Hosted Email Security

Ein Cloud-basierter, mandantenfähiger Sicherheitsservice, der Schutz vor den hoch entwickelten E-Mail-Bedrohungen von heute bietet

E-Mails sind für große wie kleine Organisationen weltweit das wichtigste Medium für die geschäftliche Kommunikation – doch leider auch der Bedrohungsvektor Nr. 1 für Cyberangriffe. E-Mail-Bedrohungen haben sich von Massen-Spammails und Phishing-E-Mail-Kampagnen zu zielgerichteten Phishing-Angriffen weiterentwickelt, die Ransomware und Zero-Day-Malware übertragen können. Diese Attacken sind häufig auch als Business-E-Mail-Compromise (BEC)-Angriffe getarnt und haben das Ziel, die Überweisung von Geldbeträgen anzustoßen oder an vertrauliche Informationen zu gelangen. Herkömmliche Anti-Spam- und Anti-Malware-Lösungen können diese neue Welle raffinierter Phishing-Angriffe nicht stoppen. Darüber hinaus sind Unternehmen laut Gesetz verpflichtet, vertrauliche Daten zu schützen, einen sicheren Austausch sensibler Kundendaten oder vertraulicher Informationen über E-Mail zu gewährleisten und zu verhindern, dass vertrauliche Daten in fremde Hände geraten.

Um sich vor ständig wechselnden E-Mail-Bedrohungen zu schützen, brauchen Organisationen eine mehrstufige Sicherheitslösung, die weit mehr bietet als Schutz vor Spam und Malware. Eine solche Lösung sollte spezielle hoch entwickelte Schutzfunktionen umfassen und vor böswilligen Anhängen, URLs und betrügerischen Angriffen schützen. Die Verwaltung und Wartung einer lokalen E-Mail-Sicherheitslösung kann sich zu einer kostspieligen und zeitaufwändigen Aufgabe entwickeln. Organisationen tun gut daran, ihre veralteten Produkte mit einer benutzerfreundlichen, erschwinglichen gehosteten E-Mail-Sicherheitslösung zu ersetzen, die sich einfach mit der bestehenden E-Mail-Infrastruktur integrieren und innerhalb kurzer Zeit ohne Vorabkosten bereitstellen lässt. Darüber hinaus sollte die Lösung in der Lage sein, dynamisch auf neue Bedrohungen zu reagieren und die laufenden Administrationskosten sowie den Verwaltungsaufwand zu reduzieren.

SonicWall Hosted Email Security bietet einen erstklassigen Cloud-basierten Schutz vor ein- und ausgehenden Bedrohungen wie Ransomware, Phishing, Business-E-Mail-Compromise (BEC), Spoofing, Spam und Viren – und das zu erschwinglichen, kalkulierbaren und flexiblen monatlichen oder jährlichen Abonnementkosten. Gleichzeitig werden der vorab fällige Kosten- und Zeitaufwand für die Implementierung sowie die laufenden Verwaltungskosten minimiert.

SonicWall Hosted Email Security mit dem Capture Advance Threat Protection-Service scannt dynamisch alle verdächtigen E-Mail-Anhänge und URLs, analysiert sie in einer Multi-Engine-Sandbox und blockiert gefährliche Dateien oder URLs, bevor sie in Ihr Netzwerk gelangen. Capture ATP arbeitet dabei mit unserer zum Patent angemeldeten Real-Time Deep Memory Inspection (RTDMI™)-Technologie. Die RTDMI-Engine erkennt und blockiert proaktiv Massenmalware, Zero-Day-Bedrohungen und unbekannte Malware, indem sie die Überprüfung direkt im Speicher vornimmt. SonicWall Hosted Email Security mit Capture ATP bietet einen erweiterten Schutz vor bösartigen Anhängen und URLs und wehrt so Ransomware und zielgerichtete Phishing-Angriffe ab.

Darüber hinaus bietet der Service auch erweiterte Funktionen zur Compliance-Prüfung, Verwaltung und (optional) E-Mail-Verschlüsselung. Diese gewährleisten einen sicheren Austausch sensibler Daten und verhindern, dass vertrauliche Informationen nach außen dringen bzw. interne Regeln, Standards oder gesetzliche Vorgaben verletzt werden. Die Regeln können auf Organisationsebene konfiguriert werden, um ausgehende E-Mail-Inhalte und -Anhänge auf sensible Daten zu überprüfen und E-Mails zu Genehmigungs- oder Verschlüsselungszwecken weiterzuleiten. Verschlüsselte E-Mails lassen sich nachverfolgen, sodass festgestellt werden kann, wann diese empfangen und geöffnet wurden. Der Empfänger erhält einfach eine Benachrichtigungs-E-Mail mit der Anweisung, sich in einem sicheren Portal anzumelden, um die E-Mail zu lesen oder sicher herunterzuladen. Der Service ist Cloud-basiert und erfordert keine zusätzliche Client-Software.

Vorteile:

- Schutz vor zielgerichteten Phishing-Angriffen und E-Mail-Betrug
- Abwehr von Ransomware und Zero-Day-Malware, bevor sie in Ihr Postfach gelangen
- Schutz für Office 365, G Suite und lokale E-Mail-Server
- Blockieren neuer Bedrohungen mit Echtzeitinformationen zu Bedrohungen
- Sichere Daten dank granularem Schutz vor Datenlecks (Data Loss Prevention, DLP) und Compliance-Regeln
- Echte Mandantenfähigkeit mit einer fein abgestimmten Kontrolle über Verwaltung, Provisioning, Reporting und Branding für jeden Mandanten
- Flexible Skalierbarkeit bei vorhersehbaren Abogebühren und ohne Vorabkosten
- Weniger Aufwand für Administratoren und Serviceprovider dank einfachem Management und Reporting
- Vorteile der Cloud und geringerer Bandbreitenverbrauch
- E-Mails werden immer zugestellt und die Produktivität wird weder durch planmäßige noch durch unvorhersehbare Ausfälle beeinträchtigt

Im Gegensatz zu den Lösungen anderer Anbieter können Benutzer von ihren Mobilgeräten oder Laptops aus auf verschlüsselte E-Mails zugreifen und diese lesen.

Darüber hinaus arbeitet der Service mit DMARC (Domain-based Message Authentication, Reporting and Conformance), einer leistungsstarken E-Mail-Authentifizierungstechnologie, um gespoofte E-Mails zu identifizieren und raffinierte Phishing-Angriffe wie Spear-Phishing, Whaling, CEO-Fraud und Business-E-Mail-Compromise einzudämmen. DMARC erstellt auch Berichte zu Quellen und Absendern von E-Mails. Auf diese Weise können Sie unautorisierte Absender, die E-Mails mit Ihrer Adresse fälschen, identifizieren und blockieren und somit Ihre Marke schützen.

SonicWall Hosted Email Security kombiniert mehrere Anti-Virus-Technologien, um bestmögliche E-Mail-Sicherheit zu gewährleisten. Mit SonicWall Capture Labs werden täglich Millionen E-Mails genau analysiert und evaluiert. Die laufend aktualisierten Analysedaten liefern hervorragende Spamschutz-Ergebnisse und ermöglichen so einen optimalen Schutz vor Viren und Spyware.

Ein weiterer Vorteil ist, dass mit SonicWall Hosted Email Security keine Geräte vor Ort installiert werden müssen. Somit entfallen die Vorabkosten für Hardware und Software. Gleichzeitig wird der Aufwand für die Implementierung und Verwaltung der E-Mail-Sicherheitslösung auf ein Minimum reduziert. Außerdem fallen mit einem gehosteten Service keine zusätzlichen laufenden Updates, Verwaltungsaufgaben oder Kosten für Hardware oder Software an. SonicWall kümmert sich um die kontinuierliche Aktualisierung des Services. So profitieren Sie nicht nur von einem extrem sicheren Serviceangebot – Sie haben zudem immer Zugriff auf die neuesten Features und Ihre IT-Mitarbeiter können sich auf andere Aufgaben konzentrieren. Mit SonicWall Hosted Email Security können Organisationen von einer erstklassigen E-Mail-Sicherheit profitieren und gleichzeitig den Verwaltungsaufwand reduzieren.

Für MSPs und VARs

SonicWall Hosted Email Security ist auch für MSPs und VARs erhältlich, die ihren Kunden ohne Vorabkosten und finanzielles Risiko eine differenzierte, hoch profitable Software-as-a-Service(SaaS)-basierte E-Mail-Sicherheitslösung mit einem überragenden Cloud-basierten Schutz vor ein- und ausgehenden Bedrohungen wie Spam, Phishing, BEC, Ransomware und Malware bieten möchten. Mit dieser gehosteten Lösung erweitert SonicWall sein ohnehin schon umfangreiches Angebot an E-Mail-Sicherheitsprodukten und bietet VARs und MSPs eine exzellente Chance, wettbewerbsfähig zu bleiben, ihre Umsätze zu steigern und gleichzeitig Risiken, Verwaltungsaufwand und laufende Kosten zu minimieren.

MSPs profitieren von echter Mandantenfähigkeit mit einer fein abgestimmten Kontrolle über Verwaltung, Provisioning, Reporting und Branding für jeden Mandanten. Sämtliche Mandanten lassen sich über eine zentralisierte Administrationsseite mit einer einzigen Ansicht verwalten. Die Lösung ermöglicht eine fein abgestimmte Verwaltung zur Automatisierung der Lizenzbereitstellung und Regeldurchsetzung. Zusätzlich steht ein umfangreicher Satz leistungsstarker RESTful-APIs zur Verfügung, mit denen MSPs die Lösung je nach Geschäftsanforderungen anpassen können.

SonicWall bietet darüber hinaus eine solide E-Mail-Kontinuität, um die Auswirkungen planmäßiger oder unvorhersehbarer Ausfälle lokaler E-Mail-Server oder Cloud-basierter Services wie Office 365 und G Suite auf das Geschäft zu minimieren. Durch E-Mail-Kontinuität können MSPs rund um die Uhr die Serviceverfügbarkeit sicherstellen und anspruchsvolle Service-Level-Agreements (SLAs) einhalten.

Funktionen

Advanced Threat Protection – Der SonicWall Email Security Capture Advanced Threat Protection Service ist in der Lage, hoch entwickelte Bedrohungen zu erkennen und bis zur Klärung des Sicherheitsstatus zu blockieren. Dieser Service ist die einzige Lösung zur Erkennung raffinierter Bedrohungen, die mehrstufiges Sandboxing, Real-Time Deep Memory Inspection, umfassende Systemsimulation und Virtualisierungstechniken vereint, um verdächtige Codeaktivitäten innerhalb von E-Mails zu analysieren und Kunden vor den wachsenden Gefahren von Zero-Day-Bedrohungen zu schützen. Der Capture ATP-Service bietet zudem eine feinere Granularität mit dynamischer Analyse von Anhängen und URLs, zusätzliche umfangreiche Reportingfunktionen und eine optimierte Benutzererfahrung.

Verbesserter Office-365-Support – Der SonicWall Hosted Email Security-Service lässt sich mit Office 365 und G Suite integrieren, um ein korrektes/gemapptes Matching von Nachrichten in einer gehosteten, mandantenfähigen Umgebung sicherzustellen. Darüber hinaus unterstützt Hosted Email Security die automatische Office 365- und G Suite-Freigabeliste für IP-Adressen.

Stoppen Sie raffinierte Phishing-Angriffe mit erweiterten Verfahren, darunter SonicWalls Anti-Phishing-Technologie, die Methoden wie maschinelles Lernen, heuristische Techniken sowie Reputations- und Inhaltsanalysen zur Abwehr raffinierter Phishing-Angriffe kombinieren. Die Lösung umfasst außerdem effiziente E-Mail-Authentifizierungsstandards wie SPF, DKIM und DMARC, um Spoofing-Angriffe, Business-E-Mail-Compromise (BEC) und E-Mail-Betrug zu stoppen.

Sorgen Sie für eine gute E-Mail-Hygiene – Die Technologie bietet darüber hinaus Schutz vor DHA-Angriffen (Directory Harvest Attack) und Denial-of-Service-Attacken (DoS) sowie Funktionen für die Absender-Überprüfung. Zu den erweiterten Methoden für die Analyse des E-Mail-Inhalts gehören auch Support-Vector-Machine(SVM)-Algorithmen, Adversarial-Bayesian-Filtering, Bildanalysen und die „Kauderwelsch"-Erkennung, um sowohl verborgene bekannte als auch neue Bedrohungen zu finden. SonicWall überprüft auch den ausgehenden E-Mail-Verkehr nach Zombies, unberechtigten Absendern und E-Mails mit bösartigen Viren und blockiert ihn, um die Reputation des Unternehmens zu schützen

Profitieren Sie von einem ultrapräzisen und topaktuellen Schutz vor neuartigen Spamangriffen und stellen Sie gleichzeitig sicher, dass unbedenkliche E-Mails zugestellt werden. Dabei können Sie sich auf das SonicWall Capture Threat Network verlassen, das Informationen aus Millionen von Datenquellen sammelt und Echtzeitdaten zu Bedrohungen bereitstellt. Das SonicWall Capture Labs-Research-Team analysiert diese Daten und führt eingehende Tests durch. Darauf basierend werden Reputation-Scores für Absender und Inhalt erstellt und neuartige Bedrohungen in Echtzeit erkannt.

**U.S.- Patente: 7,814,545; 7,343,624; 7,665,140; 7,653,698; 7,546,348*

Profitieren Sie von Multi-AV-Schutz. Malwaresignaturen von SonicWall Capture Labs und Anti-Virus-Technologien anderer Anbieter ermöglichen einen überragenden Schutz, den Lösungen, die auf nur eine Anti-Virus-Technologie setzen, nicht bieten können. Dabei werden prädiktive Technologien eingesetzt, um E-Mails, die vermutlich neue Viren enthalten, zu identifizieren und umgehend unter Quarantäne zu stellen. So wird das Netzwerk auch in der Zeit zwischen dem Ausbruch eines neuen Virus und der Verfügbarkeit eines Virensignatur-Updates geschützt.

Compliance-Policy-Management und Verschlüsselung für E-Mails. Stellen Sie die Einhaltung gesetzlicher Vorgaben sicher, indem Sie E-Mails, die gegen gesetzliche Vorgaben oder andere Richtlinien (z. B. HIPAA, SOX, GLBA und PCI-DSS) bzw. gegen interne Datenverlustrichtlinien verstoßen, identifizieren und überwachen und darüber Berichte erstellen. Mithilfe von Compliance-Policy-Management können Sie den Abgleich von Datensatz-IDs so konfigurieren, dass Sie ganz einfach nach vordefinierten Informationen suchen können, und das Scannen von E-Mail-Anhängen so einrichten, dass die Veröffentlichung unautorisierter Daten gestoppt wird. Außerdem können Sie auch aus vordefinierten Regeln wählen, um eine einfache Compliance sicherzustellen, einschließlich vordefinierter Wörterbücher, um den Schutz vertraulicher Informationen zu gewährleisten. Darüber hinaus können Sie Approval-Ordner einrichten, um E-Mails vor der Veröffentlichung zu prüfen und zu genehmigen, und regelbasiertes Routing von E-Mails zu Verschlüsselungszwecken ermöglichen, um den sicheren Austausch sensibler Daten zu gewährleisten.

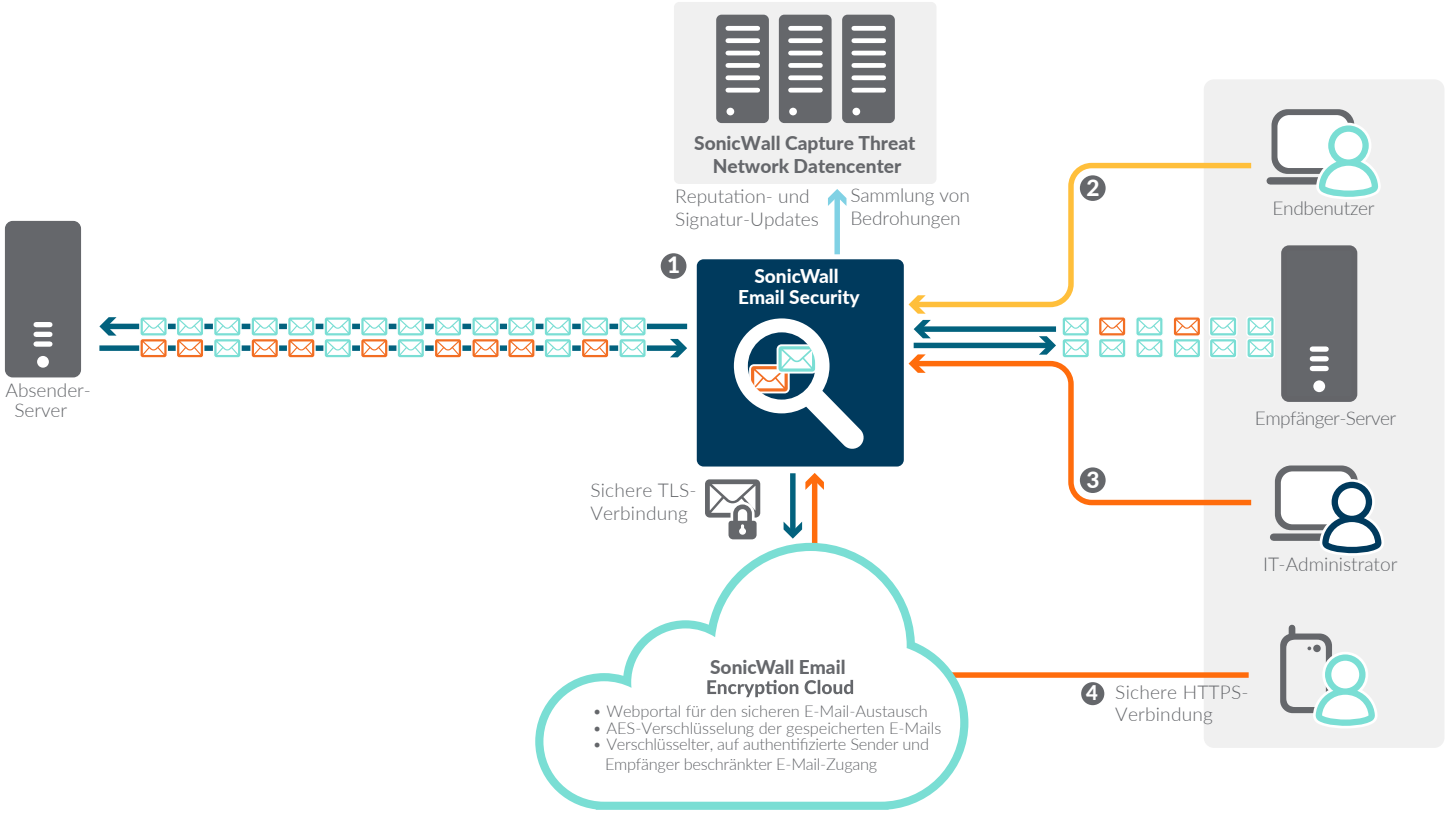
Profitieren Sie von unserer 24/7-Serviceverfügbarkeit mit E-Mail-Kontinuität. Stellen Sie sicher, dass E-Mails immer zugestellt werden und die Produktivität bei planmäßigen oder unvorhersehbaren Ausfällen lokaler E-Mail-Server bzw. bei Ausfällen eines Cloud-Providers wie Office 365 und G Suite nicht beeinträchtigt wird. Während eines Ausfalls können Benutzer auf einen sicheren, webbrowserbasierten Notfall-Posteingang zugreifen, um Nachrichten zu schreiben, zu lesen und zu beantworten. E-Mail-Spooling stellt sicher, dass keine Nachrichten verloren gehen, wenn E-Mail-Server nicht verfügbar sind. Betroffene Nachrichten werden zugestellt, sobald die Server wieder online sind.

Sparen Sie Netzwerkbandbreite, indem Sie Spam und Viren in der Cloud blockieren, bevor Sie unbedenkliche E-Mails an die E-Mail-Infrastruktur des Empfängers weiterleiten.

Vereinfachen Sie die Spamverwaltung für Endbenutzer, indem Sie die spamrelevanten Aufgaben einfach an die Endbenutzer delegieren. Die Anwender können die Granularität ihrer Spamerkennungseinstellungen personalisieren, während die IT-Abteilung die volle Kontrolle über die global verwendete Sicherheitsstufe behält.

Erhöhen Sie die Effizienz und Kosteneffektivität, indem Sie Ihre Vorabkosten für die Implementierung und Ihre laufenden Verwaltungskosten reduzieren. Mit SonicWall Hosted Email Security müssen Sie vor Ort keine Hardware oder Software installieren.

Vereinfachen Sie Prozesse für Managed-Service-Provider mit der Möglichkeit, mehrere Mandanten zu verwalten, flexiblen Kaufoptionen und automatisiertem Provisioning für mehrere Abonnenten.



1 Überprüfung und Schutz
- Mehrere bewährte, patentierte* Methoden
  - Anti-Spam
  - Anti-Phishing
  - Anti-Virus
- Mehrstufiger Virenschutz

2 Verwaltung durch den Endbenutzer
- Junkordner
- Freigabe-/Sperrliste
- Einstellungen für Junkbericht
- Notfall-Posteingang

3 Verwaltung durch den IT-Administrator
- Installation und Konfiguration
  - LDAP-Integration
  - Spooling-Verwaltung
  - Verwaltung der Bedrohungsschutzlösungen
- Verwaltung durch die Benutzer erlauben/verweigern
- Konfiguration und Überwachung des sicheren Austauschportals
- Berichte
- E-Mail-Kontinuität

4 Zugriff auf verschlüsselte E-Mails
- Zugriff auf verschlüsselte E-Mails von Mobil- und Desktopgeräten aus
- Lesen oder Herunterladen der verschlüsselten E-Mails
- Verschlüsselte Antwort senden

U.S.- Patente: 7,814,545; 7,343,624; 7,665,140; 7,653,698; 7,546,348

Berichte und Überwachung

Email Security lässt sich einfach installieren, verwalten und handhaben. Personalisierbare Drag-and-drop-Dashboards, Echtzeitberichte und Berichte im PDF-Format.

Junkordner-Berichte

Junkordner-Berichte optimieren die Produktivität von Endbenutzern bei der E-Mail-Kommunikation, sorgen für weniger Beschwerden und verbessern insgesamt die Effizienz.

Anti-Spoofing-DMARC-Bericht

Identifizierung der Quellen und Absender unerlaubter E-Mails.

**U.S.- Patente: 7,814,545; 7,343,624; 7,665,140; 7,653,698; 7,546,348*

Funktionen

UMFASSENDER E-MAIL-SCHUTZ FÜR EIN- UND AUSGEHENDEN VERKEHR	
Capture ATP (Erweiterter Schutz vor bösartigen Anhängen und URLs)	Optional
Anti-Spam-Effizienz	Ja
Absender-IP-Reputation	Ja
Schutz vor DHA- und DoS-Angriffen	Ja
Capture Labs-Reputationservices	Ja
SonicWall Cloud Anti-Virus	Ja
Multi-Anti-Virus	Ja
Erkennung bösartiger URLs	Ja
Erkennen, Klassifizieren und Blockieren von Phishing-Mails	Ja
Zombie-Erkennung, Flood-Schutz	Ja
Regeln und Richtlinien	Ja
LEICHTE ADMINISTRATION	
Verwaltung mehrerer Mandanten	Ja
Unterstützung für Office 365 und G Suite	Ja
Automatisiertes Provisioning und Set-up	Ja
Automatische Reputation-Updates	Ja
Automatische Anti-Spam-Updates	Ja
Automatische Upgrades und Wartung	Ja
Automatische Updates für Virensignaturen	Ja
Personalisierung, zeitliche Steuerung und E-Mail-Versand von Berichten	Ja
Automatische LDAP-Synchronisierung	Ja
Schnelle Nachrichten-Suchmaschine	Ja
EINFACHE HANDHABUNG FÜR ENDBENUTZER	
SMTP-Authentifizierung für ein-/ausgehenden Verkehr	Ja
Freigeben/Sperren aller Endbenutzer-Kontrollen	Ja
Notfall-Posteingang	Optional
Junkmail-Ordner pro Benutzer	Ja
Granularität für Spamschutz pro Benutzer	Ja
Freigabe-/Sperrlisten pro Benutzer	Ja
Junkmail-Berichte in 15 Sprachen	Ja
Judgement-Details	Ja
SYSTEMFUNKTIONEN	
Kompatibel mit allen SMTP-E-Mail-Servern	Ja
Unterstützung für SMTP-Authentifizierung (SMTP AUTH)	Ja
Unterstützung unbegrenzter Domänen	Ja
E-Mail-Kontinuität	Optional
Junkmails werden 15 Tage gespeichert	Ja
E-Mail-Spooling bis zu 7 Tage	Ja
COMPLIANCE-REGELN UND -VERWALTUNG	
Scannen der E-Mail-Anhänge	Ja
Abgleich von Datensatz-IDs	Ja
Wörterbücher	Ja
Approval-Ordner/Workflow	Ja
Compliance-Reporting	Ja

Funktionen (Fortsetzung)

EMAIL ENCRYPTION SERVICE FÜR HOSTED EMAIL SECURITY – OPTIONAL	
Regelbasierter, sicherer E-Mail-Austausch	Ja
Läuft nativ auf Mobilgeräten (keine App erforderlich)	Ja
Zusätzliche Outlook-Schaltfläche: „Send Secure“	Ja
Schnelle Verschlüsselung von Dateianhängen bis zu 100 MB	Ja
Direkter Versand von Nachrichten an Empfänger, ohne dass sie etwas installieren müssen	Ja
Benachrichtigung enthält Link zu automatisch bereitgestellten Empfängerkonten	Ja
Antworten werden im Posteingang des Absenders automatisch entschlüsselt	Ja
Integrierte Funktion zur Rückverfolgung aller Nachrichten und Dateien, die gesendet, empfangen und geöffnet werden	Ja
Rebranding von verschlüsselten Nachrichten	Ja
Berichte und Überwachung	Ja
500 MB pro Unternehmen	Ja
Verschlüsselung nach Industriestandards und Compliance-Vorgaben: AES 256, TLS	Ja
Keine Schlüssel, die man verwalten muss oder verlieren kann	Ja
Portal ist in zehn Sprachen lokalisiert: Englisch, Französisch, Italienisch, Deutsch, Spanisch, Japanisch, brasilianisches Portugiesisch, vereinfachtes Chinesisch und Mandarin sowie Koreanisch	Ja
Support für Outlook 2010/2013/2016	Ja
Nach SSAE 16, SAS 70 Typ II & Fedramp zertifiziertes Datencenter	Ja
SUPPORT UND SERVICES	
E-Mail- und Telefonsupport (24/7)	Ja
Mehrere Datencenter	Ja

Hosted Email Security-Aboservice (1 Jahr)	
Benutzeranzahl	Artikelnummer
10	01-SSC-5030
25	01-SSC-5033
50	01-SSC-5036
100	01-SSC-5039
250	01-SSC-5042
500	01-SSC-5045
750	01-SSC-5057
1.000	01-SSC-5048
2.000	01-SSC-5051

Email Encryption Service für Hosted Email Security (1 Jahr)	
Benutzeranzahl	Artikelnummer
10	01-SSC-5078
25	01-SSC-5081
50	01-SSC-5084
100	01-SSC-5087
250	01-SSC-5091
500	01-SSC-5094
750	01-SSC-5097
1.000	01-SSC-5104
2.000	01-SSC-5107

Capture ATP Service für Hosted Email Security (1 Jahr)	
Benutzeranzahl	Artikelnummer
10-User-Paket	01-SSC-1650
25-User-Paket	01-SSC-1653
50-User-Paket	01-SSC-1656
100-User-Paket	01-SSC-1659
250-User-Paket	01-SSC-1838
500-User-Paket	01-SSC-1511
750-User-Paket	01-SSC-1514
1.000-User-Paket	01-SSC-1517
2.000-User-Paket	01-SSC-1520
5.000-User-Paket	01-SSC-1523

Continuity für Hosted Email Security (1 Jahr)	
Benutzeranzahl	Artikelnummer
10	01-SSC-3068
25	01-SSC-3071
50	01-SSC-3074
100	01-SSC-3077
250	01-SSC-3080
500	01-SSC-3083
750	01-SSC-3086
1.000	01-SSC-3089
2.000	01-SSC-3092
5.000	01-SSC-3095

Lizenzen auch für mehrere Jahre erhältlich. Weitere Informationen erhalten Sie unter: www.sonicwall.com/de

Über uns

Seit über 25 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-HostedEmailSecurity-US-KJ-MKTG2937