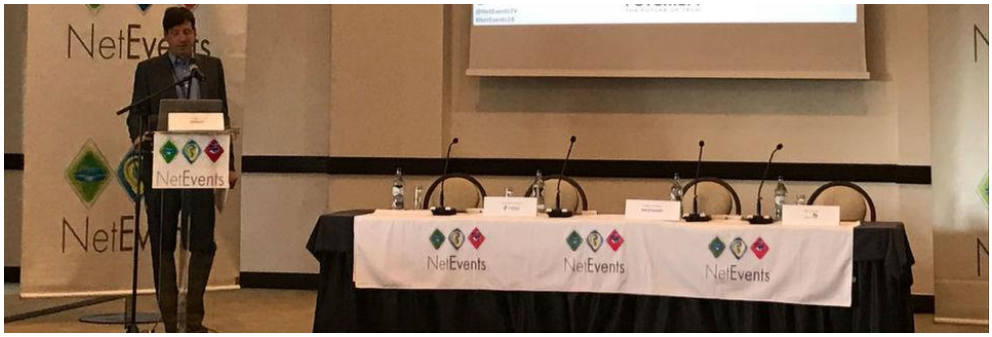
https://www.security-insider.de/neue-modelle-fuer-wans-und-endpoint-security-a-767875/
Neue Modelle für WANs und Endpoint Security
24/10/18

## Nachbericht NetEvents EMEA Press Summit 2018

# Neue Modelle für WANs und Endpoint Security

24.10.18 | Autor / Redakteur: Oliver Schonschek / Andreas Donner




Spannende Roundtables, Podiumsdiskussionen und Face-to-Face-Meetings kennzeichneten das 2018er Press-Meeting von NetEvents. (Bild: Donner / VIT)

- Multi-Clouds, IoT und Mobile Computing haben die Anforderungen an die Netzwerk- und Endpunkt-Sicherheit deutlich erhöht. Auf der Konferenz NetEvents EMEA Press Spotlight in Portugal wurden neue Lösungen und Konzepte vorgestellt, die auch für Service Provider in Deutschland spannend sind.

Cloud-basierte Anwendungen und Virtualisierung haben die Netzwerkanforderungen deutlich verändert, weg von Geräten und Boxen und hin zu nativen anwendungsbasierten Netzwerklösungen, so Scott Raynovitch, Principal Analyst bei Futuriom, auf der NetEvents-Konferenz in Portugal.

Die zunehmende Verlagerung von Anwendungen von On-Premises auf Hybrid-Cloud Umgebungen stellt IT- und Netzwerk-Manager vor viele Herausforderungen, wie eine Umfrage von Futuriom ergab:

BILDERGALERIE

Fotostrecke starten: Klicken Sie auf ein Bild (4 Bilder)

- Virtual Private Networks (VPNs) verursachen Leistungseinbußen, sagen 63,5% der befragten Unternehmen in den USA.
- 75% der VPN-Benutzer gaben an, dass sie eine bessere Lösung für Cloud-Netzwerke suchen.
- 43,5% der befragten Benutzer gaben an, dass SD-WAN keine ideale Lösung für die Vernetzung von industriellen IoT-Geräten ist.

Bestimmung der Cyber ExposureQuantifizierung des Zeitvorteils von AngreifernCyberverteidigerstrategienWas Ihre Vulnerability Assessment Praktiken zeigenAls Alternative empfahl der Futuriom-Analyst die Application Specific Networks (ASNs). ASNs sind reine Softwarelösungen, die Anwendungen verknüpfen. Im Gegensatz zu VPNs können ASNs automatisch bereitgestellt werden und benötigen kein manuelles Setup oder spezielle Hardware, so Scott Raynovitch. Als Vorteile der ASNs nannte er insbesondere:

- Einfache Bereitstellung
- Kein „Box Management“ notwendig
- Eher auf DevOps und Softwareentwickler ausgerichtet als auf Netzwerkspezialisten

Als Beispiel für ASNs wurde NetFoundry AppWAN vorgestellt. NetFoundry verbindet Apps über das Internet, während SD-WAN- und MPLS-Netzwerke Standorte mit benutzerdefinierter Hardware verbinden. NetFoundry ermöglicht es Entwicklern und Integratoren, das NetFoundry AppWAN so zu programmieren, dass es den spezifischen Anforderungen entspricht.

Ähnlich wie Unternehmen Webkonsolen von Amazon AWS und Microsoft Azure verwenden, um virtuelle Maschinen zu verwalten, können Unternehmen die Webkonsolen und APIs von NetFoundry nutzen, um globale Netzwerke nach Bedarf zu entwickeln. NetFoundry bietet dafür einen vollständig verwalteten Dienst und verwaltet die zugrundeliegenden Netzwerke und die Infrastruktur.

## SD-WAN Services

Ebenfalls als neuer Ansatz vorgestellt wurde die Lösung von Versa Networks. Versa bietet eine Cloud-native Multi-Service-Softwareplattform mit mehreren Diensten, die eine flexible Skalierung, Segmentierung, Programmierbarkeit und Automatisierung ermöglichen soll. Versa Secure Cloud IP integriert Cloud-Netzwerke, SD-WAN, drahtlose und mobile Konnektivität und softwaredefinierte Sicherheitsdienste (NGFW / UTM).

„Durch die Anwendung der Plattformarchitektur von Versa auf Multi-Cloud-, Enterprise Edge- und Managed Security-Umgebungen können Software-definierte Zweigstellen mit weniger Hardwaregeräten bereitgestellt und Vorgänge rationalisiert werden“, sagte Atchison Frazer, Marketing-Leiter bei Versa Networks.

Zu den genannten Anwendungsfällen von Unternehmen und Service Providern gehören:

- Vollständig softwaredefinierte Verzweigung (SD-Branch) für Unternehmenskunden
- Secure SD-WAN für Unternehmen mit mehrschichtiger Sicherheit
- Managed Services wie SD-Branch und SD-WAN für Service Provider
- Managed SD-Router- und SD-Security-Services für Service Provider

## Machine Learning für Endpoint Security

Ein Roundtable während der NetEvents-Konferenz war dem Trendthema „The Security Professional’s Best Friend: Artificial Intelligence“ gewidmet. Die Diskussion zeigte, dass der Weg zu einer wirklichen AI noch weit ist, und man besser von Machine Learning (ML) sprechen sollte. Es gibt zahlreiche Ansätze in der Security, die ML nutzen, darunter die auf der Konferenz präsentierte Lösung von Ziften.

Ziften bietet eine Cloud-basierte Endpunktschutzplattform, die Angriffe auf alle Endpunkte des Unternehmens, Laptops, Desktops, Server und Cloud VMs, verhindern soll. Auf den Endpunkten wird ein über die Cloud bereitgestellter Agent installiert, die Plattform liefert Antivirus-Funktionen, Endpoint Detection and Reponse sowie Härtung und Inventarisierung der Endpoints. Unterstützt werden Windows, MacOS und Linux.

Da die auf Machine Learning basierenden Funktionen auch ohne Online-Verbindung über den Agenten bereitstehen, können auch solche Endpunkte geschützt werden, die sich außerhalb des Unternehmensnetzwerkes befinden oder offline betrieben werden. Im Rahmen einer Microsoft-Partnerschaft bietet Ziften über den Azure Marketplace Unternehmen die Ausweitung von Windows Defender ATP auf MacOS und Linux Systeme an.

Ziften baut seine Channel-Partnerschaften weiter aus, insbesondere durch gemeinsame Channel-Partner mit Microsoft, darunter in Großbritannien und Irland der Microsoft Windows Defender ATP - Spezialist Threatscape, in Middle East der Channel-Partner Paramount und in den Niederlanden der Channel-Partner Insight.

## Chancen für Service Provider

Neue Ansätze zur sicheren Vernetzung bei Multi-Cloud-Nutzung, im IoT / IIoT und für Mobile Computing bieten auch neue Möglichkeiten für Service Provider, die Networking- und Security-Services für ihre Kunden anbieten und betreiben können. Studien von Analysys Mason, die auf der NetEvents-Konferenz präsentiert wurden, zeigen, dass vielen Unternehmen die Fähigkeiten und Toolsets fehlen, um komplexe Cloud-Lösungen zu verwalten. Networking- und Security-Dienste, die Service Provider über die Cloud bereitstellen können, bieten den Unternehmen passende Unterstützung an. Alleine auf Automatisierung und Künstliche Intelligenz können Unternehmen (noch) nicht hoffen, wenn es um sicheres Networking geht. Service Provider für Networking und Security sind in Zeiten des Fachkräftemangels also langfristig gefragt.