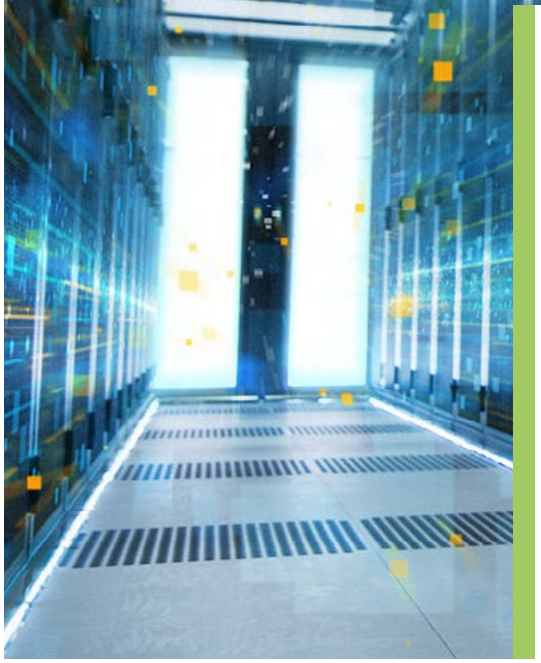


POINT OF VIEW

Developing a Modern Networking Strategy

How automated, multicloud-enabled, secure modern networking streamlines operations, reduces data breach risk, delivers savings, and more

In today's world, everything is multicloud-enabled and software-defined. Networking has shifted from traditional box-by-box approaches to more coordinated, automated strategies.

EVOLVING SOLUTIONS

A modern networking environment is not just about working with a specific networking product. It is about integrating with other components within your organization—such as identity providers (e.g., Azure AD, Okta, etc.) and network identity platforms (ClearPass and ISE)—while ensuring network access control to approve or deny what can and cannot be done based on identity and not network constructs.

Here is another way to think about it: Modern networking connects people or endpoints to applications, instead of connecting network to network. This is a critical difference from traditional networking. A modern network must be agile and scalable from a cost and business standpoint, allowing for growth depending on evolving transformational needs.

An effective modern networking strategy in today's cloud-connected world must be:

- Multicloud-enabled and software-defined
- Automated and API-driven to enable collaboration and rapid changes
- Secured from end-to-end, including:
  - Consistent, strong security polices
  - Effective access controls
  - Constant monitoring
  - Complete traceability and visibility
  - Thorough asset inventory
  - Network segmentation

USE CASE

Take a look at how Evolving Solutions has helped clients deploy effective modern networking strategies:

CLIENT:

Global logistics company

CHALLENGE:

Protect mission-critical assets with east-to-west network segmentation in their data centers

HOW WE HELPED:

- Leveraged existing network and network security technologies and seamlessly inserted segmentation into their data center environments
- Brought in experienced, certified subject matter experts to oversee Cisco ACI optimizations along with next-gen firewalls (NGFW)

RESULT:

Utilized existing technology investments to drive cost efficiencies. Approach ensured no business downtime. Most protected assets are now segmented and have closer monitoring for threat detection.

Multicloud-Enabled and Software-Defined

An organization's network is the critical connector among applications, which may reside in private or public data centers. Users require the best experience possible when connecting to applications regardless of where that application is hosted. The challenge is to build scalable, cost-efficient networks with automated centralized management with consistent visibility into network security, health, and performance, while providing the best user experience possible.

To meet those expectations and business requirements, applications require a high availability (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 multicloud world.

USE CASE

CLIENT:

Global manufacturer

CHALLENGE:

Provide a better employee experience when connecting to SaaS applications whether the user was on prem or remote

HOW WE HELPED:

- Migrated legacy WAN infrastructure to a modern SD-WAN architecture
- Introduced SASE-related security that allows traffic to be secure quickly and efficiently

RESULT:

Increased employee productivity and satisfaction, particularly related to critical web conferencing activities and SaaS applications

Automation, APIs, and Closing Organization Silos

An automated, API-driven approach ensures that new technology can be acquired, configured, deployed, consumed, maintained, and sunset with minimal disruption.

Automation offers several benefits. It can work to improve security policies by making standards repeatable and consistent for existing and future use. Automation also reduces time spent on complex, manual tasks—removing commonly faced obstacles for networking teams. Rather than manually addressing issues, the network team can use code, APIs, and automation to troubleshoot without interfering with other processes.

While some solutions boast network automation out-of-the-box, true automation requires comprehensive strategic planning. Network teams should focus on enabling agility within their organization's network and collaborate with their DevOps and cloud peers to unlock the power of modern APIs in software-defined networks.

To allow for this collaboration, it is critical to identify and close the gaps between disparate teams that oversee the data center, applications, public cloud, monitoring, networking, and security. Doing so helps an organization achieve end-to-end network visibility.

In other words, when networking has a seat at the table, an organization is not just solving issues as they occur. Instead, they are working together to anticipate issues before they arise.

To get started, technology teams should first monitor the user experience (UX). Teams can proactively 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 examined closely for the health of entire network infrastructure.

If guard rails surrounding network standards, frameworks, and templates are in place, users can realize the benefits of automation skillsets, consistency, repeatability, and security.

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

End-to-End Security

While the term "Zero Trust" is commonly used in the security space, it can often overshadow the different components of your strategy that must work together—including consistent policies, access controls, monitoring, traceability, visibility, workload segmentation, and more. Yes—your organization should adopt a Zero Trust approach—but it is important not to lose sight of the individual elements within your security strategy.

For a fully locked-down modern network, your security strategy should include:

- Consistent, strong security policies: Security has become increasingly complex—and the need for consistent, strong security policies has become more pressing to keep track of various environments. An effective, end-to-end strategy starts with maintaining consistency across security policies. This makes everything easier from an operational perspective while lowering your organization's risk profile.

- Effective access controls: Complex security means that there are several tools that may cross different realms in your modern network. It is important to have policies and controls surrounding each tool. Access controls directly impact who can operate and act on each tool or product.

- Constant monitoring: Everything—from the firewall to your organization's internal components to incoming traffic must be monitored. The internet has become the new medium of how people are connecting securely to either private applications or private services. Because monitoring the internet can be a daunting task, it often leads to a lack of accountability when it comes to who is responsible for resolving an issue. These connections are crucial in getting the job done—but the key here is making sure they happen securely with consistent monitoring. It requires a big picture view when thinking about security and how everything connects. Automating security helps enable constant monitoring as well.

- Complete traceability and visibility: You must have seamless traceability from the controls to the policy of the tools that implement the policy and beyond. Unfortunately, this does not always happen—and when it does, it can be fragmented. Focusing on traceability creates an ideal environment in which you can quickly trace issues down the stack. Similarly, network managers must have complete visibility into the security patterns of users for logging, encrypting users' connectivity and stopping potential outbreaks.

- Thorough asset inventory: Taking full inventory of what is connected to your network can be incredibly effective in enhancing your organization's security strategy.

- Network segmentation: In traditional networking, there are large zones with hundreds, if not thousands, of endpoints. With increasing instances of ransomware attacks, the risk of one of these zones becoming infected (and then infecting other mission-critical zones) continues to rise. Network segmentation—categorizing different components to deliver more granular security—can help combat these risks.

By including each of these elements, you can develop an effective security strategy that works to stop potential outbreaks, reduce risk, and avoid the exponential costs associated with security breaches.

Overcoming Common Modern Networking Challenges

There are some common challenges may arise as you work to implement your own modern networking strategy. Anticipating these challenges will be key for your organization to navigate them effectively.

A NEW CLOUD-CONNECTED PARADIGM

Some organizations are not fully prepared for the new cloud-connected modern networking paradigm and are left focusing on the business of private connectivity. Ad hoc delivery models are no longer supportable from a scalability or operational standpoint, nor are they cost effective. Accepting a cloud-connectivity paradigm and designing a modern networking strategy around it is key in overcoming this pitfall.

WEIGH THE COSTS

How you network multicloud for HA and DR has a direct cost impact—meaning the mechanism chosen to provide resilience influences cost. Moving data around is simpler in a private data center, but once you get to the cloud, moving data costs organizations money. Despite the benefits of a cloud-connected strategy, these costs often overshadow conversations.

Similarly, adopting new platforms and keeping up with the latest innovations can drive value—especially when it comes to automating what once were manual, complex, time-consuming tasks. However, organizations deploying automation often focus too heavily on the up-front price tag.

When considering cloud adoption and automation, you need to account for cost differences compared to what a traditional network might have looked like. Examine the long-term cost savings, rather than the up-front cost. What kind of time can you save? What obstacles are you removing by deploying these strategies?

HAVING A SEAT AT THE TABLE

When moving services and implementing modern networking strategies, it is crucial that the network team have a seat at the table throughout (and leading up to) the planning process. Unfortunately, many organizations overlook the importance of this step, leaving disparate silos across departments.

Closing these gaps enables your organization to develop—and evangelize—an effective modern networking strategy that encompasses agility and cost savings. Collaboration between the network team and teams overseeing the data center, applications, public cloud, monitoring, security, and more enables strategic and proactive forethought.

USE CASE

CLIENT:

Global manufacturer

CHALLENGE:

The client needed to secure their operational technology (OT) environment and ensure they met stated business goals to reducing operational risk

HOW WE HELPED:

- Implemented security segmentation measures in the client's data center, WAN and OT
- Set up "Zero Trust" architecture to help protect the vulnerable elements

RESULT:

Reduced threat risk by more than 50% for client's OT network

7 Steps to Modern Networking

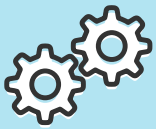
Deploying a modern networking strategy is an all-encompassing journey. Here are seven steps to get you started:

1. Develop a software-defined network adoption roadmap to support multicloud solutions
2. Assess your existing network and end-user security posture and policies to evaluate their effectiveness in a multicloud environment
3. Ensure traceability, consistency and visibility across security policies
4. Evaluate inventory across your network, and take note of what is connected to what
5. Prioritize API-driven software-defined capabilities when considering new infrastructure solutions and implement those capabilities gradually in support of initiatives
6. Close the gaps between IT and network teams to enable a proactive approach to modern networking strategy
7. Consider business benefits, long-term cost savings and cost differences compared to what a traditional network might have looked like when evaluating and advocating for your modern networking plan

Modern Networking Benefits at a Glance

An automated, cloud-enabled, secure modern networking strategy can:

Increase business agility



Streamline operations

Reduce risk of a breach

Remove obstacles to enable cross-departmental collaboration

Unlock cost and time savings

We're here to help your organization take a more proactive approach to observability.

Let's get to work.

 ESI-031522-X102