LÖSUNGSPROFIL

Sind Ihre Filialen eine offene Tür für Cyberangriffe?

Wie SD-Branch bei erhöhter Expositionsgefahr, begrenzten Ressourcen und steigenden Kosten eine sichere Lösung bieten kann

Zusammenfassung

Herkömmliche Methoden zur Bereitstellung und Aufrechterhaltung von Sicherheit an Filialstandorten sind unwirksam, zu teuer und unüberschaubar geworden. Eine SD-Branch-Lösung kann als Grundstein für grenzenlose Sicherheit in verteilten Unternehmensumgebungen dienen.

Wir stehen einer explosionsartigen Vermehrung von Schwachstellen gegenüber

2019 verzeichneten die Bedrohungsforscher von SonicWall Capture Labs 9,9 Milliarden Malware-Angriffe. In den letzten fünf Jahren überwältigten Cyberkriminelle ihre Opfer mit einem enormen Angriffsvolumen. Ihr Ziel: ein größtmögliches Netz auswerfen und dann davon profitieren. Mit der Weiterentwicklung von Cyberabwehrmethoden sind leider auch die Angriffe gezielter und noch erfolgreicher geworden.

Darüber hinaus erlebt die Netzwerk- und Securityumgebung eine digitale Transformation, die durch eine explosionsartige Vermehrung von mobilen und IoT-Geräten ausgelöst wurde. In großen Unternehmen führte dieser Wandel dazu, dass man sich verstärkt auf mobile Clients verlässt und Mobile-First-Netzwerke einrichtet. Ein weiterer Katalysator für diese Änderung ist der Umzug in die Cloud und der weit verbreitete Einsatz von Cloud-Anwendungen. Da geschäftskritische Anwendungen wie MS Office in die Cloud verlagert werden und Unternehmen Cloud-Anwendungen wie Salesforce oder Workday für ihre alltägliche Arbeit nutzen, kommt dem Schutz dieser Cloud-Anwendungen eine noch größere Bedeutung zu. Diese digitale Transformation treibt die Nachfrage nach leistungsstarken Appliances an, die mit den steigenden Datenanforderungen Schritt halten können.

Die stetig steigenden Kosten der Konnektivität

Mobile-First-Standorte oder Filialen sind bei der Ausführung ihrer alltäglichen Arbeit stark auf bandbreitenintensive Anwendungen angewiesen. Von diesen für das Streaming von Videos oder anderen Inhalten oder das Arbeiten mit Office 365 verwendeten bandbreitenintensiven Anwendungen sind einige geschäftskritisch und andere wiederum nicht. Diese Verkehrsarten müssen effizient getrennt werden. Stellen Sie sich die unerschwinglichen Kosten vor, die entstehen würden, wenn Sie den gesamten Datenverkehr der Filialstandorte über teure MPLS-Verbindungen in die Unternehmenszentrale zurück transportieren würden.

Glücklicherweise können Kosten gesenkt werden, indem für unkritischen Datenverkehr ein kostengünstiger Internetzugang genutzt wird, während geschäftskritischer Datenverkehr durch einen dynamischen Pfadauswahlmechanismus priorisiert werden kann. Einige der für den Betrieb eines verteilten Unternehmens oder Filialen kritischen Anwendungen erfordern jedoch redundante Konnektivität, um eine unterbrechungsfreie Betriebszeit sicherzustellen.

Eine Möglichkeit, redundante Konnektivität für diese Niederlassungen zu gewährleisten, ist eine Lösung, die hochverfügbare und leistungsstarke WANs mit WAN-Lastverteilung bietet. Dies kann durch den Einsatz von softwaredefinierter WAN-Technologie (SD-WAN) erreicht werden.

Durch Verwendung eines kostengünstigen Internetzugangs (Breitband, 3G/4G/LTE, Glasfaser) können Unternehmen teure WAN-Verbindungstechnologien wie MPLS durch kostengünstige SD-WAN ersetzen. Doch die Umsetzung dieser Lösungen und gleichzeitige Ermöglichung einer

Verwaltung der gesamten Netzwerksicherheitslösung von einer zentralen Benutzeroberfläche aus scheint schwer machbar zu sein.

Der Kampf mit schrumpfenden Ressourcen

Die Kosten der konventionellen Sicherheit werden zunehmend unerschwinglich und der Mangel an geschultem Personal wird akuter. Begrenzte Budget- und Personalressourcen können einfach nicht mithalten und führen zu einer Lücke im Cybersecurity-Geschäft.

Multipoint-Produkte erschweren den Filialen die Bereitstellung, Konfiguration, Verwaltung und Fehlerbehebung der Lösung. Mit einem End-to-End Security Stack können Firewalls, Switches, Access Points, Cloud-Security und End-Point-Clients vereinheitlicht werden, um ein Single-Pane-of-Glass-Management zu ermöglichen, das die produktübergreifende Transparenz und Kontrolle verstärkt. Dieser End-to-End Security Stack ermöglicht ein hohes, einheitliches Sicherheitslevel.

Entscheidend ist auch, dass sich die Art und Weise der Netzwerkwartung verändert hat. Sie können mit dieser digitalen Transformation Schritt halten, wenn Sie Ihre Organisation auf einem hohen Sicherheitsniveau halten. Wenn es nicht gelingt, ein einheitliches Sicherheitslevel zu erreichen, wird es für Organisationen bei der Verwaltung und Kontrolle der wachsenden Anzahl an Geräten im Netzwerk zu Komplikationen kommen. Bedrohungen würden nicht erkannt und Unternehmen wären gezwungen, einen reaktiven anstatt einen proaktiven Ansatz zu verfolgen.

Darüber hinaus kann die großangelegte Implementierung zur Herausforderung werden, wenn keine Technologien wie Zero-Touch Deployment verfügbar sind. Techniker müssten zu jeder Filiale fahren, um jedes dieser Geräte manuell zu konfigurieren. Die Implementierung an allen Filialen und letztendlich auch weltweit wäre mit einem enorm erhöhten Kosten- und Zeitaufwand verbunden.

Außerdem müssen Filialen ebenso wie die Unternehmenszentrale einen sicheren WLAN-Zugang bieten, der eine hohe Leistung und hervorragende Benutzererfahrung bietet. Mitarbeiter und Gäste erwarten ein allgegenwärtiges WLAN, das zuverlässig, schnell und leistungsstark ist.

Wie Ihnen SD-Branch nutzen kann

Die Weiterentwicklung der Technologie auf Filialenebene ist heute wichtiger denn je. Herkömmlich ausgestattete Filialen können mit den steigenden Anforderungen der raschen Vermehrung von mobilen und IoT-Geräten nicht Schritt halten. Bei diesem raschen Anstieg der Anzahl von Geräten werden Verwaltung und Sicherheit zur Herausforderung, da möglicherweise ganz andere Regeln erforderlich sind. Die Verfügbarkeit einer einheitlichen Regelung für Ihr LAN und WAN über eine zentrale Benutzeroberfläche wird von entscheidender Bedeutung.

Darüber hinaus können über die Managementkonsole umfassende Analysen erstellt werden, die das gesamte Sicherheitsökosystem erfassen. Mit zunehmendem Einsatz von Cloud-Technologie ist für die WAN-Konnektivität filialenübergreifend eine intelligente Architektur erforderlich, um neben den teuren MPLS-Verbindungen auch billigere Internetverbindungen nutzen und Zero-Touch Deployment ermöglichen zu können.

Nur so lässt sich eine betriebliche Agilität erreichen. Zero-Touch Deployment-fähige Geräte lassen sich von Unternehmen schnell von zentraler Stelle aus implementieren und einführen, sodass IT-Fachkräfte nicht mehr an zahlreiche Standorte fahren müssen, um diese Lösungen zu konfigurieren und einzubinden. Für die Gewährleistung von Kontinuität, Integration und Skalierbarkeit brauchen Unternehmen ein optimiertes SPOG-Management mit Dienstleistungen von einem zentralen Anbieter.

Die SD-Branch-Lösung ergänzt das SD-WAN und befördert es auf eine neue Ebene von Konnektivität und Flexibilität. SD-Branch verwandelt die SD-WAN-Technologie in eine maßgeschneiderte Lösung für den Einsatz in Filialen. Diese Lösung bietet eine erweiterte Funktionalität und weitaus mehr Möglichkeiten als nur die Bereitstellung von Konnektivität zwischen Filialen. SD-Branch umfasst SD-WAN, LAN-Konnektivität und Sicherheit. Darüber hinaus wird durch Zero-Touch Deployment und die SPOG-Verwaltung der Bedarf an IT-Personal reduziert, was wiederum zu reduzierten Betriebskosten führt.

Fazit

Für verteilte Unternehmen ist die Sicherung ihrer Filialen aufgrund des Anstiegs potentieller Schwachstellen, begrenzter Ressourcen und steigender Kosten oft eine große Herausforderung. Dies trägt letztendlich zu einer wachsenden Cybersicherheitslücke im Unternehmen bei.

Eine effektive Lösung kombiniert die Agilität von SD-Branch mit End-to-End-Sicherheit, Netzwerksegmentierung und Compliance. Dies ermöglicht die Durchsetzung einheitlicher Regeln im gesamten Netzwerk-Ökosystem und bietet granulare Sicherheitskontrollen zur Erkennung und Verhinderung von komplexen und noch nie dagewesenen Attacken, bevor diese Ihr Netzwerk kompromittieren.

SonicWall sieht SD-Branch als Eckpfeiler für die grenzenlose Sicherheit in unserem hyperverteilten Zeitalter. Die SonicWall SD-Branch-Lösung sichert die Konnektivität und transformiert die Benutzererfahrung in den Filialen durch die Bereitstellung einer integrierten Plattform, die es Filialen ermöglicht, günstigere Konnektivität (SD-WAN) zu nutzen, BYOD zu aktivieren, SaaS-Anwendungen anzunehmen und sich mit der Unternehmenszentrale und anderen Filialen zu verbinden. SD-Branch integriert SD-WAN, Zero-Touch Deployment, Single-Pane-of-Glass-Management, einheitliche Transparenz und Bedrohungserkennung, Firewalls der nächsten Generation, sichere Switches, Wireless Access Points, Endpoint Security und Cloud App Security.

Mehr erfahren: Lesen Sie unser SonicWall SD-Branch-Lösungsprofil.

Über SonicWall

SonicWall bietet Boundless Cybersecurity für das hyperverteilte Umfeld einer neuen Arbeitsrealität, in der jeder remote, mobil und ungeschützt ist. Indem SonicWall das Unbekannte kennt, Echtzeit-Transparenz und skalierbare Ökonomien ermöglicht, werden Cybersicherheitslücken bei Unternehmen, Regierungen und KMU weltweit geschlossen. Weitere Informationen finden Sie auf www.sonicwall.com.

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

ExecutiveBrief-AreYourBranchSites-US-VG-1980