Vier SD-WAN-Sicherheitshürden, die es zu überwinden gilt

Die größte Herausforderung bei SD-WAN besteht darin, dass herkömmliche Sicherheitslösungen nicht ausreichen

Lassen Sie uns vier Hürden untersuchen, die Sie auf Ihrem Weg zu SD-WAN überwinden müssen, und die effektivste Methode zur Absicherung Ihres Deployment aufzeigen.

HÜRDE 1 Verlässlichkeit der Firewall im SD-WAN Edge-Gerät

Eine Beschränkung auf die native Sicherheit von SD-WAN hinterlässt erhebliche Schwachpunkte.

Die meisten verfügen nicht über einen angemessenen Schutz vor modernen Bedrohungen mit Funktionen wie NGFW, Sandboxing, Advanced Threat Prevention, IPS und DNS-Sicherheit.

Worauf sollte man bei einer Lösung achten?

- Eine auf Anwendungen, Protokolle und Inhalte ausgerichtete Cloud-basierte Firewall.
- Untersuchung von Traffic innerhalb und außerhalb des Netzwerks für alle Benutzer, Applikationen, Geräte und Standorte.
- Fähigkeit, Zugangsentscheidungen aufgrund des angeforderten Inhalts statt nur des Ziels zu treffen.

HÜRDE 2 Geben Sie den Gedanken auf, dass herkömmliche Sicherheitsansätze der Aufgabe gewachsen sind

Bei Abstrichen leidet die Effizienz.

Die Platzierung von Appliances in jeder Niederlassung ist unerschwinglich teuer und führt zu Sicherheits- oder Leistungseinbußen.

Backhauling von Traffic zu regionalen Hubs ist ebenfalls keine Lösung, da dies zu Latenzen und erhöhten Kosten führt.

Worauf sollte man bei einer Lösung achten?

- Identischer Schutz für alle Benutzer mit umfassender Sicherheit aus der Cloud.
- Breakout und Überprüfung aller Ports und Protokolle, einschließlich SSL-verschlüsseltem Traffic.

HÜRDE 3 Verlassen Sie sich für die Überprüfung von verschlüsseltem Traffic nicht auf vorhandene Sicherheitsarchitekturen

Die Überprüfung von verschlüsseltem Traffic ist äußerst wichtig.

Herkömmliche Firewalls überprüfen SSL-Traffic nicht standardmäßig.

Das Aktivieren der Überprüfung beeinträchtigt in der Regel die Leistung. Deshalb umgehen einige Unternehmen die SSL-Überprüfung, was sie einem höheren Risiko aussetzt.

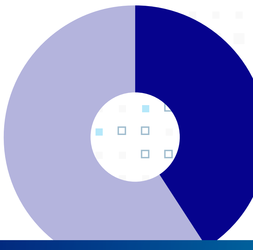
Worauf sollte man bei einer Lösung achten?

- Eine Proxy-basierte Architektur, die SSL-verschlüsselten Traffic standardmäßig überprüft.
- Überprüfung des gesamten Traffic ohne Leistungseinbußen.
- Elastische Skalierbarkeit mit Zunahme des Traffic und der Benutzerzahl.

Mehr als

41%

aller Netzwerkangriffe sind heutzutage verschlüsselt, um nicht entdeckt zu werden[1].



HÜRDE 4 Vermeiden sie die falle mehrerer plattformen für die sicherheitsverwaltung

Veraltete Technologien stellen eine Herausforderung dar.

Das Erfassen und Korrelieren von Aktivitäten ist schwierig.

Die Durchsetzung von Richtlinienänderungen erfordert normalerweise individuelle Verwaltungsschnittstellen oder manuelles Deployment.

Eine zeitnahe Bereitstellung von Transparenz und Reporting ist mit Appliances in jeder Niederlassung äußerst schwierig.

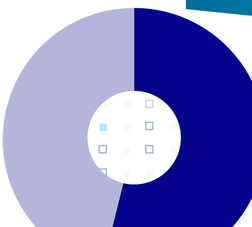
Worauf sollte man bei einer Lösung achten?

- Ein flexibles Framework, das umsetzbare Erkenntnisse liefert.
- Eine einzige Plattform zum Korrelieren und Anzeigen von Logs.
- Ist in der Lage, Richtlinien zentral zu definieren und sofort an allen Standorten durchzusetzen.

54%

aller Organisationen

nannten erhöhte Technologiekomplexität als Hauptbedenken in Bezug auf gegenwärtige Methoden zur Absicherung von Internetverbindungen an den Standorten[2].



Möchten Sie mehr darüber erfahren?

Lesen Sie das vollständige Whitepaper

zscaler™

[1] Ponemon Institute, „Hidden Threats in Encrypted Traffic: A Study of North America and EMEA." 2016
[2] Umfrage von Network World, Inc. unter IT-Direktoren von 100 Organisationen

zscaler.com