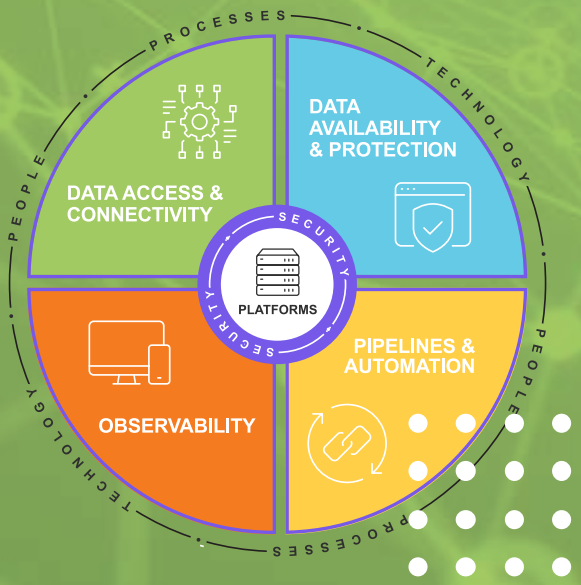
EVOLVING SOLUTIONS

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.

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 (for example, Azure AD, Okta, and others) and network identity platforms (ClearPass, Ordr, Medigate, 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

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,

Case Study

Multinational Chemical Company

CHALLENGE:

In preparation of future expansion, the IT organization identified that its existing network infrastructure had limitations in scalability, flexibility, and integration. Our client needed an adaptive plan to ensure seamless connectivity, robust performance, and the ability to scale rapidly in line with the organization's growth trajectory.

HOW WE HELPED:

Evolving Solutions undertook a Workshop with the client to develop a framework that combined a deep understanding of its current network architecture and future goals. This involved:

- Working collaboratively with the client to assess the existing network infrastructure and identify potential bottlenecks and future scalability requirements.
- Developing a custom network design that will support anticipated business growth and enable flexible upgrades in both speed and capacity.
- Incorporating adaptable hardware and management tools that enable seamless integration with existing performance hubs without interruption to day-to-day operations.

RESULT:

The updated network infrastructure framework will allow the client to enhance adaptability and operational efficiency across regional and cloud-connected hubs while providing the scalability and reliability needed to support future technology initiatives and business growth.

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.

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.

According to IDC, "50% of CIOs will accelerate robotization, automation and augmentation, 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.

Implementing Zero Trust

Implementing a successful zero trust architecture is not easy, which is why many organizations struggle to get it right.

Zero trust starts with identity and access management (IAM) — having a good handle on how your identities are set up and how you want to give access. Some organizations that are moving to the cloud may have multiple identity sources, which is not recommended. IAM needs to be centralized to ensure consistency across clouds and on-premise.

Zero trust also requires network connectivity assessments that can help network administrators find opportunities to limit the "blast radius" of an unfortunate event. To do that, it is crucial to have standards for communication between applications so that they can only connect with the data and applications they need to work. On top of that, you can add cloud security posture management (CSPM) to automatically monitor the security of application communication.

When implementing zero trust, it is best to settle on a standardized framework that can be applied across multiple cloud providers, such as a structure where you have a centralized tool set and automation to deploy network configurations consistently across environments. If your organization is already using this approach on-premise, we recommend using the same vendor for cloud configuration management. It is more secure and provides better visibility, which is important for securing environments through zero trust.

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.

The Role of AI in Modern Networking

As networks grow increasingly complex and distributed, traditional approaches to management, monitoring, and optimization struggle to keep pace. AI is emerging as a transformative force in modern networking, enabling organizations to tackle challenges that were previously insurmountable. By automating routine tasks, enhancing visibility, and providing actionable insights, AI is reshaping how networks operate, ensuring they are agile, secure, and resilient.

AI for Dynamic Risk Assessment

Assessing risk in a hybrid cloud environment is difficult at best using manual processes. Emerging AI tools are now helping network administrators assess risk continuously in the background by automating threat detection, network monitoring, and security policy enforcement. AI can be used to continuously evaluate the risk levels of systems, devices, and users, and adapt security policies in real time using behavioral analytics to detect unusual behavior across a plethora of distributed systems — behaviors that are difficult for people to identify.

Case Study

National Specialty Healthcare Payer

CHALLENGE:

Our client needed to integrate IT systems following an acquisition. They required additional compute and storage capacity to manage increased workloads while ensuring compatibility with existing systems and minimizing disruption.

HOW WE HELPED:

The Evolving Solutions team collaborated with the client to deliver an infrastructure update tailored to their integration needs. Key steps included:

- Providing additional UCS resources to address increased demands from the acquisition.
- Configuring and testing the new infrastructure to ensure compatibility with existing systems.
- Supporting the client's team in deploying and stabilizing the new environment, allowing them to focus on application migrations.

RESULT:

The client's refreshed and expanded UCS environment was fully operational within three months. The updated infrastructure provided the compute and storage capacity necessary to integrate the acquired company's IT systems. Additionally, it extended the lifespan of existing systems while positioning the organization for future growth.

Consistent Security Policy Enforcement

AI can help meet the challenge of consistently applying security policies across the organization's IT estate. Emerging AI tools can automatically perform dynamic audits and risk assessments, making it easier to monitor and enforce security policies in real-time. AI can continuously audit based on different users and groups of users, evaluating what data and information they have access to or do not have access to, with the ability to easily report on that. AI can even generate the security tests it should run.

Many organizations are attempting to enforce security policies across disparate cloud service providers using multiple unique cloud-native toolsets, which leads to inconsistencies in applying access control policies for users and devices, and/or application to application.

This is a good reason to consider one-vendor solutions where integrations and centralized policy management are already in place, giving administrators a consistent method to enforce security policies across users, as well as applications that share information.

If a one-vendor solution is not practical, organizations can create their own centralized security policy manager through systems integration. These integrations tend to be complex and need to be well thought out. Organizations also need the right skill sets to execute integrations. Sometimes projects like this are best handled by a trusted partner.

AI for Incident Response

AI is also being used to automate incident response for lower-risk events, such as users logging in from unusual locations. More intrusive events should be investigated by security analysts based on system alerts. In these cases, AI can recommend actions that security analysts can approve or reject. The most common way to automate incident response is through the security, orchestration, automation, and response (SOAR) framework, which gathers data from various detection tools to identify anomalies and automate responses for those tools.

Case Study

Private Meat Production & Distribution Company

CHALLENGE:

Our client needed to establish reliable and scalable connectivity from multiple business locations to Azure, with the ability to easily integrate additional locations as the business expanded. It was essential to ensure seamless network segmentation and robust performance was essential.

HOW WE HELPED:

The Evolving Solutions Network team worked with the client to design and implement a scalable solution tailored to their growing network needs. Our approach included:

- Delivering a comprehensive end-to-end solution with built-in redundancy and scalability, ensuring future expansion could be easily supported.
- Developing a detailed design and migration plan to implement the necessary Azure networking changes and ensure proper network segmentation and seamless integration.
- Deploying Cisco Meraki SD-WAN virtual appliances within Azure, utilizing Azure Route Server, BGP routing, Azure Firewall, and other native Azure networking features to ensure reliable, secure connectivity.

RESULT:

The existing Azure environment was successfully transitioned into a hub-and-spoke topology, with SD-WAN and Azure Firewall integrated into the central hub. This solution provides redundant connectivity to business locations, offering enhanced visibility and strong network segmentation. As additional locations are deployed in the future, they will seamlessly integrate with Azure via Cisco Meraki SD-WAN. Similarly, as workloads expand within Azure, they can be easily segmented or isolated to meet evolving business needs.

AI for Self-Optimizing Networks

AI is also being used to create self-optimizing networks that dynamically adjust network configurations to reduce latency, improve reliability, and improve the user experience. For example, if there is a spike in Wi-Fi congestion, AI can dynamically change the RF profile to accommodate the traffic. In addition, AI is being used for predictive network maintenance to anticipate hardware failures and make recommendations, such as upgrade code to avoid a bug in a network appliance or automatically write a return authorization to replace a failed component.

Overcoming Common Modern Networking Challenges

There are some common challenges that 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.

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 and consider how AI impacts your ability to run your network
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

Meet the Demands of Today and the Future

To meet the demands of business growth and to keep data, users, and endpoints protected, network teams need to shift to a centralized, coordinated approach to administration in a software-defined environment where change can be implemented quickly using automation. With end-to-end visibility and security, network teams can help ensure that networks can handle the connectivity and performance needs of today and the future.

EVOLVING SOLUTIONS

We're here to help you take a more proactive approach to networking.

Let's get to work.

 ESI-010325-X105