SONICWALL

EMAIL SECURITY-APPLIANCES UND -SOFTWARE

Leistungsstarke, benutzerfreundliche Lösungen zum Schutz vor raffinierten E-Mail-Bedrohungen und Compliance-Verstößen

So wichtig E-Mails für die geschäftliche Kommunikation sind, so groß sind auch der Schaden und die Produktivitätsverluste, die sie verursachen können – etwa wenn E-Mail-basierte Bedrohungen wie Ransomware, Phishing, Business-E-Mail-Compromise (BEC), Spoofing, Spam und Viren Ihre Mailserver und Posteingänge überfluten. 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. Ob es sich bei Ihrer Organisation um eine kleine oder mittelständische Firma mit Wachstumspotenzial, ein großes Unternehmen mit verteilten Netzwerken oder einen Managed-Service-Provider (MSP) handelt – Sie brauchen eine kostengünstige Lösung für E-Mail-Sicherheit und -Verschlüsselung, die so skalierbar und flexibel ist, dass sie mit Ihrem Unternehmen mitwächst und sich dezentral – z. B. entsprechend Ihren Organisationseinheiten und Domänen – verwalten lässt.

Die SonicWall Email Security-Appliance- und -Software-Lösungen bieten maximalen Schutz vor Bedrohungen durch ein- und ausgehende E-Mails sowie Compliance-Verstößen. Unsere Lösung prüft den gesamten ein- und ausgehenden E-Mail-Verkehr inklusive Anhänge auf vertrauliche Daten und liefert einen überlegenen Echtzeitschutz vor Ransomware, raffinierten Phishing-Attacken, Spoofing, Viren, bösartigen URLs, Zombie-, Directory-Harvest(DHA)- und Denial-of-Service(DoS)-Attacken sowie vor anderen Angriffen. SonicWall verwendet dabei unterschiedliche patentierte Methoden zur Erkennung von Bedrohungen sowie ein weltweit einzigartiges Frühwarnsystem zur Identifizierung und Überwachung von Angriffen.

SonicWall Email Security ist jetzt mit dem Capture Advanced Threat Protection-Service integriert und ermöglicht so eine fein abgestimmte, transparente Prüfung des SMTP-basierten Datenverkehrs. Der Cloud-basierte Capture ATP-Service ist in der Lage, viele verschiedene Typen von E-Mail-Anhängen zu durchleuchten, sie in einer Multi-Engine-Sandbox zu analysieren und gefährliche Dateien oder E-Mails zu blockieren, bevor sie in Ihr Netzwerk gelangen. Email Security mit Capture ATP bietet Ihnen einen hocheffektiven und reaktiven Schutz vor Ransomware und Zero-Day-Angriffen.

Darüber hinaus umfasst die Lösung auch DKIM (Domain Keys Identified Mail), SPF (Sender Policy Framework) und DMARC (Domain-based Message Authentication, Reporting and Conformance), eine leistungsstarke Technologie für die E-Mail-Authentifizierung. Damit können Sie gespoofte E-Mails einfacher identifizieren, Spam- und raffinierte Phishing-Angriffe wie Spear-Phishing, Whaling, CEO-Fraud und Business-E-Mail-Compromise eindämmen und Berichte zu Quellen und Absendern von E-Mails erstellen. Auf diese Weise können Sie unautorisierte Absender, die E-Mails mit Ihrer Adresse fälschen, identifizieren und blockieren und somit Ihre Marke schützen. Darüber hinaus verhindert Email Security mit seinen erweiterten Funktionen zur Compliance-Prüfung und -Verwaltung sowie dem integrierten E-Mail-Verschlüsselungs-Cloud-Service für den sicheren Austausch sensibler Daten, dass vertrauliche Daten nach außen dringen bzw. interne Regeln, Standards oder gesetzliche Vorgaben verletzt werden.

Die Email Security-Lösung lässt sich intuitiv, schnell und einfach verwalten. Dabei können Sie die Spamverwaltung problemlos an die Endbenutzer delegieren und dabei trotzdem die volle Kontrolle über die Sicherheitsfunktionen behalten. Dank der nahtlosen Multi-LDAP-Synchronisierung ist es ein Kinderspiel, Benutzer- und Gruppenkonten zu administrieren. Bei großen verteilten Umgebungen können Sie dank Mandantenfähigkeit Subadministratoren einsetzen, um die Einstellungen in mehreren Organisationseinheiten (wie z. B. Unternehmensabteilungen oder MSP-Kunden) innerhalb einer einzigen Email Security-Implementierung zu verwalten.

Vorteile:

- Der Capture ATP-Service für E-Mail-Sicherheit bietet Schutz vor raffinierten Bedrohungen wie Ransomware und Zero-Day-Malware
- Erweiterte Analysetechniken, um Spam-, Phishing-, Spoofing-, Zombie- und Viren-Angriffe zu stoppen
- 24/7-Zugriff auf SonicWall Capture Labs, um neue Bedrohungen im Keim zu ersticken
- Add-on-Schutz vor Viren und Spyware für eine mehrschichtige Sicherheit
- Optionale Email Compliance and Encryption-Aboservices, um den sicheren mobilen bzw. konventionellen Austausch sowie die Verschlüsselung von E-Mails sicherzustellen
- Intelligente Automatisierung, Aufgabendelegierung, übersichtliches und personalisierbares Dashboard sowie robustes Reporting für eine einfache Verwaltung
- Flexible Implementierungsoptionen, um einen dauerhaften Wert zu gewährleisten

Funktionen

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 mehrschichtiges Sandboxing, 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. Außerdem ist Email Security Capture jetzt in der Lage, eine größere Anzahl an Dateitypen zu prüfen, und bietet zudem eine feinere Granularität, zusätzliche umfangreiche Reportingfunktionen und eine optimierte, reibungslose Benutzererfahrung.

Erweiterte Analysetechniken. Stoppen Sie Spam-, Phishing-, Spoofing-, Zombie- und Virenangriffe mithilfe mehrerer bewährter und patentierter[1] Methoden wie den Reputationsprüfungen. Hierbei werden nicht nur die IP-Reputation des Absenders, sondern auch Inhalt, Struktur, Verknüpfungen, Bilder und Anhänge überprüft. Email Security schützt vor DHA- und DoS-Angriffen und validiert den Absender. Zu den erweiterten Analysetechniken gehören ein Support-Vector-Machine(SVM)-Algorithmus, das Adversarial-Bayesian-Filtering, die Bildanalyse und die „Kauderwelsch"-Erkennung, um sowohl verborgene bekannte als auch neue Bedrohungen aufzudecken.

SonicWall Capture Threat Network. Erhalten Sie ultrapräzisen und topaktuellen Schutz vor neuartigen Spamangriffen und stellen Sie gleichzeitig sicher, dass unbedenkliche E-Mails korrekt zugestellt werden. Dabei können Sie sich auf das SonicWall Capture Threat Network verlassen, das Daten aus Millionen von Datenquellen sammelt und Echtzeitinformationen zu Bedrohungen bereitstellt. Das SonicWall-Threat-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.

Schutz vor Viren und Spyware. Holen Sie sich den aktuellen Anti-Virus- und Anti-Spyware-Schutz mit SonicWall Cloud Anti-Virus. Zusätzlich nutzt die Lösung Signaturen führender Antivirendatenbanken sowie Funktionen zur Erkennung bösartiger URLs. So profitieren Sie von einem mehrschichtigen Schutz, den andere Lösungen, die auf nur eine Antivirentechnologie setzen, nicht bieten können.

Darüber hinaus können Sie Ihr Netzwerk auch in der Zeit zwischen dem Ausbruch eines neuen Virus und der Verfügbarkeit einer Virensignatur schützen, indem Sie die prädiktive Technologie von SonicWall Time Zero Virus Protection verwenden.

Intelligente Automatisierung, Aufgabendelegierung und robustes Reporting. Vereinfachen Sie die Verwaltung dank intelligenter Automatisierung, Aufgabendelegierung und robustem Reporting. Verwalten Sie E-Mail-Adressen, Konten und Benutzergruppen automatisch. Nutzen Sie die nahtlose Integration mit mehreren LDAP-Servern. Mit dem herunterladbaren Outlook®-Plug-in Junk Button können Sie die Spam-Verwaltung ruhigen Gewissens an die Endbenutzer delegieren und behalten trotzdem die volle Kontrolle. Finden Sie jede beliebige E-Mail in Sekundenschnelle mit der Rapid Message Search Engine. Die zentrale Berichterstellung bietet Ihnen (selbst im Split Mode) flexibel anpassbare, systemweite und granulare Informationen zu Angriffstypen, zur Effizienz der Gegenmaßnahmen sowie zur integrierten Performance-Überwachung. Die Berichte sind im PDF- und JPEG-Format verfügbar.

Compliance-Policy-Management. Mit diesem Zusatzservice 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. Der Aboservice ermöglicht auch das regelbasierte Routing von E-Mails zu Genehmigungs-, Archivierungs- und Verschlüsselungszwecken.

E-Mail-Verschlüsselung. Ein leistungsstarkes Framework, um Datenlecks zu verhindern, Compliance-Anforderungen zu verwalten und umzusetzen und einen sicheren mobilen bzw. konventionellen Austausch von E-Mails in kleinen und großen Organisationen sicherzustellen.

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 Cloud-basierte Service erfordert keine zusätzliche Client-Software. Im Gegensatz zu den Lösungen anderer Anbieter können Benutzer von ihren mobilen Geräten oder Laptops aus auf die verschlüsselte E-Mail zugreifen und diese lesen.

Flexible Implementierungsoptionen. Sichern Sie sich eine skalierbare Lösung von dauerhaftem Wert. Konfigurieren Sie Ihre Lösung für Wachstum und Redundanz bei minimalen Investitionskosten. Sie können Email Security als gehärtete High-Performance-Appliance, als Software (Nutzung der vorhandenen Infrastruktur) oder als Virtual Appliance (gemeinsame Nutzung der IT-Ressourcen zur Optimierung der Auslastung, Vereinfachung der Migration und Senkung der Investitionskosten) implementieren. Beginnen Sie mit einem einzigen System und bauen Sie es einfach auf eine Split-Mode-Architektur mit Failover aus, wenn Ihr Unternehmen größer wird. Die Mandantenfähigkeit erlaubt es großen Unternehmen und MSPs mit mehreren Abteilungen bzw. Kunden, organisatorische Einheiten mit einer oder mehreren Domänen festzulegen. Die Implementierung kann zentral verwaltet werden, gestattet es einzelnen Organisationseinheiten aber dennoch, eigene Benutzer, Subadministratoren, Richtlinien, Junkordner usw. zu definieren.

SonicWall Email Security – Implementierungsoptionen

Dank seiner extrem flexiblen Architektur lässt sich SonicWall Email Security in Unternehmen implementieren, die eine hochskalierbare, redundante und verteile E-Mail-Sicherheitslösung mit zentraler Verwaltung benötigen. SonicWall Email Security kann entweder in einer All-in-one-Konfiguration oder im Split Mode eingesetzt werden.

Im Split Mode kann das System als Remote Analyzer oder als Kontrollzentrum konfiguriert werden. Bei einer typischen Split-Mode-Konfiguration ist mindestens ein Remote Analyzer an ein Kontrollzentrum angeschlossen. Der Remote Analyzer empfängt E-Mails von einer oder von mehreren Domänen und wendet Funktionen zur Verbindungsverwaltung, E-Mail-Filterung (Anti-Spam, Anti-Phishing und Anti-Virus) sowie erweiterte Regeln an, um unbedenkliche E-Mails an den nachgeschalteten E-Mail-Server zu leiten. Das Kontrollzentrum verwaltet alle Remote Analyzer zentral. Außerdem werden alle Junkmails von den Remote Analyzern gesammelt und gespeichert. Das zentrale Management umfasst die Erstellung von Berichten und die Überwachung aller angeschlossenen Systeme. Auf diese Weise lässt sich die Lösung kostengünstig skalieren, um in schnell wachsenden Organisationen sowohl den eingehenden als auch den ausgehenden E-Mail-Verkehr zu schützen. Die SonicWall Email Security Virtual Appliances erlauben eine vollständige Implementierung im Split Mode auf einem oder auf mehreren Servern und sorgen so für optimale Skaleneffekte.

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

Funktionen

	APPLIANCE, VIRTUAL APPLIANCE	WINDOWS SERVER®
Umfassender E-Mail-Schutz für ein- und ausgehenden Verkehr		
Anti-Spam-Effizienz	Ja	Ja
Verbindungsverwaltung mit erweiterter IP-Reputation	Ja	Ja
Erkennen, Klassifizieren und Blockieren von Phishingmails	Ja	Ja
Schutz vor DHA-, DoS- und NDR-Angriffen	Ja	Ja
Schutz vor Spoofing mit SPF-, DKIM- und DMARC-Unterstützung	Ja	Ja
Sicherheitsregeln für Benutzer, Gruppen oder für alle Benutzer	Ja	Ja
In-Memory-MTA für verbesserten Durchsatz	Ja	Ja
Umfassender Schutz vor ein- und ausgehenden E-Mail-Bedrohungen in einem System	Ja	Ja
Leichte Administration		
Installation	Weniger als 1 Stunde	Weniger als 1 Stunde
Verwaltungsaufwand pro Woche	Weniger als 10 Min.	Weniger als 10 Min.
Automatische Multi-LDAP-Synchronisation für Benutzer und Gruppen	Ja	Ja
Kompatibel mit allen SMTP-E-Mail-Servern	Ja	Ja
Unterstützung für SMTP-Authentifizierung (SMTP AUTH)	Ja	Ja
Freigeben/Sperren von Endbenutzer-Kontrollen	Ja	Ja
Personalisierung, zeitliche Steuerung und E-Mail-Versand von über 30 Berichten	Ja	Ja
Judgment-Details	Ja	Ja
Übersichtliches, personalisierbares Management-Dashboard	Ja	Ja
Schnelle Nachrichten-Suchmaschine	Ja	Ja
Skalierbare Split-Mode-Architektur	Ja	Ja
Clustering und Remote Clustering	Ja	Ja
Hohe Benutzerfreundlichkeit für Endbenutzer		
Single-Sign-on	Ja	Ja
Junkmail-Ordner pro Benutzer, Junkordner-Bericht mit Freigabemöglichkeit	Ja	Ja
Granularität für Spamschutz pro Benutzer, Freigabe-/Sperrlisten	Ja	Ja
Email Protection-Abo mit Dynamic Support erforderlich		
Automatische Updates im Minutentakt für SonicWall Cloud Anti-Virus, Anti-Spam und Anti-Phishing	Ja	Ja
24/7-Support	Ja	Ja
RMA (Appliance-Austausch)	Ja	Ja
Software- und Firmware-Updates	Ja	Ja
Anti-Virus-Abo – optional		
Signatur-Feeds von führenden Antivirendatenbanken	Ja	Ja
SonicWall TimeZero Anti-Virus	Ja	Ja
Zombie-Erkennung	Ja	Ja
Compliance-Abo – optional		
Zuverlässige Regelverwaltung	Ja	Ja
Scannen der E-Mail-Anhänge	Ja	Ja
Abgleich von Datensatz-IDs	Ja	Ja
Wörterbücher	Ja	Ja
Approval-Ordner/Workflow	Ja	Ja
E-Mail-Archivierung	Ja	Ja
Compliance-Reporting	Ja	Ja
Verschlüsselungs-Abo – optional		
Compliance-Abo, regelbasierte E-Mail-Verschlüsselung und sicherer E-Mail-Austausch	Ja	Ja
TotalSecure-Abo – optional		
Umfasst Email Protection-Abo mit Dynamic 24/7, mehrschichtigen Virenschutz, Erkennung bösartiger URLs und Compliance-Management	Ja	Ja
Schutz vor Ransomware und Zero-Day-Angriffen – optional		
SonicWall Capture ATP-Add-on für das TotalSecure-Paket	Ja	Ja
Erweitertes TotalSecure-Abo – optional		
Umfasst neben dem TotalSecure-Paket auch SonicWall Capture ATP	Ja	Ja

Systemdaten

EMAIL SECURITY-APPLIANCES	5000	7000	9000
Domänen	Unbegrenzt		
Betriebssystem	Gehärtete SonicWall Linux OS-Appliance		
Rackoptimiertes Gehäuse	1 HE	1 HE	1 HE
CPU(s)	Celeron G1820	i3-4330	E3-1275 v3
RAM	8 GB	16 GB	32 GB
Festplatte	500 GB	1 TB	1 TB
RAID (Redundant Disk Array)	–	RAID 1	RAID 5
Hot-swappable Laufwerke	Nein	Ja	Ja
Redundante Stromversorgung	Nein	Nein	Ja
SAFE-Mode-Flash	Ja	Ja	Ja
Abmessungen	43,18 x 41,59 x 4,44 cm	43,18 x 41,59 x 4,44 cm	69,9 x 48,3 x 8,9 cm
Gewicht	7,26 kg	7,26 kg	22,7 kg
WEEE-Gewicht	7,37 kg	22,2 kg	22,2 kg
Leistungsaufnahme (Watt)	46	48	158
BTUs	155	162	537
MTBF bei 25 °C in Stunden	130.919	150.278	90.592
MTBF bei 25 °C in Jahren	14,9	17,2	10,3
Email Security-Software			
Domänen	Unbegrenzt		
Betriebssystem	Microsoft Hyper-V Server 2012 (64 Bit) oder höher Windows Server 2008 R2 oder höher, nur x64 Bit		
CPU	Intel- oder AMD-64-Bit-Prozessor		
RAM	8 GB Minimalkonfiguration		
Festplatte	160 GB Minimalkonfiguration		
Email Security Virtual Appliance			
Hypervisor	ESXi™ und ESX™ (ab Version 5.0)		
Installiertes Betriebssystem	8 GB (erweiterbar)		
Zugewiesener Speicher	4 GB		
Festplattenkapazität der Appliance	160 GB (erweiterbar)		
VMware-Kompatibilitätsrichtlinien für Hardware:	http://www.vmware.com/resources/compatibility/search.php		

SonicWall Email Security – Bestellinformationen

SonicWall Email Security-Appliances

Artikelnummer	Produkt
01-SSC-7605	SonicWall Email Security-Appliance 9000
01-SSC-7604	SonicWall Email Security-Appliance 7000
01-SSC-7603	SonicWall Email Security-Appliance 5000
01-SSC-6636	SonicWall Email Security-Software
01-SSC-7636	SonicWall Email Security Virtual Appliance

SonicWall Email Security-Abos

Artikelnummer	Abo
SonicWall Email Protection-Abo	
01-SSC-6669	SonicWall Email Protection-Abo und 24/7-Support, 25 Nutzer, 1 Server (1 Jahr)
01-SSC-6678	SonicWall Email Protection-Abo und 24/7-Support, 1.000 Nutzer, 1 Server (1 Jahr)
01-SSC-6730	SonicWall Email Protection-Abo und 24/7-Support, 10.000 Nutzer, 1 Server (1 Jahr)
SonicWall Email Anti-Virus-Abo	
01-SSC-6759	SonicWall Email Anti-Virus, 25 Nutzer, 1 Server (1 Jahr)
01-SSC-6768	SonicWall Email Anti-Virus, 1.000 Nutzer, 1 Server (1 Jahr)
01-SSC-7562	SonicWall Email Anti-Virus, 10.000 Nutzer, 1 Server (1 Jahr)
SonicWall Email Encryption-Abo	
01-SSC-7427	SonicWall Email Encryption-Service, 25 Nutzer (1 Jahr)
01-SSC-7471	SonicWall Email Encryption-Service, 1.000 Nutzer (1 Jahr)
01-SSC-7568	SonicWall Email Encryption-Service, 10.000 Nutzer (1 Jahr)
SonicWall Email Compliance-Abo	
01-SSC-6639	SonicWall Email Compliance-Service, 25 Nutzer, 1 Server (1 Jahr)
01-SSC-6648	SonicWall Email Compliance-Service, 1.000 Nutzer, 1 Server (1 Jahr)
01-SSC-6735	SonicWall Email Compliance-Service, 10.000 Nutzer, 1 Server (1 Jahr)
SonicWall TotalSecure Email-Abo	
01-SSC-7399	SonicWall TotalSecure Email-Abo, 25 Nutzer (1 Jahr)
01-SSC-7398	SonicWall TotalSecure Email-Abo, 1.000 Nutzer (1 Jahr)
01-SSC-7405	SonicWall TotalSecure Email-Abo, 10.000 Nutzer (1 Jahr)
Capture ATP-Add-on für TotalSecure Email-Abo	
01-SSC-1526	Capture ATP für SonicWall TotalSecure Email-Abo, 25 Nutzer (1 Jahr)
01-SSC-1874	Capture ATP für SonicWall TotalSecure Email-Abo, 1.000 Nutzer (1 Jahr)
01-SSC-1883	Capture ATP für SonicWall TotalSecure Email-Abo, 10.000 Nutzer (1 Jahr)
SonicWall Advanced TotalSecure Email-Abo (einschließlich Capture ATP)	
01-SSC-1886	SonicWall Advanced TotalSecure Email-Abo, 25 Nutzer (1 Jahr)
01-SSC-1904	SonicWall Advanced TotalSecure Email-Abo, 1.000 Nutzer (1 Jahr)
01-SSC-1913	SonicWall Advanced TotalSecure Email-Abo, 10.000 Nutzer (1 Jahr)

SonicWall Email Security Appliance-Pakete und -Abos sind mit 1-, 2- oder 3-jähriger Laufzeit und in den folgenden User-Packs erhältlich: 25, 50, 100, 250, 500, 1.000, 2.000, 5.000 und 10.000. Support ist auch als 8/5-Option verfügbar. Für eine vollständige Liste der Artikelnummern wenden Sie sich bitte an Ihren lokalen SonicWall-Ansprechpartner.

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 globalen Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, Kalifornien 95054, USA
Weitere Information erhalten Sie auf unserer Website.
www.sonicwall.com

DataSheet-EmailSecurityAppsAndSoftware-US-VG-MKTG971

SONICWALL®