SONICWALL

E-Mail Security Appliances und Software

Schützen Sie Ihre Infrastruktur vor komplexen E-Mail-Bedrohungen und Compliance-Verstößen mit leistungsstarken, benutzerfreundlichen Lösungen

E-Mails sind extrem wichtig für Ihre Geschäftskommunikation, doch gleichzeitig sind sie der beliebteste Angriffsvektor für Bedrohungen wie Ransomware, Phishing, Business-E-Mail-Compromise (BEC), Spoofing, Spam und Viren. 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 (KMU) 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.

E-Mail Security Appliances und Software von SonicWall bieten mehrschichtigen Schutz vor eingehenden und ausgehenden E-Mail-Bedrohungen und Compliance-Verstößen, indem sie alle eingehenden und ausgehenden E-Mail-Inhalte, URLs und Anhänge auf sensible Daten durchsuchen und in Echtzeit vor Ransomware, gezielten Phishing-Angriffen, Spoofing, Viren, bösartigen URLs, Zombies, Directory Harvest Attacks (DHA), Denial of Service (DoS) und anderen Angriffen schützen. Bei dieser Lösung kommen mehrere patentierte SonicWall-Bedrohungserkennungstechniken und ein einzigartiges, weltweites Netzwerk zur Erkennung und Überwachung von Angriffen zum Einsatz.

Der SonicWall Capture Advanced Threat Protection Service nutzt branchenführendes Multi-Engine-Sandboxing mit der zum Patent angemeldeten RTDMI™ Technologie (Real-time Deep Memory Inspection) zum Aussondern unbekannter Bedrohungen, die in verdächtigen Dateianhängen und URLs gefunden werden. Somit können komplexe Bedrohungen gestoppt werden, bevor sie die Posteingänge der Benutzer erreichen. Mit der Kombination aus E-Mail Security und Capture ATP erhalten Sie eine hocheffektive und reaktionsschnelle Lösung zur Abwehr von Ransomware und Zero-Day-Angriffen.

Die Lösung umfasst außerdem Domain-basierte Message Authentication, DKIM (Domain Keys Identified Mail), SPF (Sender Policy Framework), Reporting and Conformance (DMARC), eine leistungsstarke E-Mail-Authentifizierungsmethode für die Identifizierung von gefälschten E-Mails, Reduzierung von Spam und gezielten Phishing-Angriffen, wie Speer-Phishing, Whaling, CEO-Betrug und Kompromittierung von geschäftlichen E-Mails. Auch Ursprung und Absender der E-Mails werden gemeldet, damit unberechtigte Absender, die E-Mails unter Verwendung Ihrer Adresse verfälschen, identifiziert und blockiert und Ihre Marke geschützt werden kann. Darüber hinaus bietet die Lösung eine erweiterte Compliance-Prüfung und Verwaltung sowie einen Cloud-Dienst für die integrierte E-Mail-Verschlüsselung, um einen sicheren Austausch sensibler Daten zu gewährleisten und Datenklau und regulatorische Verstöße zu verhindern.

Die Email Security-Lösung lässt sich intuitiv, schnell und einfach verwalten. Dabei können Sie die Spamverwaltung problemlos an Endbenutzer delegieren und trotzdem die volle Kontrolle über die Durchsetzung der Sicherheitsmaßnahmen behalten. Dank der nahtlosen Multi-LDAP-Synchronisierung ist die Verwaltung von Benutzer und Gruppenkonten ein Kinderspiel. Dank Mandantenfähigkeit können in großen verteilten Unternehmen auch Subadministratoren eingesetzt werden, um die Einstellungen in mehreren Organisationseinheiten (wie z. B. Unternehmensabteilungen oder MSP-Kunden) innerhalb einer E-Mail Security-Implementierung zu verwalten.

Vorteile

- Mit Capture Advanced Threat Protection wird verhindert, dass Ransomware und Zero-Day-Malware Ihren Posteingang erreichen
- Schutz der Benutzer vor schädlichen Links auf allen Geräten und Standorten mit Schutz vor URL-Analysen zum Klickzeitpunkt
- Erweiterte Analysetechniken, um gezielte Phishing-Angriffe, E-Mail-Betrug und Business E-Mail Compromise (BEC) zu stoppen
- Neue Bedrohungen werden mittels Echtzeit-Updates der Bedrohungsinformationen von SonicWall Capture Labs gestoppt
- Leistungsstarker Anti-Spam- und Antivirus-Schutz sorgt für gute E-Mail-Hygiene
- Sichere Daten dank granularem Schutz vor Datenlecks (Data Loss Prevention, DLP) und Compliance-Regeln
- Vereinfachte Verwaltung durch intelligente Automatisierung, Aufgabendelegierung, konfigurierbares übersichtliches Dashboard und robustes Reporting
- Flexible, skalierbare Implementierungsoptionen mit gehärteten physischen Appliances, robusten virtuellen Appliances und leistungsstarker Windows Server® Software

[1] *US-Patente 7.814.545; 7.343.624; 7.665.140; 7.653.698; 7.546.348*

Funktionen

Schutz vor komplexen Bedrohungen

Komplexe Bedrohungen werden erkannt und bis zur endgültigen Klärung blockiert. Dieser Dienst zur Erkennung raffinierter Bedrohungen ist die einzige Lösung, die mehrschichtiges Sandboxing, Real-Time Deep Memory Inspection, komplette Systememulation und Virtualisierungstechniken vereint, um verdächtige Codeaktivitäten innerhalb von E-Mails zu analysieren und Kunden vor den wachsenden Gefahren von Zero-Day-Bedrohungen zu schützen. Zu diesem Dienst gehört auch ein erweiterter URL-Schutz mit dynamischer Analyse eingebetteter URLs, durch den Nachrichten mit schädlichen URLs bereits im Vorfeld blockiert und unter Quarantäne gestellt werden, damit die Benutzer erst gar nicht darauf klicken und Schaden erleiden können. Der Capture ATP Dienst bietet zudem eine feiner granulierte Analyse von Dateianhängen und URLs, zusätzliche tiefgreifende Reportingfunktionen und eine optimierte Benutzererfahrung.

SonicWall E-Mail Security schreibt alle eingebetteten URLs neu und blockiert so E-Mails mit schädlichen oder Phishing-URLs, damit Benutzer zum Klickzeitpunkt auf allen Geräten und an allen Orten geschützt sind.

Einige Organisationen und Regierungsbehörden können Cloud-basierte Techniken zur Dateiinspektion, wie Capture ATP, aus Compliance- oder Latenzgründen nicht nutzen. Sie können Ihre E-Mail Security Appliance mit der SonicWall Capture Security Appliance (CSa) integrieren, um verdächtige Dateien zu untersuchen, die per E-Mail in Ihre eigenen Rechenzentren gelangen. Die CSa kann mit IP-Adresse oder FQDN referenziert werden, was sie zu einer ausgezeichneten Ressource für die Bedrohungsprävention macht.

Schutz vor gezielten Angriffen

SonicWalls Anti-Phishing-Lösung nutzt verschiedene Techniken wie Machine Learning, Heuristik sowie Reputations- und Inhaltsanalyse zur Abwehr raffinierter Phishing-Angriffe. 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.

Bedrohungsinformationen in Echtzeit

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.

Schutz vor Viren und Spyware

Nutzen Sie den neuesten Antivirus- und Anti-Spyware-Schutz. Diese Lösung nutzt Signaturen aus branchenführenden Antivirus-Datenbanken und Lösungen zur Erkennung bösartiger URLs. Das Resultat ist ein mehrschichtiger Schutz, der besser ist als Lösungen, die auf einer einzigen Antivirus-Technologie basieren.

Darüber hinaus wird das Netzwerk durch die vorausschauende Analyse vom Zeitpunkt des Virusausbruchs bis zur Verfügbarkeit eines Updates der Antivirus-Signatur geschützt.

Intelligente Automatisierung, Aufgabendelegierung und robustes Reporting

Mit intelligenter Automatisierung, Aufgabendelegierung und robustem Reporting kann die Verwaltung drastisch vereinfacht werden. E-Mail-Adressen, Konten und Benutzergruppen können automatisch verwaltet werden. Es ist eine nahtlose Integration mit mehreren LDAP-Servern möglich. Mit dem als Plugin herunterladbaren Junk-E-Mail-Button für Outlook® können Sie das Spam-Management an die Endbenutzer delegieren und trotzdem die volle Kontrolle behalten. Mit der Rapid Message-Suchmaschine lässt sich jede E-Mail in Sekundenschnelle auffinden. Zentralisiertes Reporting (auch im Split-Modus) bietet leicht anpassbare, systemweite und granulare Informationen über die Arten der Angriffe und die Wirksamkeit der Lösungen. Integrierte Leistungsüberwachung und Berichte sind im PDF- und JPEG-Format verfügbar.

Compliance Policy Management

Dieser Add-on-Service sorgt für die Einhaltung gesetzlicher Vorgaben und unterstützt Sie bei der Erkennung, Überwachung und Protokollierung von E-Mails, die gegen Compliance-Vorschriften und Richtlinien (z. B. HIPAA, SOX, GLBA und PCI-DSS) oder gegen interne Datenschutzrichtlinien verstoßen. Dieser per Abo erhältliche Dienst ermöglicht auch regelbasiertes Weiterleiten von E-Mails zur Genehmigung, Archivierung und Verschlüsselung.

E-Mail-Verschlüsselung

Mit diesem leistungsstarken Framework können Sie Datenlecks stoppen, Compliance-Anforderungen verwalten und durchsetzen und einen für Mobilgeräte sicheren E-Mail-Austausch für Organisationen jeder Größenordnung bereitstellen.

Verschlüsselte E-Mails lassen sich nachverfolgen, sodass festgestellt werden kann, wann diese empfangen und geöffnet wurden. Der Empfänger erhält per E-Mail eine Benachrichtigung mit der Anweisung, sich in einem sicheren Portal anzumelden, um die E-Mail zu lesen oder sicher herunterzuladen. Der Dienst ist Cloud-basiert und erfordert keine zusätzliche Client-Software. Im Gegensatz zu den Lösungen anderer Anbieter können Benutzer von ihren Mobilgeräten oder Laptops aus auf verschlüsselte E-Mails zugreifen und diese lesen.

Flexible Implementierungsoptionen

Profitieren Sie von einem skalierbaren, langfristigen Wert, indem Sie Ihre Lösung für Wachstum und Redundanz mit minimalen Vorlaufkosten konfigurieren. E-Mail Security kann als gehärtete High-Performance-Appliance, als eine die bestehende Infrastruktur nutzende Software oder als Virtual Appliance implementiert werden, wodurch eine gemeinsame Nutzung der IT-Ressourcen zur Optimierung der Auslastung, Vereinfachung der Migration und Senkung der Investitionskosten ermöglicht wird. Sie beginnen mit einem einzelnen System und fügen dann dem Wachstum Ihres Geschäfts entsprechend Kapazität hinzu, um schließlich auf eine Failover-fähige Split-Modus-Architektur umzusteigen. Mandantenfähigkeit ermöglicht Großunternehmen oder Managed-Service-Providers die Implementierung

mit zahlreichen Abteilungen oder Kunden, um Organisationseinheiten mit einer oder mehreren Domänen aufzubauen. Die Implementierung kann zentral verwaltet werden, erlaubt aber bestimmten Organisationseinheiten trotzdem die Einrichtung eigener Benutzer, Subadministratoren, Richtlinien und Regeln, Junk-E-Mail-Ordnern und mehr.

Implementierungsoptionen für SonicWall E-Mail Security

Die hochflexible Architektur von SonicWall E-Mail Security eignet sich optimal für Organisationen, die eine hochskalierbare, redundante und verteilte E-Mail-Schutzlösung benötigen, die zentral verwaltet werden kann. SonicWall E-Mail Security kann entweder im All-in-One-Modus oder im Split-Modus eingesetzt werden.

Im Split-Modus können Systeme als Remote Analyzer oder als Kontrollzentrum konfiguriert werden. In einer typischen Split-Modus-Konfiguration werden ein oder mehrere Remote Analyzer mit einem Kontrollzentrum verbunden. Der Remote Analyzer empfängt E-Mails von einer oder mehreren Domänen und wendet Verbindungsmanagement, E-Mail-Filterung (Anti-Spam, Anti-Phishing und Antivirus) und erweiterte Regeltechniken an, um gutartige E-Mails an den nachgeschalteten E-Mail-Server zu leiten. Das Kontrollzentrum verwaltet zentral alle Remote Analyzer und erfasst und speichert sämtliche Junk-E-Mails von den Remote Analyzer. Die zentrale Verwaltung umfasst auch das Reporting für und die Überwachung aller zugehörigen Systeme. Dieses Lösungskonzept ermöglicht es wachsenden Organisationen ihre ein- und ausgehenden E-Mails auf kostengünstige Weise zu skalieren und zu schützen. Mit SonicWall E-Mail Security Virtual Appliances kann der Split-Modus für optimale Skalenvorteile komplett auf einem oder auf mehreren Servern implementiert werden.

Funktionen

	APPLIANCE, VIRTUELLE APPLIANCE	WINDOWS SERVER®
Advanced Total Secure Abo – Advanced Protection Bündel		
Enthält SonicWall Capture ATP Advanced Attachment und URL-Schutz zusätzlich zum Total Secure Abo	Ja	Ja
URL-Schutz zum Klickzeitpunkt	Ja	Ja
Total Secure Abo – Basic Protection Bündel		
Enthält Abo für 24/7 dynamischen E-Mail-Schutz plus mehrschichtiger Antivirus-Schutz, Erkennung bösartiger URLs und Compliance-Management Abo-Features	Ja	Ja
Ransomware und Zero-Day-Schutz – optional		
SonicWall Capture ATP erweiterter Attachment und URL-Schutz zusätzlich zum Total Secure Abo	Ja	Ja
Umfassender E-Mail-Schutz für ein- und ausgehenden Verkehr		
Anti-Spam	Ja	Ja
Verbindungsmanagement mit erweiterter IP-Reputation	Ja	Ja
Erkennung, Klassifizierung und Blockierung von Phishing-Mails	Ja	Ja
Schutz vor DHA, DoS und NDR	Ja	Ja
Anti-Spoofing mit Unterstützung für SPF, DKIM und DMARC	Ja	Ja
Regeln und Richtlinien für Benutzer, Gruppen, alle	Ja	Ja
Im Arbeitsspeicher basierter Message Transfer Agent (MTA) für verbesserten Durchsatz	Ja	Ja
Leichte Administration		
Installation	< 1 Stunde	< 1 Stunde
Verwaltungszeit pro Woche	< 10 Minuten	< 10 Minuten
Automatische Multi-LDAP Synchronisation für Benutzer, Gruppen	Ja	Ja
Kompatibel mit allen SMTP-E-Mail-Servern	Ja	Ja
Unterstützung für SMTP-Authentifizierung (SMTP AUTH)	Ja	Ja
Erlauben/Ablehnen der Endbenutzerkontrolle	Ja	Ja
Personalisierung, zeitliche Steuerung und E-Mail-Versand von 30+ Berichten	Ja	Ja
Beurteilungs Details	Ja	Ja
Konfigurierbares übersichtliches Management-Dashboard	Ja	Ja
Schnelle Nachrichten-Suchmaschine	Ja	Ja
Skalierbare Split-Modus-Architektur	Ja	Ja
Clustering und Remote Clustering	Ja	Ja
Einfache Handhabung für Endbenutzer		
Single Sign-on	Ja	Ja
Junkmail-Ordner pro Benutzer, Junkmail-Ordner-Berichte mit umsetzbaren Informationen	Ja	Ja
Granularität für Spamschutz pro Benutzer, Sperren/Erlauben-Listen	Ja	Ja
E-Mail-Schutz Abo mit dynamischer Unterstützung – erforderlich		
SonicWall Cloud Antivirus, Anti-Spam, Anti-Phishing Auto-Updates jede Minute	Ja	Ja
24/7 Support	Ja	Ja
RMA (Appliance-Austausch)	Ja	Ja
Software/Firmware Updates	Ja	Ja
Antvirus Abo – optional		
Signature Feeds aus branchenführenden Antivirus-Datenbanken	Ja	Ja
SonicWall TimeZero Antivirus	Ja	Ja
Zombie-Erkennung	Ja	Ja
Compliance Abo – optional		
Robustes Management für Richtlinien und Regeln	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
Verschlüsselungsabo – optional		
Compliance Abo Features inkl. durch Regeln durchgesetzte E-Mail-Verschlüsselung und sicherer E-Mail Austausch	Ja	Ja

Technische Daten zum System

E-MAIL SECURITY APPLIANCES	5000	7000	9000
Domänen		Uneingeschränkt	
Betriebssystem		Gehärtete SonicWALL Linux OS Appliance	
Rackmount-Chassis	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-System (Redundant Array of Independent Disks)	—	RAID 1	RAID 5
Hot-Swap-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
BTU	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
E-MAIL SECURITY SOFTWARE			
Domänen		Uneingeschränkt	
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 Mindestkonfiguration	
Festplatte		160 GB Mindestkonfiguration	
E-MAIL SECURITY VIRTUELLE APPLIANCE			
Hypervisor		ESXi™ und ESX™ (ab Version 5.0)	
Installiertes Betriebssystem		8 GB (erweiterbar)	
Zugewiesener Speicher		4 GB	
Für Appliance benötigter Festplattenspeicher		160 GB (erweiterbar)	
Kompatibilitätsleitfaden für VMware Hardware		http://www.vmware.com/resources/compatibility/search.php	

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.

Bestellinformationen für SonicWall E-Mail Security

SonicWall E-Mail Security-Appliances

Produkt	Artikelnummer
Sonicwall E-Mail Security Appliance 9000	01-SSC-7605
Sonicwall E-Mail Security Appliance 7000	01-SSC-7604
Sonicwall E-Mail Security Appliance 5000	01-SSC-7603
SonicWall E-Mail Security Software	01-SSC-6636
SonicWall E-Mail Security Virtuelle Appliance	01-SSC-7636

SonicWall E-Mail Security Abo

Aboservice	Artikelnummer
SonicWall E-Mail-Schutz Abo	
SonicWall E-Mail-Schutz Abo und 24/7 Support für 25 Benutzer – 1 Server (1 Jahr)	01-SSC-6669
SonicWall E-Mail-Schutz Abo und 24/7 Support für 1.000 Benutzer – 1 Server (1 Jahr)	01-SSC-6678
SonicWall E-Mail-Schutz Abo und 24/7 Support für 10.000 Benutzer – 1 Server (1 Jahr)	01-SSC-6730
SonicWall E-Mail-Antivirus Abo	
SonicWall E-Mail-Antivirus 25 Benutzer – 1 Server (1 Jahr)	01-SSC-6759
SonicWall E-Mail-Antivirus 1.000 Benutzer – 1 Server (1 Jahr)	01-SSC-6768
SonicWall E-Mail-Antivirus 10.000 Benutzer – 1 Server (1 Jahr)	01-SSC-7562
SonicWall E-Mail-Verschlüsselung Abo	
SonicWall E-Mail-Verschlüsselungsdienst 25 Benutzer (1 Jahr)	01-SSC-7427
SonicWall E-Mail-Verschlüsselungsdienst 1.000 Benutzer (1 Jahr)	01-SSC-7471
SonicWall E-Mail-Verschlüsselungsdienst 10.000 Benutzer (1 Jahr)	01-SSC-7568
SonicWall E-Mail Compliance Abo	
SonicWall E-Mail-Compliance-Dienst 25 Benutzer – 1 Server (1 Jahr)	01-SSC-6639
SonicWall E-Mail-Compliance-Dienst 1.000 Benutzer – 1 Server (1 Jahr)	01-SSC-6648
SonicWall E-Mail-Compliance-Dienst 10.000 Benutzer – 1 Server (1 Jahr)	01-SSC-6735
SonicWall TotalSecure E-Mail Abo	
SonicWall TotalSecure E-Mail Abo 25 Benutzer (1 Jahr)	01-SSC-7399
SonicWall TotalSecure E-Mail Abo 1.000 Benutzer (1 Jahr)	01-SSC-7398
SonicWall TotalSecure E-Mail Abo 10.000 Benutzer (1 Jahr)	01-SSC-7405
Capture ATP Add-on für TotalSecure E-Mail Abo	
Capture ATP für SonicWall TotalSecure E-Mail Abo 25 Benutzer (1 Jahr)	01-SSC-1526
Capture ATP für SonicWall TotalSecure E-Mail Abo 1.000 Benutzer (1 Jahr)	01-SSC-1874
Capture ATP für SonicWall TotalSecure E-Mail Abo 10.000 Benutzer (1 Jahr)	01-SSC-1883
SonicWall Advanced TotalSecure E-Mail Abo (Capture ATP inklusive)	
SonicWall Advanced TotalSecure E-Mail Abo 25 Benutzer (1 Jahr)	01-SSC-1886
SonicWall Advanced TotalSecure E-Mail Abo 1.000 Benutzer (1 Jahr)	01-SSC-1904
SonicWall Advanced TotalSecure E-Mail Abo 10.000 Benutzer (1 Jahr)	01-SSC-1913

*SonicWall E-Mail Security Appliance Bündel und Abos sind für 25, 50, 100, 250, 500, 1.000, 2.000, 5.000 und 10.000 Benutzer für 1, 2 und 3 Jahre erhältlich. 8/5 Support ist optional verfügbar. *Für eine vollständige Liste der Artikelnummern wenden Sie sich bitte an Ihren lokalen SonicWall-Ansprechpartner*

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
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

DataSheet-EmailSecurityAppsAndSoftware-US-COG-2150