Secure Mobile Access Appliance

Remote-Arbeit und BYOD-Initiativen unterstützen bei gleichzeitigem Schutz von Unternehmensdaten

Die Mobilitäts- und BYOD-Trends stellen IT-Organisationen vor neue Herausforderungen in puncto Sicherheit, Compliance und Zugriff. Sicherheitsverletzungen können aus ganz verschiedenen Situationen resultieren, z. B. wenn nicht autorisierte Personen auf verloren gegangene oder gestohlene Geräte zugreifen, nicht verwaltete Mobilgeräte genutzt werden, um das Netzwerk über diese mit Malware zu infizieren, Unternehmensdaten über nicht gesicherte Wireless-Netzwerke oder mobile Services von Dritten übermittelt und dann abgefangen werden oder nicht autorisierte Anwendungen auf die auf einem Gerät gespeicherten Daten zugreifen.

Um diesen Problemen zu begegnen und Unternehmensdaten auf mobilen und Remote-Geräten abzusichern, ziehen viele Organisationen die Bereitstellung von Lösungen für gehostete virtuelle Desktops (HVD), die Verwaltung von mobilen Geräten in Unternehmen (Enterprise Mobility Management, EMM) oder anderen Datenverschlüsselungslösungen in Betracht. Einige haben solche Lösungen auch bereits implementiert – und das ist schon ein guter Anfang. Wenn aber nur die Daten, die sich auf den Geräten befinden, geschützt werden, sind andere Unternehmensdaten und die Netzwerke dennoch Risiken ausgesetzt. Bei mobilen Workflows muss durchgängige Sicherheit gewährleistet werden.

Durchgängiger Schutz von Daten und Sicherheit
Mit dem Dell Secure Mobile Access (SMA) Gateway können Administratoren unkompliziert sicheren mobilen Zugriff provisionieren und rollenbasierte Berechtigungen für verwaltete und nicht verwaltete Geräte vergeben. Sie können mobilen Mitarbeitern für jede einzelne App richtliniengesteuerten VPN-Zugriff auf alle freigegebenen Unternehmensdaten und -ressourcen geben, die sie benötigen, und gleichzeitig das Unternehmensnetzwerk vor mobilen Sicherheitsbedrohungen schützen.

Das SMA Gateway lässt sich mit den Lösungen aller führenden EMM-Anbieter integrieren, einschließlich Dell Enterprise Mobility Management. So erhalten Sie die sicherste durchgängige Verwaltung- und Sicherheitslösung für BYOD-, CYOD- und verwaltete mobile Geräte. Mit der EMM-Technologie können Richtlinien zum Schutz von Daten auf Geräten erstellt sowie Anwendungen verwaltet werden und SMA ermöglicht die Erzwingung von Zugriffssteuerungsrichtlinien. Aus dieser Kombination resultiert eine umfassende, durchgängige Lösung für den Schutz und die Sicherheit von Daten, mit der Sie sicherstellen können, dass nur vertrauenswürdigen Benutzern und Geräten sowie autorisierten mobilen Anwendungen VPN-Zugriff gewährt wird – und das auch nur auf erlaubte Unternehmensnetzwerke und -ressourcen.

Darüber hinaus kann der Administrator den Zugriff auf das Unternehmens-VPN auf bestimmte vertrauenswürdige Mobil-Apps beschränken, während der Zugriff auf VPN-Ressourcen für nicht autorisierte Apps blockiert wird. Alle Mobil-Apps oder sicheren Container können ohne Modifikation, App-Wrapping oder SDK-Entwicklung unterstützt werden. Darüber hinaus macht es unsere Lösung leichter, auf Benutzerseite die Einhaltung Ihrer Richtlinien für die Geräteautorisierung zu erzwingen und nachzuverfolgen und so rechtliche Risiken zu reduzieren.

Sicherer Zugriff für mobile Geräte
Für Benutzer, die mit Mobilgeräten arbeiten, beinhaltet die Lösung die intuitive Dell Mobile Connect App. In Kombination mit dem SMA Gateway ermöglicht diese App OS, Mac OS X, Android, Kindle Fire oder Windows 8.1 Geräten einen einfachen, auf App-Ebene gesteuerten VPN-Zugriff auf erlaubte Ressourcen wie freigegebene

Vorteile:

- Förderung der Produktivität mobiler Mitarbeiter mit einer sicheren SSL-VPN-Verbindung und granularem, richtliniengesteuertem Zugriff auf Ressourcen
- Beschränkung des VPN-Zugriffs auf autorisierte, vertrauenswürdige mobile Apps und gleichzeitige Reduzierung der Geschäftsrisiken, da die IT BYOD-Autorisierungsrichtlinien verwalten und erzwingen kann
- Mobile Connect App, die iOS, Mac OS X, Android, Kindle Fire oder Windows 8.1 Geräten einen einfachen, auf App-Ebene gesteuerten VPN-Zugriff auf erlaubte Ressourcen ermöglicht
- Kontextsensitive Authentifizierung, um sicherzustellen, dass ausschließlich autorisierten Benutzern und vertrauenswürdigen mobilen Anwendungen und Geräten der VPN-Zugriff gewährt wird
- Effiziente objektbasierte Richtlinienverwaltung für alle Benutzer, Gruppen, Ressourcen und Geräte

Ordner, Client/Server-Anwendungen, Intranetseiten, E-Mail-Programme und virtuelle Desktop-Anwendungen wie Citrix, VMware View, RDP (Remote Desktop Protocol) und Dell vWorkspace.

Dell SMA WorkPlace Portal

Das SMA WorkPlace Portal bietet sicheren Browserzugriff ohne Client für Webanwendungen, Client/Server-Anwendungen sowie Dateifreigaben über iOS, Android, Windows, Apple Mac oder Linux Endpunkte. Das Portal unterstützt den Zugriff auf Ressourcen über Standard-HTML5-Browser (für die meisten Smartphones, Tablet-PCs und Notebooks verfügbar), einschließlich des Zugriffs auf via RDP veröffentlichte Anwendungen und Desktops, Citrix XenDesktop und XenApps (Unterstützung für ICA). Benutzer mit HTML5-Browsern können nun ohne die bei Legacy-Webbrowsern erforderlichen Java oder ActiveX Browser-Plug-ins auf sichere Weise auf diese Ressourcen zugreifen und profitieren nicht nur von weniger Komplexität, sondern auch einem geringeren Bedrohungsrisiko. Auch Benutzer mit Geräten, die Java oder ActiveX Webbrowser-Plug-ins üblicherweise nicht unterstützen, wie z. B. iOS Geräte, können mit einem Standard-HTML5-Browser auf erlaubte Ressourcen zugreifen.

Mehrstufiger Bedrohungsschutz

Bei Integration mit einer Dell SonicWALL Firewall der nächsten Generation im Rahmen eines Clean VPN entschlüsselt und dekontaminiert die SMA Lösung jeglichen autorisierten SSL-VPN-Datenverkehr, bevor er in die Netzwerkumgebung gelangt. Zudem ermöglicht die kombinierte Lösung die Zentralisierung von Zugriffssteuerung, Malwareschutz, Webanwendungskontrolle und Inhaltsfilterung.

Funktionen und Merkmale

Sicherer, richtliniengesteuerter Zugriff auf Netzwerkressourcen

Die IT kann ganz einfach einen richtliniengesteuerten SSL-VPN-Zugriff und rollenbasierte Berechtigungen für mobile Benutzer mit verwalteten und nicht verwalteten Geräten bereitstellen. Mit der Mobile Connect App können mobile Mitarbeiter eine verschlüsselte SSL-VPN-Verbindung zu einer SMA Gateway-Appliance herstellen und schnell auf die erlaubten Unternehmensdaten sowie Anwendungen und Ressourcen zugreifen, die sie benötigen – einschließlich webbasierten, hostbasierten, Client/Server-, VDI- und Back-Connect-Anwendungen wie VoIP (Voice over IP). Die Lösung schützt das Unternehmensnetzwerk vor mobilen Sicherheitsbedrohungen wie nicht autorisierten Datenzugriffen und Malwareangriffen.

Auf App-Ebene gesteuerter VPN-Zugriff

Administratoren können Richtlinien erstellen und erzwingen, mithilfe derer festgelegt wird, welche Mobil-Apps auf einem mobilen Gerät per VPN-Zugriff Zugang zum Netzwerk erhalten. Dadurch ist sichergestellt, dass nur autorisierten mobilen Geschäftsanwendungen der VPN-Zugriff gewährt wird. Außerdem erfordert das SMA Gateway keinerlei Veränderungen an mobilen Anwendungen. Alle Mobil-Apps oder sicheren Container können ohne Modifikation, App-Wrapping oder SDK-Entwicklung unterstützt werden.

BYOD-Geräteregistrierung und -Sicherheitsrichtlinienverwaltung

Wenn ein Benutzer versucht, über ein nicht bei der SMA Appliance registriertes Gerät auf Ressourcen zuzugreifen, werden ihm die Autorisierungsrichtlinien für persönliche Geräte angezeigt. Administratoren können die Bedingungen der Sicherheitsrichtlinien individuell anpassen. Der Benutzer muss den in den Richtlinien vermerkten Bedingungen zustimmen, um sein Gerät registrieren und auf erlaubte Unternehmensressourcen und -daten zugreifen zu können. Da Benutzer die Richtlinien akzeptieren müssen, können die mit der Implementierung einer BYOD-Richtlinie verbundenen Geschäftsrisiken reduziert werden.

Einfacher Zugriff auf autorisierte Ressourcen

Mit der intuitiven Mobile Connect App können iOS, MacOS X, Android, Kindle Fire und Windows 8.1 Mobilgeräte über verschlüsselte SSL-VPN-Verbindungen auf erlaubte Netzwerkressourcen zugreifen. Sobald der Benutzer und das verwendete Gerät verifiziert sind, stellt Mobile Connect vorkonfigurierte Lesezeichen bereit, die mit einem Klick den Zugriff auf autorisierte Unternehmensanwendungen und -ressourcen ermöglichen.

Kontextsensitive Authentifizierung

Der Zugriff wird erst dann gewährt, wenn der Benutzer authentifiziert und die Integrität der Mobilgeräts (einschließlich Jailbreak- und Root-Status, Geräte-ID, Zertifikatstatus und Betriebssystemversion) verifiziert wurde.

Technologie zur Aufrechterhaltung von Sitzungen

Die SMA Gateway-Appliance ermöglicht einen sicheren, stabilen und zuverlässigen Zugriff auf Ressourcen über Notebooks, Smartphones und Tablet-PCs. Außerdem bietet sie Technologie, mit der Sitzungen über verschiedene Orte hinweg (z. B. im Büro, zu Hause oder unterwegs) aufrechterhalten werden, ohne dass eine erneute Authentifizierung erforderlich ist.

Dell SMA Installationsassistent

Dank eines intuitiven Installationsassistenten können die Dell SMA Appliances problemlos eingerichtet und innerhalb nur weniger Minuten bereitgestellt werden.

Unified Policy

Die SMA Gateway-Appliance ermöglicht die einfache, objektbasierte Richtlinienverwaltung für alle Benutzer, Gruppen, Ressourcen und Geräte. Mittels Benutzerauthentifizierung und Endpunktabfrage ist zudem granulare Kontrolle sichergestellt. Dank Policy Zones ist es möglich, nicht autorisierte Zugriffsversuche zu verweigern oder unter Quarantäne zu stellen, bis bestimmte Sicherheitslücken behoben wurden.

Ermittlung des Sicherheitsstatus von Endpunkten

Zuverlässige Abfragen für strenge Endpunktkontrolle

Mit Dell SMA End Point Control (EPC) können granulare Zugriffssteuerungsregeln für Windows, Apple Mac OS X und iOS sowie Android, Kindle Fire und Linux Endpunkte erzwungen werden. Dank EPC können mithilfe von Abfragen bereits vor der Authentifizierung bestimmte Kriterien auf den Endpunkten überprüft werden, z. B. ob der Virenschutz auf dem neuesten Stand ist.

- **Policy Zones:** Sie haben die Möglichkeit, Endpunktkriterien in die automatische Richtlinienerzwingung zu integrieren. So können beispielsweise Zugriffsversuche unter Quarantäne gestellt und umgeleitet werden, sodass dem Benutzer Anweisungen zur Behebung einer Sicherheitslücke angezeigt werden und ihm der Zugriff erst dann gewährt wird, wenn das entsprechende Sicherheitspatch installiert wurde.
- **Device Watermarks:** Dank der Erkennung von Client-Zertifikaten können Zugriffsrechte für verloren gegangene oder gestohlene Geräte ganz einfach entzogen werden.
- **Device Identification:** Administratoren können die Seriennummer oder System-ID eines bestimmten Geräts mit einem bestimmten Benutzer oder einer bestimmten Gruppe verknüpfen.

- **Virtual Keyboard:** Dank Virtual Keyboard ist der Schutz vor Keyloggern auf nicht vertrauenswürdigen Endpunkten sichergestellt.

Recurring EPC: Um die fortlaufendes Integrität von Endpunkten zu verifizieren, werden bei der Benutzeranmeldung und in vom Administrator festgelegten Abständen Endpunkt-Scans durchgeführt. Außerdem bietet die SMA weitere Funktionen zur Endpunktkontrolle, mit denen ermittelt werden kann, ob auf einem iOS Gerät ein Jailbreak durchgeführt oder ein Android System gerootet wurde.

Erweiterte Endpunktkontrolle für optimalen Schutz

Mit der Dell SMA Advanced EPC Option profitieren Sie neben granularer Erkennung von Endpunkten und Kontrolle auch von erstklassigen Schutzfunktionen für Ihre Daten.

- Ein erweitertes Abfragesystem vereinfacht die Erstellung von Geräteprofilen anhand einer umfassenden, vordefinierten Liste an Virenschutz-, Spywareschutz- und persönlichen Firewall-Lösungen für Windows, Mac und Linux Plattformen. Dabei kann sogar abgeprüft werden, welche Version installiert ist und ob die Signaturdateien aktuell sind.
- Cache Control sorgt dafür, dass der Browser-Cache geleert und Sitzungsverläufe, Cookies und Kennwörter gelöscht werden.
- Dell SMA Gateways blockieren auch verdächtige E-Mail-Anhänge, wenn Outlook Web Access oder Lotus iNotes verwendet wird. Ebenso sperren sie den Zugriff auf Finanzdaten und Patientenakten.
- Für maximalen Schutz sind die Verbindungen mit SMA Appliances nur dann möglich, wenn eine Richtlinie es erlaubt – wie bei der Deny-All-Strategie einer Firewall.

Unkomplizierter Schutz von Unternehmensressourcen

Einrichtung und Richtlinienverwaltung

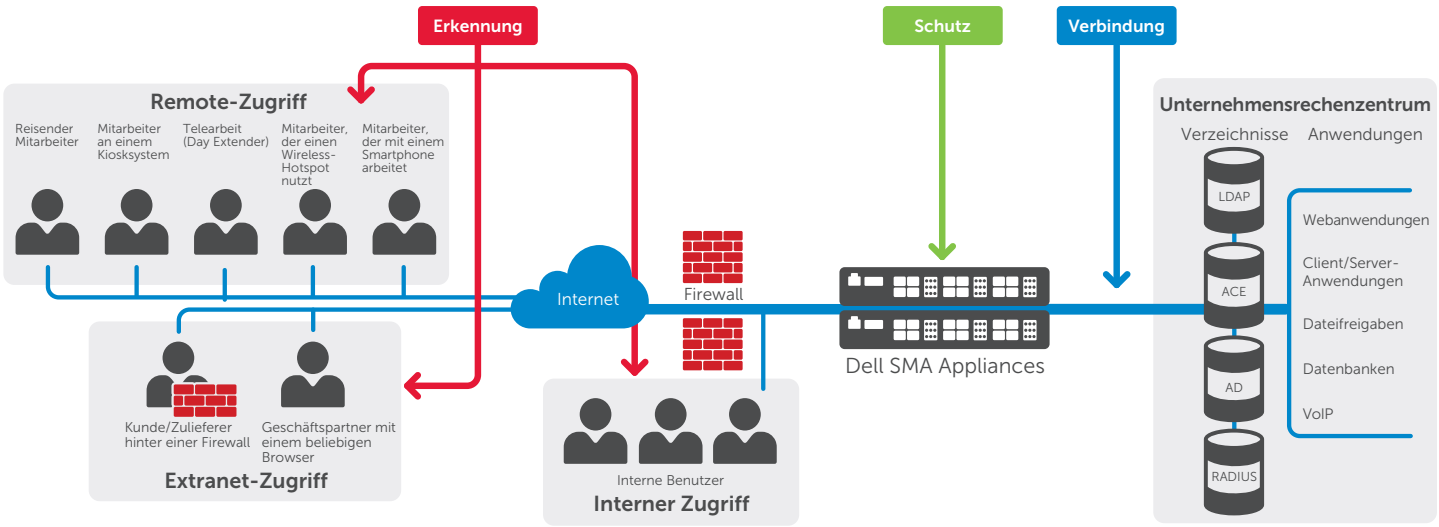
Dank ihrer kontextsensitiven Hilfe und eines Installationsassistenten können die SMA Lösungen mühelos bereitgestellt werden. Mit Unified Policy kann der Zeitaufwand für die Richtlinienverwaltung auf Minuten reduziert werden, da die Steuerung aller Webressourcen, Dateifreigaben und Client/Server-Ressourcen an einem einzigen Ort konsolidiert wird. Gruppen können basierend auf RADIUS, LDAP oder Active Directory Authentifizierungsrepositorys eingerichtet werden. Das gilt auch für geschachtelte Gruppen. Dank Policy Replication ist die IT in der Lage, Richtlinien ganz einfach über mehrere Appliance-Knoten hinweg zu replizieren – ganz gleich, ob im selben Cluster oder geographisch verteilt.

Einmalige Anmeldung und Zwei-Faktor-Authentifizierung

Die SMA Appliances unterstützen die einmalige Anmeldung (Single Sign-On) sowie formularbasierte Webanwendungen. Benutzer können darüber hinaus ganz einfach und ohne IT-Unterstützung ihre Kennwörter aktualisieren. Dank der unterstützten Authentifizierung mit Einmalkennwort (OTP, One-Time Password) verfügt die Lösung über eine integrierte Methode, sekundäre Faktoren zu generieren und zuzuweisen, um einfache und kostengünstige zweistufige Authentifizierung zu ermöglichen. Administratoren können OTPs nach Bereichen zuordnen, um mehr Flexibilität bei der Authentifizierungskontrolle zu gewährleisten.

Intuitive Verwaltung und Reporting

Die Dell SMA Verwaltungskonsole bietet ein Dashboard, über das Sie für die Verwaltung erforderliche Informationen auf einen Blick erhalten, sowie eine breite und zentralisierte Platte an Überwachungsfunktionen, die zu Prüfungs- und Verwaltungszwecken, zur Sicherstellung der Compliance sowie für die Ressourcenplanung genutzt werden können. Mit der SMA Advanced Reporting Option haben Sie die Möglichkeit, anhand von Standard- oder benutzerdefinierten Berichten, die in jedem Webbrowser angezeigt werden können, zu überprüfen, wer auf welche Unternehmensressourcen zugegriffen hat und von welchem Remote-Standort aus der Zugriff erfolgt ist.



Erkennung **Dell SMA End Point Control** erzwingt die Zugriffssteuerung für Geräte und stellt sicher, dass Benutzer nur auf autorisierte Anwendungen zugreifen.

Schutz **Dell SMA Unified Policy** erzwingt die Zugriffssteuerung für Geräte und stellt sicher, dass Benutzer nur auf autorisierte Anwendungen zugreifen.

Verbindung **Dell SMA Smart Access und Smart Tunneling** gewährleisten den einfachen und sicheren Benutzerzugriff auf alle Netzwerkressourcen.

Die Dell Secure Mobile Access Lösungen ermöglichen es Ihnen, allen Benutzern, Geräten und Anwendungen sicheren Zugriff bereitzustellen.

Technische Daten

Leistung	E-Class SRA 6000	SMA 6200	E-Class SRA 7000	SMA 7200	E-Class SRA 9000
Gleichzeitige Benutzer	Unterstützung für bis zu 250 gleichzeitige Benutzer pro Knoten oder HA-Paar	Unterstützung für bis zu 2.000 gleichzeitige Benutzer pro Knoten oder HA-Paar	Unterstützung für bis zu 5.000 gleichzeitige Benutzer pro Knoten oder HA-Paar	Unterstützung für bis zu 10.000 gleichzeitige Benutzer pro Knoten oder HA-Paar	Unterstützung für bis zu 20.000 gleichzeitige Benutzer pro Knoten oder HA-Paar
Hardware	**E-Class SRA 6000**	**SMA 6200**	**E-Class SRA 7000**	**SMA 7200**	**E-Class SRA 9000**
Formfaktor	1-HE-Gehäuse für Rack-Montage	1-HE-Gehäuse für Rack-Montage	1-HE-Gehäuse für Rack-Montage	1-HE-Gehäuse für Rack-Montage	2-HE-Gehäuse für Rack-Montage
Abmessungen	43,18 x 42,54 x 4,44 cm (17 x 16,75 x 1,75 Zoll)	43 x 41,5 x 4,5 cm (17 x 16,5 x 1,75 Zoll)	43,18 x 42,54 x 4,44 cm (17 x 16,75 x 1,75 Zoll)	43 x 41,5 x 4,5 cm (17 x 16,5 x 1,75 Zoll)	68,6 x 48,2 x 8,8 cm (27 x 18,9 x 3,4 Zoll)
Prozessor	Intel Celeron mit 2 GHz, 1 GB DDR533	Intel i5-4570S mit 2,9 GHz	Intel Core2 Duo mit 2,1 GHz, 2 GB DDR533	Intel E3-1725 v3 mit 3,5 GHz	Intel Xeon Quad-Core-Prozessor mit 2,46 GHz
Netzwerk	4 x 1GbE-PCIe-Stapelports	6 x 1GbE-Ports	6 x 1GbE-PCIe-Stapelports	2 x 10GbE-Ports, 6 x 1GbE-Ports	4 x 10GbE-SFP+-Ports, 8 x 1GbE-Ports
Stromversorgung	Festes Netzteil	Festes internes Netzteil	Zwei Netzteile (Hot-Swap-fähig)	Zwei Netzteile (Hot-Swap-fähig)	Zwei Netzteile (Hot-Swap-fähig)
Eingang	100 bis 240 V Wechselspannung, 1,2 A	100 bis 240 V Wechselspannung, 1,1 A	100 bis 240 V Wechselstrom, 1,5 A, 50 bis 60 Hz oder -36 bis -72 V Gleichspannung, 3,2 A	100 bis 240 V Wechselspannung, 1,7 A	100 bis 240 V Wechselspannung, 2,8 A
Stromverbrauch	75 W	78 W	150 W	127 W	320 W
MTBF	100.000 Stunden bei 35 °C (95 °F)	–	100.000 Stunden bei 35 °C (95 °F)	–	120.000 Stunden bei 35 °C (95 °F)
Umweltstandards	WEEE, RoHS EU, China RoHS				
Betriebstemperatur	0 bis 40 °C (32 bis 104 °F)				
Stoßbelastung (außer Betrieb)	110 g, 2 ms				
Gesetzliche Bestimmungen					
Emissionen	FCC, ICES, CE, C-Tick, VCCI, MIC				
Sicherheit	TÜV/GS, UL, CE, PSB, CCC, BSMI, CB Scheme				
Hauptmerkmale					
Sicherheit					
FIPS und ICSA Zertifizierung*	Ja				
Verschlüsselung	Konfigurierbare Sitzungslänge; Verschlüsselungsverfahren: DES, 3DES, RC4, AES; Hashfunktionen: MD5, SHA				
VPN-Protokolle	TLS 1.0, 1.1, 1.2, ESP				
Authentifizierungsmethoden	Digitale X.509-Zertifikate, serverseitige digitale Zertifikate, clientseitige digitale Zertifikate, RSA SecurID, Dell Defender und andere Authentifizierungs-Tokens für OTP-/Zwei-Faktor-Authentifizierung, Common Access Card (CAC), duale/mehrschichtige Authentifizierung, Captcha-Unterstützung, Benutzername/Kennwort				
Verzeichnisse	Microsoft Active Directory, LDAP (Active Directory, Sun iPlanet usw.), RADIUS; dynamische Gruppen auf Basis von LDAP-/AD Abfragen, Zertifikatsperrlisten (Certificate Revocation Lists, CRLs)				
Kennwortverwaltung	Benachrichtigung bei Ablauf und Änderung von Kennwörtern über das Dell SMA WorkPlace Portal, Connect Tunnel und Mobile Connect				
Zugriffssteuerungsoptionen	Benutzer und Gruppe, Quell-IP und Netzwerk, Zielnetzwerk, Dienst/Port (nur OnDemand und Connect); Ressourcen können anhand von Folgendem definiert werden: Ziel-URL, Hostname oder IP-Adresse, IP-Bereich, Subnetz und Domäne, Tag, Datum, Zeit, Länge des Browser-Verschlüsselungsschlüssels, Policy Zones, Zugriffssteuerungsoptionen des Dateisystems, VPN-Zugriffssteuerung für mobile Anwendungen.				
Dell SMA End Point Control (EPC)	Erkennung von Dateien, Registrierungsschlüsseln, laufenden Prozessen und Device Watermarks; erweitertes Abfragesystem (vereinfachte granulare Erkennung von Endpunkten, einschließlich detaillierter Konfigurationsinformationen für über 100 Virenschutz-, Spywareschutz- und persönliche Firewall-Lösungen, darunter McAfee, Symantec, Sophos und Trend Micro; Cache Control (Schutz von Daten); Erkennung, ob auf iOS Geräten ein Jailbreak durchgeführt oder Android Systeme gerootet wurden				
Automatische VPN-Verbindung	Ein netzwerksensitiver VPN-Client erkennt, ob das Gerät sich außerhalb des Unternehmensgeländes befindet, und stellt automatisch eine VPN-Verbindung her. Diese wird wieder getrennt, sobald das Gerät auf ein vertrauenswürdiges Netzwerk zugreift.				
Unterstützung in puncto Zugriff und Anwendungen					
Zugriff mit Dell SMA WorkPlace (browserbasierter Zugriff)	Clientloser Zugriff auf webbasierte Ressourcen; Zugriff auf Webdateien: SMB/CIFS, DFS, persönliche Lesezeichen; verschiedene optimierte WorkPlace Portale für verschiedene Benutzergruppen, die den Zugriff auf TCP- oder UDP-basierte Anwendungen ermöglichen (durch Nutzung des OnDemand Tunnel Agenten); HTML5-Browserzugriff auf Citrix XenDesktop und XenApps sowie auf via RDP veröffentlichte Anwendungen und Desktops				
Mobilzugriff über Dell SMA WorkPlace	Unterstützung für das anpassbare WorkPlace Portal für Smartphone- und Tablet-PC-Browser; HTML5-Browserzugriff auf Citrix XenDesktop und XenApps sowie auf via RDP veröffentlichte Anwendungen und Desktops				
Connect Tunnel	Zugriff auf TCP- oder UDP-basierte Anwendungen dank eines vorinstallierten Agenten (Windows, Mac und Linux Unterstützung)				
SonicWALL Mobile Connect	Vollständiger Zugriff aus Netzwerkebene für Web- und Client/Server-Anwendungen über Apple iOS, Mac OS X, Kindle Fire, Android und Windows 8.1 Geräte (Umfassende Informationen finden Sie im SonicWALL Mobile Connect Datenblatt.)				
Verwaltung und Administration					
Verwaltung	Die Verwaltungskonsole ermöglicht die zentralisierte, webbasierte Verwaltung für alle Zugriffsoptionen sowie die Konfiguration der Endpunktkontrolle und die Verwaltung von Zugriffssteuerungsrichtlinien, Zugriffssteuerungsrichtlinien für mobile Anwendungen und WorkPlace Portalkonfigurationen. Sie bietet Funktionen für die einfache Replikation von Richtlinien über mehrere Appliances und Standorte hinweg sowie die rollenbasierte Verwaltung über ein Dashboard, das Informationen auf einen Blick bereitstellt.				
Prüfungen	SMA Advanced Reporting, integrierte Überwachung/integriertes Accounting auf Basis von RADIUS				
Überwachung und Protokollierung	Überwachung von Benutzerverbindungen, Alarme bei Ereignissen; Dell SNMP-Integration zur Anzeige von Protokollen und Leistungsinformationen, einschließlich SMA-spezifischer SNMP-MIB (Management Information Base); Unterstützung für einen zentralen Syslog-Server				
Planer	Benutzer haben die Möglichkeit Aufgaben (wie Bereitstellungen, die Replikation von Einstellungen und die Anwendung von Änderungen) ohne manuelle Eingriffe zeitplangesteuert ausführen zu lassen.				
Integration mit Technologien zur Mobilgeräteverwaltung	Problemlose Integration mit führenden Produkten für die Verwaltung von mobilen Geräten in Unternehmen wie Dell EMM, AirWatch und MobileIron; Bei einer Bereitstellung mit dem Dell Mobile Workspace (DMW) Container bietet der Container richtlinienbasierten Schutz vor Datenverlust für gespeicherte Daten und die SMA Lösung erzwingt Proxy-Schutz am Netzwerkrand für wichtigen ActiveSync und HTTP-Datenverkehr. Mit der Richtlinien-Engine für Endpunktkontrolle stellt die SMA sicher, dass nur dem abgesicherten DMW Browser und E-Mail-Client der Zugriff auf Daten gewährt wird – alle anderen Anwendungen auf dem Gerät werden blockiert.				
Hochverfügbarkeit					
Hochverfügbarkeit	Unterstützung für Zwei-Knoten-Hochverfügbarkeitscluster mit integriertem Lastausgleich und Stateful Authentication Failover				
Sonstiges					
Unterstützung für IPv6	Unterstützung der Authentifizierung eines Clients mit IPv6-Internetkonnektivität, der dann über die SMA Appliance auf Ressourcen zugreifen kann				
Für die Nutzung durch Mitarbeiter mit Behinderung geeignet (ADA 508)	Verwaltungskonsole, WorkPlace und Connect Tunnel mit Unterstützung für ADA 508 zur Einhaltung von Abschnitt 508 des Americans with Disabilities Act, einschließlich Benutzerfreundlichkeit der Tastatur und Kompatibilität mit unterstützenden Technologien				
Browser-Unterstützung	Die SMA Appliances unterstützen alle branchenführenden Browser, einschließlich Internet Explorer, Firefox, Chrome und Safari (und die Liste der unterstützten Versionen wird fortlaufend aktualisiert). Außerdem unterstützen sie den HTML5-Browserzugriff auf Citrix XenDesktop und XenApps sowie auf via RDP veröffentlichte Anwendungen und Desktops. Benutzer mit HTML5-kompatiblen Browsern können auf sichere Weise auf diese Anwendungen zugreifen, ohne den Risiken oder Bedrohungen ausgesetzt zu sein, die mit den bei Legacy-Browsern erforderlichen Java oder ActiveX Plug-ins verbunden sind. Außerdem können auch Benutzer mit Geräten, die Java oder ActiveX nicht unterstützen, einen HTML5-Browser nutzen, um über das SMA Webportal auf die Anwendungen zuzugreifen.				
	E-Class SRA Virtual Appliance				
Gleichzeitige Benutzer	Bis zu 5.000				
Hypervisor	ESG und ESX (Version 4.0 und höher), HyperV				
Installiertes Betriebssystem	Gehärtetes Linux				
Zugewiesener Arbeitsspeicher	2 GB				
Benötigter Festplattenspeicher	80 GB				
Handbuch zur Hardwarekompatibilität	http://www.vmware.com/resources/compatibility/search.php				

* Die FIPS und ICSA Zertifizierungen für die SMA 6200/7200 Appliances sind im Gange.

Bestellinformationen

Produkt	SKU
E-Class SRA 6000	01-SSC-9601
SMA 6200	01-SSC-2300
E-Class SRA 7000	01-SSC-9602
SMA 7200	01-SSC-2301
E-Class SRA 9000	01-SSC-9574
E-Class SRA Virtual Appliance	01-SSC-8468
Dell SMA Lizenz für fünf Benutzer – stapelbar	01-SSC-7856
Dell SMA Lizenz für zehn Benutzer – stapelbar	01-SSC-7857
Dell SMA Lizenz für 25 Benutzer – stapelbar	01-SSC-7858
Dell SMA Lizenz für 50 Benutzer – stapelbar	01-SSC-7859
Dell SMA Lizenz für 100 Benutzer – stapelbar	01-SSC-7860
Dell SMA Lizenz für 250 Benutzer – stapelbar	01-SSC-7861
Dell SMA Lizenz für 500 Benutzer – stapelbar	01-SSC-7862
Dell SMA Lizenz für 1.000 Benutzer – stapelbar	01-SSC-7863
Dell SMA Lizenz für 2.500 Benutzer – stapelbar	01-SSC-7864
Dell SMA Lizenz für 5.000 Benutzer – stapelbar	01-SSC-7865
Dell SMA Lizenz für 7.500 Benutzer – stapelbar	01-SSC-7948
Dell SMA Lizenz für 10.000 Benutzer – stapelbar	01-SSC-7949
Dell SMA Lizenz für 15.000 Benutzer – stapelbar	01-SSC-7951
Dell SMA Lizenz für 20.000 Benutzer – stapelbar	01-SSC-7953

Über Dell Software

Dell Software unterstützt Kunden dabei, ihr Potenzial durch den Einsatz von Technologie voll auszuschöpfen – mit skalierbaren, erschwinglichen und benutzerfreundlichen Lösungen, die die IT vereinfachen und Risiken minimieren. In Kombination mit Hardware und Services von Dell versetzen unsere Softwareprodukte Kunden in die Lage, effizienter und produktiver zu arbeiten und schnellere Geschäftsergebnisse zu erzielen. www.dellsoftware.de

Dell Software
www.dell.com
Informationen zu unseren Niederlassungen außerhalb Nordamerikas finden Sie auf unserer Webseite.

Datasheet-SMA-US-KS-26075