POINT OF VIEW: MODERN NETWORKING

Networking must be dynamic, flexible, and secure to enable new and unanticipated connectivity required to support digital transformation.

EVOLVING SOLUTIONS

www.evolvingsol.com

MODERN NETWORKING

Networking must be dynamic, flexible, and secure to enable new and unanticipated connectivity required to support digital transformation. To accomplish this, an effective networking strategy must encompass several key characteristics:

- Multi-cloud-enabled and software-defined
- Automated and API-driven
- Consistent security posture from core to edge to cloud
- End-to-end Zero Trust approach
- Enhanced network monitoring

MULTI-CLOUD-ENABLED AND SOFTWARE-DEFINED

An organization's network is the critical connector between applications, which may reside in private or public data centers, and its end users. Those users are constantly changing modes of access based on how their business is accomplished: they may be working at the office, from home, or in a public place, all while utilizing a variety of devices, from corporate PCs to personal mobile devices.

Users require the same level of connectivity to applications regardless of where that app resides. The challenge is to automate centralized management with consistent visibility into network and security health and performance, while providing the best user experience geographically and connectivity-wise.

To meet those expectations and business requirements, applications require a highly available (HA) infrastructure, regardless of hosting environment. A robust Disaster Recovery (DR) plan is also a critical requirement for enterprise applications. Modern software-defined networking technologies help technology professionals build infrastructures with effective HA and DR capabilities to meet their organization's needs in a multi-cloud world.

A robust overlay of software-defined networks on top of the network framework is quickly scalable to support emerging technologies and address unexpected changes. It allows users to easily spin up new clouds or services, complete basic network changes, make applications run faster and more reliably, and enables advanced monitoring.

AUTOMATED AND API-DRIVEN

According to IDC, "**50%** of CIOs will accelerate robotization, automation and augmentation by **2024**, making change management a formidable imperative." [1]

By using an automated Application Programming Interface (API) driven methodology, new technology can be acquired, configured, deployed, consumed, maintained, and sunset in a self-service or automated manner with minimal disruption.

Some solutions boast network automation out of the box, but true automation requires comprehensive strategic planning. Network teams should focus on enabling agility within their organization's network and collaborate with their Dev/Ops and cloud peers to unlock the power of modern APIs in SDN networks. This is how true flexibility is achieved.

Network teams should be empowered to create network standards, frameworks, and templates to guide and govern other developers and technologies.

Within the established network guard rails, users then have free reign with the benefits of automation skillsets, consistency, repeatability, and security.

The ideal end state is infrastructure as code, which allows an organization the ability to abstract a complex network into as set of APIs and treat its data center similar to a public cloud. In this scenario, users can quickly build open APIs, third party platform integration, and more.

[1] IDC FutureScape 2021: Worldwide CIO Agenda 2021 Predictions

CONSISTENT SECURITY POSTURE FROM CORE TO EDGE TO CLOUD

According to IDC, "The need to deliver infrastructure, application, and data resources to edge locations will spur adoption of new, cloud-centric edge and network solutions that enable faster responses to current business needs while serving as a foundation for boosting long-term digital resilience, enabling business scaling, and ensuring greater business operational flexibility." [2]

Today's networks face many evolving concerns and issues: geographically diverse data centers, public and private clouds connectivity with SaaS and PaaS applications and services, and end users who are on the move—working on a variety of secured and unsecured networks. As a result, enforcing and maintaining security is more challenging and more critical than ever before. Controls and logs are difficult to implement or non-existent. Ensuring an organization's employees adhere to security controls is difficult at best and further complicated by a diversity of devices and locations. Further, networks are under attack from outside threats at unprecedented rates.

Network managers must have visibility into the security patterns of users for logging, encrypting users' connectivity, and to stop potential outbreaks. A consistent security posture, once established, allows the enforcement of pre-defined security policies that segment access and enable administrators to disable access to back-end systems quickly when the policies are violated.

END-TO-END ZERO TRUST APPROACH

According to RiskBased Security, thousands of vulnerabilities across networks, applications, and a multitude of technology solutions are detected annually.

[2] IDC FutureScape: Worldwide IT and Industry 2021 Predictions

More than 15 billion records were exposed in 2019 alone, which represented a 284% increase on the previous year.[3]

Traditional network security models rely on the principle of trusted and untrusted networks. With current user mobility and multi-cloud architectures, this model is no longer assured. Zero Trust eliminates the idea of trust from an organization's network. By default, it assumes a breach is always ongoing. With over 23,000 vulnerabilities detected during 2020[4], an organization would be prudent to adopt this approach.

There is no single solution to an effective Zero Trust approach, but organizations can implement a strategy for locking down user-to-application, user-to-user, and app-to-app communications. Teams can begin by allowing communication only between required components, thus limiting access via segmentation. In addition, a Zero Trust strategy must include logging and encryption for all assets within the company's network topology. With this strategy in place, an organization will have multiple avenues to solve issues and create a constant tracking and feedback system for existing security and alerting tools.

ENHANCED NETWORK MONITORING

It is critical to identify and close the gaps between disparate teams that oversee the data center, applications, public cloud, monitoring, networking, and security. How can technology leaders deliver on this? How can these gaps be bridged? A critical objective should be to enable monitoring more broadly to achieve network visibility end-to-end.

To get started, technology teams should first monitor the user experience (UX). Teams can be proactive and use simulated/synthetic user tests to identify issues. Rigorous UX testing exposes issues when and where they exist: site, switch, connection, computer, app, internet, etc. Successfully executing this approach is far more effective than leveraging centralized monitoring only. A main component of user experience, internet uptime, is more critical than ever and must be monitored closely for the health of entire network infrastructure.

[3] Risk Based Security 2019 Year End Report | Data Breach QuickView [4] Risk Based Security 2020 Year End Report | Data Breach QuickView

ACTION RECOMMENDATIONS

- Assess your existing network and end user security posture and policies to evaluate their effectiveness in a multi-cloud and mobile user environment
- Prioritize API-driven software-defined capabilities when considering new infrastructure solutions and implement those capabilities gradually in support of initiatives
- Develop a software-defined network adoption roadmap to support multi-cloud solutions
- When undertaking cloud or new application initiatives, begin with a Zero Trust approach

---

Contact networking@evolvingsol.com for more information