichen oder behördlichen Bedarf angepasste Richtlinien eingesetzt werden. Diese Lösung lässt sich ohne zusätzliche Installation und Verwaltung von Hardware genau auf Ihren Bedarf zuschneiden – egal ob Sie ein paar hundert oder weltweit hunderttausend Mitarbeiter beschäftigen.

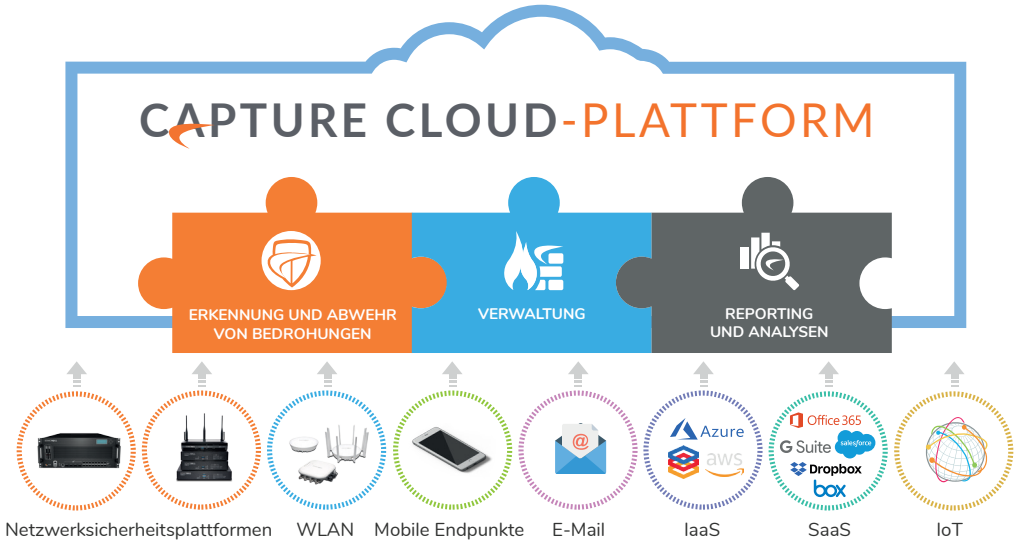
API-gestützte SaaS-SaaS-Sicherheit mit CASB-Funktionalität



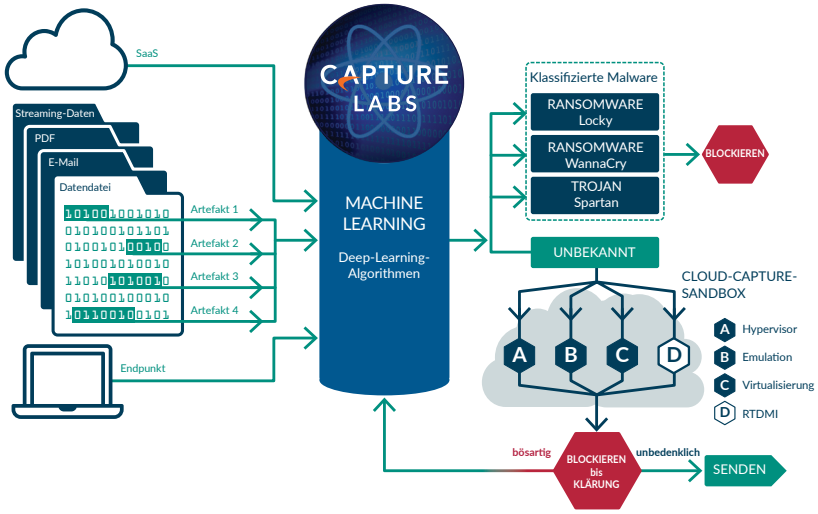
Das Echtzeit-Dashboard ermöglicht Administratoren die Überwachung risikobehafteter Anwendungen, Verfolgung der Benutzeraktivitäten, des Transaktionsvolumens und des Ortes, von dem aus die Anwendung verwendet wird. Die Lösung sorgt für eine sichere Annahme von SaaS-Anwendungen ohne Auswirkung auf die Produktivität der Mitarbeiter.

Integriert in die SonicWall Capture Cloud Plattform

SonicWall Cloud App Security ist ein Cloud-nativer, in die Capture Cloud-Plattform integrierter Security-Service, der durch das Capture Security Center bereitgestellt wird. Die Capture Cloud-Plattform von SonicWall bietet kleinen wie großen Organisationen eine Cloud-basierte Lösung für Bedrohungsschutz und Netzwerkverwaltung sowie Reporting und Analysen. Die Plattform konsolidiert Bedrohungsinformationen aus mehreren Quellen, zum Beispiel aus unserem prämierten Multi-Engine-Netzwerk-Sandboxing-Service Capture Advanced Threat Protection sowie aus über 1 Million SonicWall Sensoren, die rund um den Globus verteilt sind. Das Capture Security Center bietet eine zentrale Stelle für die Verwaltung, über die Administratoren auf einfache Weise historische und Echtzeitberichte über die Bewegungen im Netzwerk und in der Cloud erstellen können.



Zum Schutz von SaaS-Anwendungen nutzt SonicWall Cloud App Security die SonicWall Capture Cloud Plattform, die das globale Sicherheitswissen des Capture Threat Network und die Prävention moderner Bedrohungen der mehrere Engines umfassenden Sandbox Capture ATP kombiniert. Mit diesem Ansatz kann SonicWall seine Fähigkeiten bei der in Echtzeit ausgeführten automatischen Einbruchsverhinderung in SaaS-Umgebungen erweitern und Unternehmen einen sicheren Umzug in die Cloud ermöglichen. Native APIs werden direkt in die Cloud-Dienste integriert. Dadurch kann die Lösung auch Dateien in Anwendungen wie OneDrive oder Dropbox mittels dem Capture ATP Service und Real-Time Deep Memory Inspection™ (RTDMI™) scannen, um Ransomware und Zero-Day-Attacken noch vor dem Eindringen in das Netzwerk zu stoppen.



Umfassende Sicherheit für Office 365 und G Suite

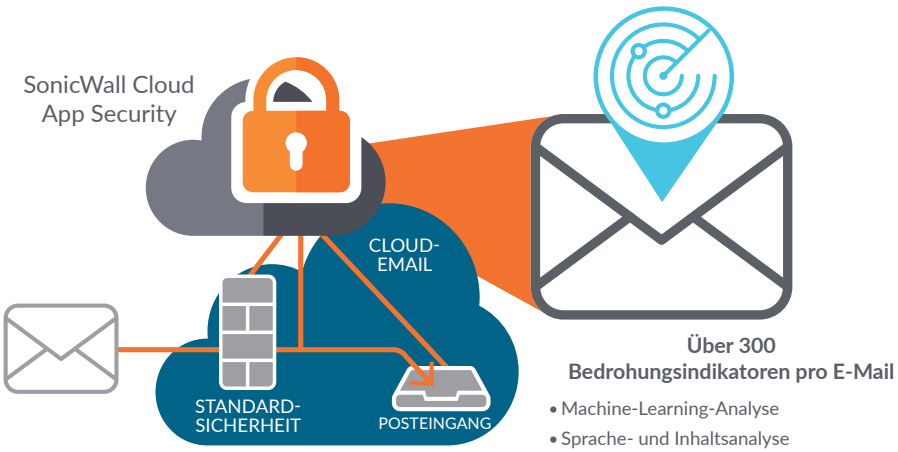
Sicherheit der nächsten Generation für Cloud-E-Mail

SonicWall Cloud App Security bietet E-Mail-Sicherheit der nächsten Generation, die speziell für Cloud-E-Mail-Plattformen ausgeführt ist. Wenn Organisationen ihre E-Mail in die Cloud verlagern, verlassen sie sich in der Regel entweder ausschließlich auf die eingebaute Sicherheit des Anbieters oder ergänzen diese mit einem herkömmlichen MTA-Proxy. Externe E-Mail-Gateways können aber eventuell nicht alle heutigen Bedrohungen erkennen und abwehren.

Neben den herkömmlichen E-Mail Sicherheitsstufen SPF, DKIM und DMARC sowie URL-Filterung durch Nutzung von drei zentralen Datenquellen für URL-Blacklists bietet die einzigartige Cloud App Security-Architektur einen speziellen Schutz, der von keiner externen Gateway-Lösung geboten werden kann:

- Eine zusätzliche Stufe für erweiterten Bedrohungsschutz: Cloud App Security blockiert Phishing-Nachrichten, die von Office 365 und G Suite nicht erfasst werden. Diese Lösung verwendet Machine Learning, künstliche Intelligenz und Big-Data-Analysen für die Bereitstellung eines leistungsstarken Schutzes vor Gefahren wie Phishing, Sandboxing von Anhängen, erweiterten URL-Analysen und Identitätsfälschung.
- Überwachung ein- und abgehender sowie interner E-Mails: Cloud App Security integriert SaaS, so dass jede E-Mail vor Erreichen des Postkastens des jeweiligen Benutzers gescannt und in Quarantäne gesetzt werden kann – egal, ob die E-Mail von außerhalb der Organisation oder von einem kompromittierten internen Konto stammt.
- Scannt ältere Nachrichten auf Bedrohungen: Bei der erstmaligen Verbindung scannt Cloud App Security auch ältere Nachrichten (und sogar geschlossene E-Mail-Konten) auf potenzielle Einbrüche oder kompromittierte Konten.
- Globaler E-Mail-Rückruf: Schädliche E-Mails können jederzeit bearbeitet oder zurückgerufen werden, einschließlich bösartiger Nachrichten, E-Mails, die vertrauliche Daten enthalten oder wegen einer unbeabsichtigten Absendung.

Da Cloud App Security den E-Mail-Schutz vor Ankunft der E-Mail im Postkasten des Benutzers, aber nach Passieren der nativen Microsoft- oder Google-Filter (sowie nach jedem eventuell eingebundenen externen MTA-Gateway) anwendet, sind die Machine-Learning-Algorithmen dieses Systems einzigartig auf die Bedrohungen ausgerichtet, die von den anderen Filtern nicht erfasst werden. Des Weiteren kann Cloud App Security die Ergebnisse der nativen Scans in seine eigenen Erkennungsalgorithmen integrieren.



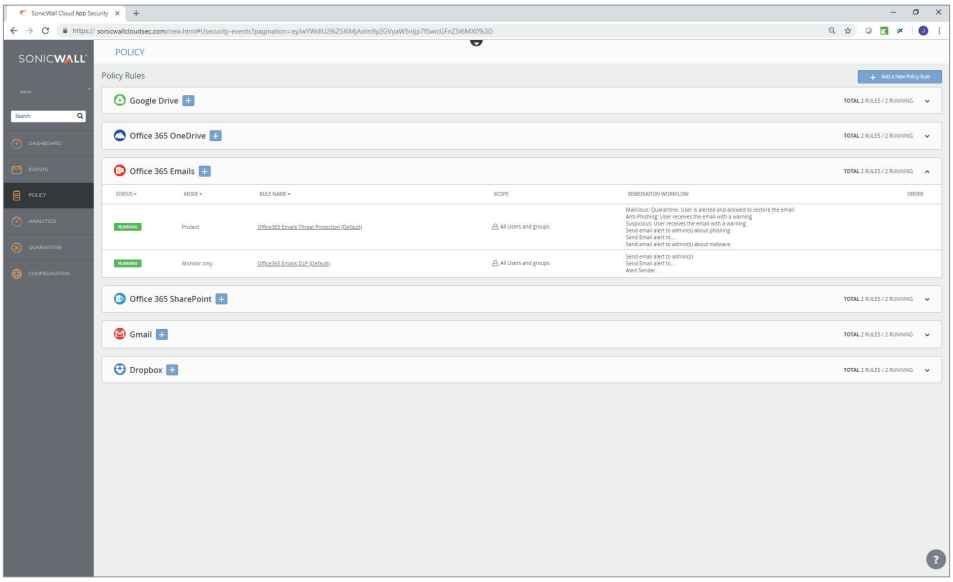
Virtueller In-line-Schutz stoppt schädliche Nachrichten, bevor diese den Posteingang des Benutzers erreichen

Sicherheit der nächsten Generation für die komplette Produktivitäts-Suite

Cloud App Security bietet umfassende Defense-in-Depth-Sicherheit für Office 365 oder G Suite. Ob für E-Mail, Share-Drives, IMs oder komplette Kollaborationssysteme, diese Lösung hilft Ihnen bei der Durchführung folgender Sicherheitsmaßnahmen:

- Verhindern einer Ausbreitung von Phishing und Malware innerhalb Ihrer Organisation oder auf Ihre Kunden und Partner.
- Prüfung jeder Datei auf schädlichen Inhalt unter Verwendung von Capture ATP Sandboxing sowie Analyse von aktivem Inhalt, um Bedrohungen in Quarantäne zu setzen, bevor sie von einem Benutzer heruntergeladen werden.
- Identifizieren vertraulicher Informationen und Anwendung von Cloud-Aware-Richtlinien, um solche Informationen innerhalb der Organisation oder Arbeitsgruppe zu halten. Ihre Benutzer können die volle Leistung der Cloud-basierten Produktivitäts-Suite nutzen, während automatische Workflows für die behördliche Konformität sorgen und sicherstellen, dass PCI, HIPAA, PII oder andere vertrauliche Daten nicht extern weitergegeben werden.

Umfassender Schutz für die komplette Cloud-basierte Office-Suite



Jede SaaS-Anwendung hat eine völlig andere Policy-Engine mit eigenen Regeln und Durchsetzungsfunktionen. Die Lösungen von SonicWall protokollieren diese über alle genehmigten SaaS-Anwendungen hinweg und ermöglichen somit eine detailliertere Kontrolle. So ermöglicht Ihnen Cloud App Security die Erstellung einer einzelnen Richtlinie, die auf einheitliche Weise für alle Anwendungen zur Anwendung kommt.

Diese kontextbewussten Richtlinien ermöglichen die Erstellung von Durchsetzungsabläufen, bei denen Benutzer über das vorliegende Problem und richtiniengemäße sichere Alternativen informiert werden, während zugleich weit über die normalerweise in den SaaS zulässigen Genehmigungskontrollen hinausgehende Prüfungen durchgeführt werden.

SaaS-Sicherheit

SonicWall Cloud App Security bietet folgende Schutzfunktionen für die Sicherung des SaaS-Umfelds in Unternehmen:

Sicherheit von genehmigten IT-Systemen – Wird direkt in die Cloud-Dienste integriert und nutzt APIs für den Schutz vor komplexen Bedrohungen und die Verhinderung von Datenverlust innerhalb der SaaS-Umgebungen.

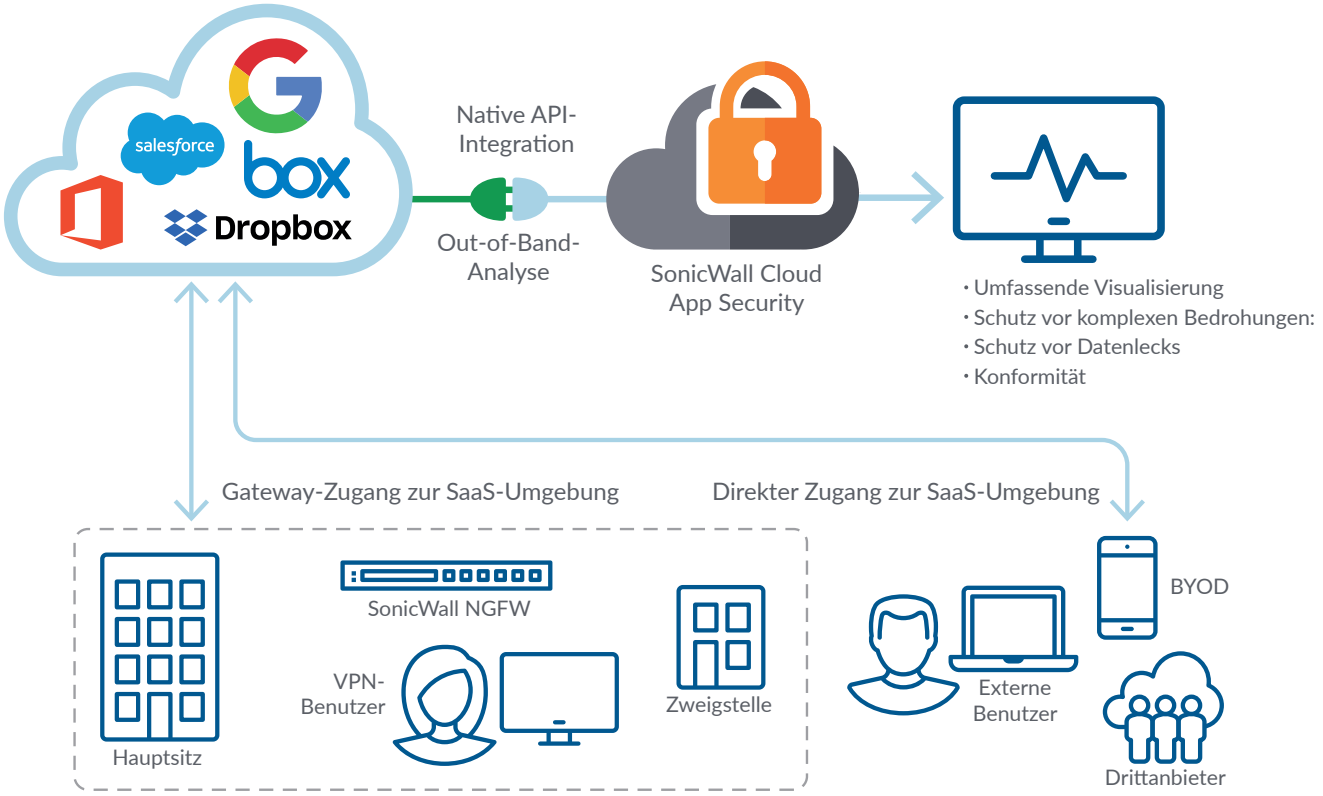
Visualisierung und Kontrolle von Schatten-IT-Systemen – Ist nahtlos mit SonicWall NGFW integriert und sorgt für die automatische Erkennung und Risikobewertung von Cloud-Anwendungen unter Verwendung einer Verkehrsprotokollanalyse.

Sicherheit genehmigter IT-Systeme

Bei Verwendung von SaaS-Anwendungen wie Box und Dropbox ist das Unternehmen – nicht der Cloud-Service-Anbieter (CSP) – für die letztendliche Sicherheit aller Daten verantwortlich. Dies wird oft im Kleingedruckten der Serviceverträge festgelegt und entbindet die CSPs von jeglicher Haftung im Fall eines Datenlecks oder einer Infektion oder Verbreitung von Malware. Deshalb müssen Unternehmen, die solche Anwendungen nutzen, eine Lösung für die Inspektion der Daten in den Cloud-Anwendungen implementieren.

Nur API-basierte Lösungen können ruhende Daten innerhalb von SaaS-Anwendungen untersuchen, weil proxybasierte Lösungen inline nur die Daten untersuchen, die von der geschützten Seite einer Firewall in die Cloud hochgeladen werden. Weil viele Organisationen bereits eine große Menge Daten in der Cloud gespeichert haben, werden API zur Durchsetzung von Richtlinien zu diesen Daten eingesetzt. Andere Fähigkeiten – die nur laufen, wenn eine direkte Verbindung zu einer App über API hergestellt wird – umfassen die Prüfung der Sicherheitskonfigurationseinstellungen in der App und die Empfehlung von Änderungen zur Erhöhung der Sicherheit sowie die Prüfung der gemeinsamen Zugriffsgenehmigungen auf Dateien und Ordner, um das Zugangsrisiko von Dritten oder Fremden auf Unternehmensdaten beurteilen zu können. Die Lösung bietet eine detaillierte Sicht, hohen Schutz vor Bedrohungen mit der Capture ATP Sandbox und Vorbeugung gegen Datenverlust für SaaS-Anwendungen wie cloudbasierte E-Mail und Apps zur Datenfreigabe und zur Speicherung in der Cloud wie Google G Suite und Microsoft Office 365.

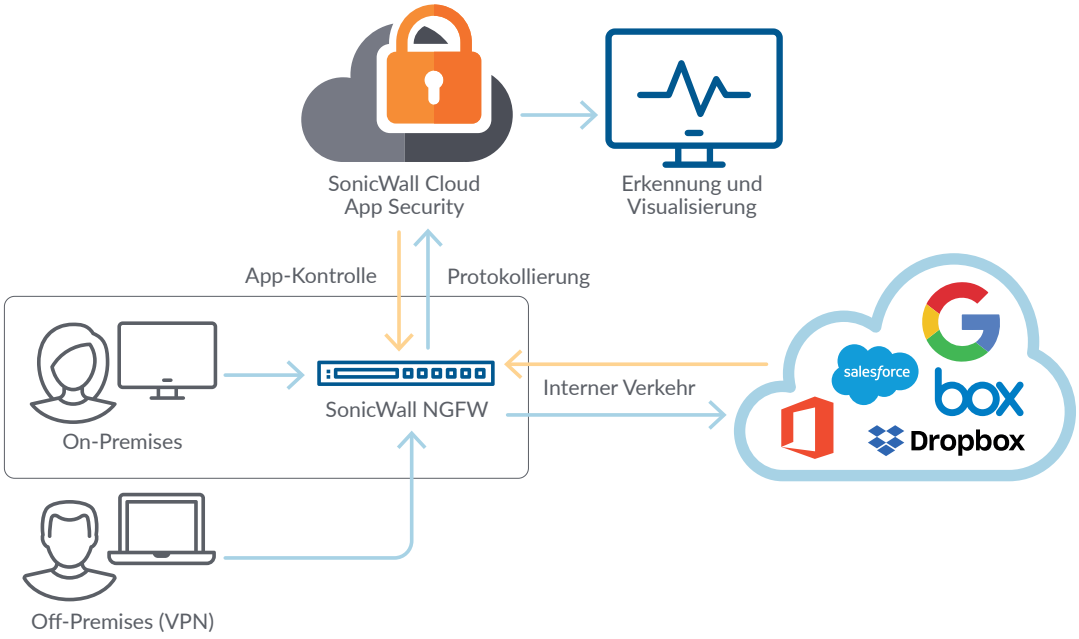
SonicWall Cloud App Security analysiert den gesamten Verkehr (Ereignisprotokoll, Nutzeraktivitäten, Datendateien und Objekte, Konfigurationszustand usw.) und setzt die notwendigen Sicherheitsrichtlinien über direkte Integrationen mit den nativen APIs des Cloud-Dienstes durch. Da die Lösung native APIs nutzt, ist keine Proxy- oder Inline-Anfrage zwischen dem Benutzer und der Cloud erforderlich. Damit kann die Lösung unabhängig vom Gerät oder Netzwerk des Nutzers die genehmigten Apps abdecken. Dieser API-basierte Ansatz ermöglicht außerdem eine leichte Einbindung sowie granulare Kontrolle ohne Beeinträchtigung der Benutzererfahrung.



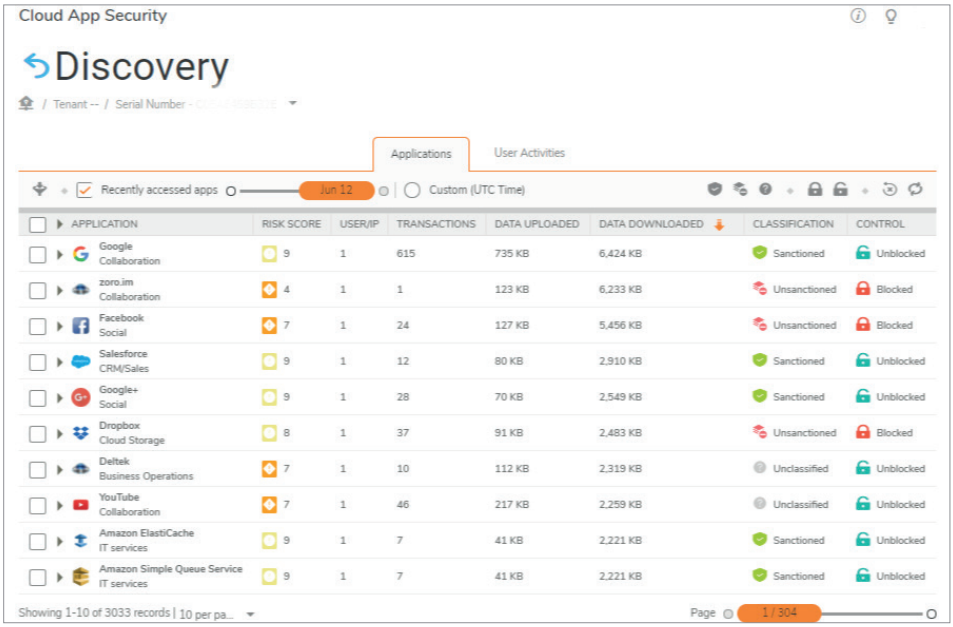
Sichere genehmigte SaaS-Anwendungen

Visualisierung und Kontrolle von Schatten-IT

Die Next-Generation-Firewalls von SonicWall analysieren und protokollieren den gesamten Datenverkehr, der ins Netzwerk gelangt oder dieses wieder verlässt. Protokolle, die für ausgehende Verkehrsdaten generiert wurden, sind nicht in der Lage, präzise zwischen den genutzten Cloud-Anwendungen zu unterscheiden oder das Risiko für Anwendungen einzustufen, die von den Mitarbeitern eingesetzt werden. Bei Remote-Mitarbeitern, die über eine Next-Generation-Firewall mittels VPN weitergeleitet werden, nutzt die Lösung diese Protokolle, um zusätzliche Details zu den Aktivitäten der Nutzer innerhalb der Cloud-Services zu sammeln. Cloud App Security verarbeitet Protokolldateien der SonicWall-Next-Generation-Firewalls und gibt an, welche Cloud-Services von welchen Usern genutzt werden, welche Daten in die Cloud geladen bzw. aus der Cloud heruntergeladen werden und welches Risiko bzw. welche Kategorie jeder Cloud-Service hat. Im Grunde sorgt Cloud App Security für eine robuste Cloud-Unterstützung über die gesamte bestehende Infrastruktur hinweg. Gerade bei Mitarbeitern, die Cloud-Anwendungen immer mehr zu Arbeitszwecken einsetzen, ermöglicht Cloud App Security Administratoren, Lücken in der Sicherheitsstrategie aufzudecken, Cloud-Anwendungen in genehmigte und nicht genehmigte IT-Anwendungen zu unterteilen und Zugriffsregeln umzusetzen, um risikoreiche Anwendungen zu blockieren. Cloud App Security ist ein wichtiger Teil der Vision von SonicWall, die eine Bereitstellung automatischer Einbruchserkennung und -verhinderung in Echtzeit für Kunden, die auf die Cloud-Technologien umsteigen, umfasst.



Entdeckung von Schatten-IT-Systemen in Ihrem Netzwerk



SonicWall Cloud App Security erkennt und meldet gefährliche Schatten-IT-Dienste unter Verwendung einer exklusiven Reputation Cloud-Services-Datenbank, die von SonicWall gepflegt wird.

Den erkannten Anwendungen wird neben den Sicherheits- und Konformitätszertifikationen ein aus einem Reputationsalgorithmus gewonnener Risikoscore zugewiesen. IT-Administratoren können die Anwendungen auf Basis des Risikoscores als genehmigte oder nicht genehmigte IT-Anwendungen für die Verwendung freigeben. Die Lösung ermöglicht den Administratoren, durch das Capture Security Center Sperrungs- und Entsperrungsrichtlinien festzusetzen und Schatten-IT-Aktivitäten im Netzwerk zu kontrollieren.

Funktionen

FUNKTION		VORTEIL
Visualisierung	Erkennung von Cloud-Anwendungen	Automatische Erkennung von Cloud-Anwendungen durch Nutzung der SonicWall Firewall-Protokolldateien für die Identifizierung von Schatten-IT-Aktivitäten im Netzwerk
	Visualisierung der Cloud-Nutzung	Visualisierung der verwendeten Anwendungen, des Verkehrsvolumens, der Benutzeraktivitäten und des Verwendungsortes in Echtzeit
	Bewertung des Anwendungsrisikos	Informierte Entscheidungen in Bezug auf die Sperrung/Entsperrung von Anwendungen auf Basis der Risikobewertung
	Event-Überwachung	Überwachung aller Aktionen, einschließlich historischer und Echtzeitereignisse in Ihrer SaaS-Umgebung
E-Mail-Sicherheit der nächsten Generation	Anti-Phishing	Gezielte Phishing-Attacken, welche die in Office 365 oder G Suite angebotene Standardsicherheit umgehen können, werden gestoppt
	Anti-Spoofing	Schutz für Ihre Unternehmensmarke und Ihre Benutzer vor E-Mail-Betrug und Identitätsfälschungen
	Sandboxing von Anhängen	Abwehr von schädlichen E-Mail-Anhängen, bevor diese den Posteingang des Benutzers erreichen
	Erweiterter URL-Schutz	Schutz der Benutzer vor bösartigen eingebetteten URLs
Schutz vor komplexen Bedrohungen	Schutz vor Zero-Day-Malware	Verhindert die Speicherung und Verbreitung von Malware durch Anwendungen wie Box, Dropbox, OneDrive und G Drive
	Account-Takeover-Schutz	Schutz der SaaS-Anmeldedaten durch Erkennung von anomalem Benutzerverhalten, Verstöße gegen Berechtigungen oder Konfigurationsänderungen
Datensicherheit	Datenklassifizierung	Identifizierung von sensiblen oder vertraulichen Daten und Anwendung der Richtlinien bei allen SaaS-Anwendungen, um den Austausch dieser Informationen zu kontrollieren-
	Datenzentrische Zugangskontrolle	Verwaltung der Dateiberechtigungen nach Benutzerrolle und der in der Datei enthalten Art von Daten
	Abhilfeablauf	Durchsetzung in Echtzeit, um sicherzustellen, dass der Geschäftsablauf nicht beeinträchtigt wird
Konformität	Konformitäts-Vorlagen	Reduzierung des administrativen Aufwands durch Verwendung einfacher Konformitäts-Vorlagen zur Erfüllung der SOX, PCI, HIPAA und DSGVO
	Audit-Trail	Zugang zu historischen Event-Daten für die retrospektive Konformitätsprüfung und Echtzeit-Reporting
	Richtliniendurchsetzung	Durchsetzung der Konformität in Echtzeit durch Kontrolle jeder SaaS-Anwendung auf Zugangsberechtigungen, Dateiverschiebungen, E-Mail-Sperrung und -Bearbeitung sowie Kommunikation mit Benutzern und Administratoren

SonicWall Cloud App Security	CLOUD APP SECURITY – BASIC	CLOUD APP SECURITY – ADVANCED
Unified Cloud Management (Capture Security Center)	●	●
Unterstützte Cloud-Anwendungen	Wählen Sie 1 SaaS-Anwendung (Office 365 oder G Suite)	Wählen Sie bis zu 10 SaaS-Anwendungen
Anti-Phishing für O365 Mail oder Gmail	●	●
Capture ATP* für E-Mail-Anhänge	●	●
Erweiterter URL-Schutz	●	●
Capture ATP* für in SaaS gespeicherte Dateien	●	●
Account-Takeover-Schutz	●	●
Schutz vor Datenlecks	—	●
Visualisierung von Schatten-IT**	—	●

SonicWall Capture ATP beinhaltet Real-Time Deep Memory Inspection™ (RTDMI™)
***Erfordert SonicWall NGFW*

Bestellinformationen für Cloud App Security:

Bestellinformationen und Preise für Cloud App Security erfragen Sie bitte bei Ihrem Partner oder bei SonicWall Sales hier.

Klicken Sie hier, um eine 30-tägige kostenlose Probeversion von SonicWall Cloud App Security – Advanced zu erhalten

Für weitere Informationen über Cloud App Security besuchen Sie bitte www.sonicwall.com/casb.

Partner Enabled Services

Brauchen Sie Hilfe bei der Planung, Einbindung oder Optimierung Ihrer SonicWall-Lösung? SonicWall Advanced Services Partners sind umfassend ausgebildet, um Ihnen erstklassigen professionellen Service zu bieten. Weitere Informationen finden Sie auf www.sonicwall.com/PES.

Über SonicWall

SonicWall kämpft seit über 27 Jahren gegen Cyberkriminalität und verteidigt kleine und mittelständische Betriebe, größere Unternehmen und Regierungsbehörden weltweit. Unsere preisgekrönten Lösungen zur Erkennung und Prävention von Datenschutzverletzungen in Echtzeit bauen auf der Forschung aus den SonicWall Capture Labs auf und sichern mehr als eine Million Netzwerke sowie E-Mails, Anwendungen und Daten in mehr als 215 Ländern und Gebieten. Die betreffenden Organisationen können sich besser auf ihr Geschäft konzentrieren und müssen sich weniger um ihre Sicherheit sorgen. Weitere Informationen finden Sie auf www.sonicwall.com oder folgen Sie uns auf Twitter, LinkedIn, Facebook und Instagram.

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

Datasheet-CloudAppSecurity-US-VG-MKTG5359