kyndryl / CLOUDFLARE

WHITEPAPER

The Need for Network and Security Convergence

Contents

Evolution of the Network

How it "used to be" is how it still is for many organizations. Networks were built to connect point A to point B in a very controlled, static, hardware-centric way. And networks were responsible for the protective barrier, or moat, that surrounds the business, containing its infrastructure. Maybe there were branch sites and multiple data centers, but you fully owned and controlled the infrastructure and the point-to-point connectivity.

Three major trends have disrupted this simplistic network architecture.

1. Adoption of cloud for compute and application hosting
2. Remote and roaming users working from anywhere
3. New data architectures with information residing in data center, on mobile devices, tied to SaaS services, in the cloud

As a result, the traditional perimeter has dissolved. But many parts of the traditional network are still in place for many organizations along with new connectivity services and tools required to connect remote users and clouds, creating a patchwork network that's hard to manage and can't support the modern pace of a digital business.

Network Challenges

Apps are developed more quickly, but time-to-market and agility are hindered by slow network change to accommodate

Teams are entrenched in organizational and technical silos that made sense before, but now hold back needed change

The traditional network cannot act as an effective policy enforcement agent

Organic evolution of network technologies has maybe solved immediate problems but with point solutions bolted on, new interoperability issues emerge, complexity to manage.

The network was never designed to be intelligent. It was a way to connect site to site, server to server, device to device. Some evolution has happened with software-defined and abstracting away from the hardware layer to make change easier and things like micro-segmentation and SD-WAN possible, but the journey is early stages for most organizations and should be more intertwined and supportive of security goals.

State of Security and Its Challenges

In parallel, the job of security has also grown in complexity. In addition to the infusion of cloud, hybrid workforces, and distributed data and apps expanding the attack surface exponentially and eroding visibility and control, cyber threats have grown in volume, velocity, and sophistication.

The common response to threats that pop up is the addition of a new tool that focuses on that particular problem. This "best-of-breed" approach may solve immediate issues, but creates complexity and technical debt that compounds over time. Security has evolved into a very tool laden, noisy job. Expertise is spent understanding and wielding the tens of tools in the arsenal and filtering through scattered, unprioritized alerts rather than instituting holistic strategies and frameworks to intelligently address potential threats and ensure rapid recovery.

Add to this the pressure of compliance and new levels of rigor required to prove cyber hygiene and recoverability for executive-level accountability, complex audit responses, and cyber insurance requirements.

The Vision: Network and Security Convergence

The state of networking is a combination of legacy on-premises network, pockets of MPLS, connected remote branches, and customized connectivity through native tooling to each cloud. What's needed is a place where all these things can come together and create a paradigm shift of super connectivity with security. Because it's not just about where a request is coming from, but who it's coming from.

Zero Trust and Security Frameworks

Zero trust is a paradigm shift in how you view the role of the network. In a traditional "moat" network, the guard is at the door, but once granted access, you are free to roam the castle unchecked. In a zero trust architecture, the default assumption is users, devices, and apps shouldn't have access unless proven otherwise. The assumption is a breach has already happened and every request could come from a bad actor. This flip in thinking empowers teams to architect a secure network that spans data center to cloud to edge to roaming devices and users and can include components you don't own or have control over. It's fair to say zero trust is the only approach that allows you to expand your network to the cloud and edge safely.

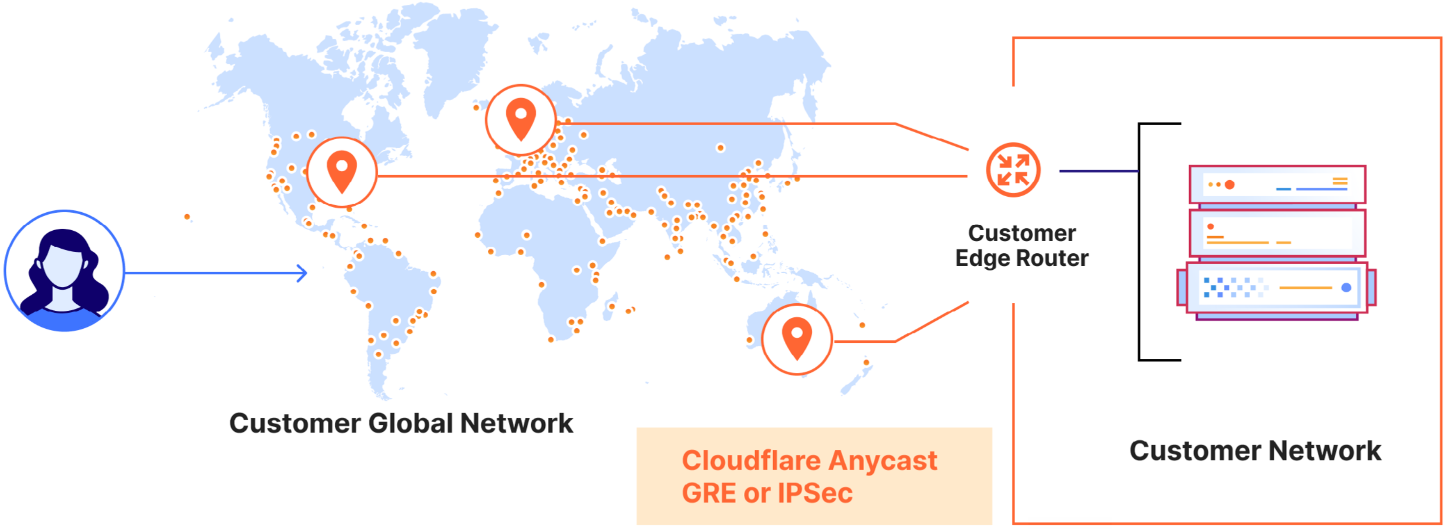
Complying with security frameworks, such as NIST, complements zero trust efforts and can provide even more rigor for a robust, holistic security strategy.

The Role of Anycast Routing

Instrumental to this paradigm shift is enforcing permissions at the closest point to where traffic enters your “big connectivity cloud”—and that function is enabled by **anycast routing**. Anycast routing allows for an overlay network based on a single IP. Remote users can connect to the overlay network entry point closest to them, and internal anycast routing then chooses the fastest or prioritized route to minimize latency from the network edge to the data center or cloud resources. The result is simplified, identity-based policies, scalability, built-in load balancing, and cross-cloud connectivity.

Anycast is a network addressing and routing method in which incoming requests can be routed to a variety of different locations or nodes.

Also with anycast routing, you have built-in high availability and resiliency for applications through intelligent routing and provide more resilience in the face of high traffic volume, network congestion, or DDoS attacks. The distributed and morphic nature of anycast networks make it naturally harder for DDoS and other automated attacks to be effective.



Network and Security Converge with Cloud-Based Platforms

Cloud launched a new era in applications, allowing for extreme development acceleration. Weeks and months-long procurement cycles were replaced with cloud “taps” ready to turn on resources when needed to rapidly develop, test, and deploy applications. While the developer world has been revolutionized, the network and security domains are now feeling the pressure to modernize and enable more agility.

By consolidating toolsets and moving into a single platform, you can create an on-demand, more cloud-like experience with increased visibility and new opportunities for correlation and advanced analytics, all of which drive perspectives and uncover problems you haven’t anticipated or identified yet. You’ll reduce the overall noise for SOC teams and enable better response to true incidents rather than chase “ghosts” in the system.

Now when a new threat emerges, the automatic response should not be to acquire another specialized tool. You want to ensure that new tools are absolutely necessary and can plug into your new platform ecosystem:

1

Evaluate what’s changed, whether it’s a new threat, new vulnerability, or new vector you can be attacked from.

2

Take the time to understand that threat and make sure you’re considering tools that effectively address that.

3

Make sure you’ve appropriately categorized the new threat that’s shown up in the system. Is it a zero-day threat? Do you have a week to patch? What’s the true level of the vulnerability and are your tools set up to accommodate? Can you simply patch systems or do you really need a new tool?

4

Make sure you’ve appropriately categorized the new threat that’s shown up in the system. Is it a zero-day threat? Do you have a week to patch? What’s the true level of the vulnerability and are your tools set up to accommodate? Can you simply patch systems or do you really need a new tool?

Falling short or struggling with any one of these steps can be an indicator you need to take a look at your landscape and understand if there are vulnerabilities in your architecture—and that’s a bigger conversation to have with cross-functional teams.

Following these steps can help avoid new tool sprawl and technical debt that creates complexity, hinders visibility, and impacts security posture.

The Culture Shift

There is no switch to flip to achieve network and security convergence. It's a transformation journey. And like all journeys that take time, you need stakeholder buy-in, a path to quick wins to show ROI, and a roadmap for success. But teams are stuck in fire-fighting mode and don't have the bandwidth to drive change. They may not also have the perspective to bring about the paradigm shift needed to approach networking and security differently. A third-party can help set that North Star for your vision, create the roadmap, identify quick wins and milestones, and inform the ongoing journey based on best practices and experience helping other businesses like yours. They can help address not only the technology decisions, but the people and processes. This includes adjusting or elevating roles and redirecting resources to more strategic projects that drive business outcomes.

Business Oriented KPIs

Rather than solely measuring success by metrics such as network uptime, consider adding more business oriented KPIs to better align with agility and market goals.

- Time to acquire and integrate a company
- Time to onboard a new employee
- Time to launch a new application
- Time to launch a new digital channel
- 100% avoiding news-worthy cyber events
- Ability to limit threat damage: speed to threat detection (MTTD), containment (MTTC), and recovery (MTTR)
- Speed and cadence for patch updates
- Compliance with industry frameworks (such as NIST)

Cloudflare and Kyndryl for Managed Network Transformation Services

The expansive IT advisory services Kyndryl, plus combined cloud networking and network security through Cloudflare solutions, helps organizations overcome technological barriers for a seamless digital transformation. With our collaboration, we can guide customers through their end-to-end network modernization journeys which can include Cloud-Centric WAN and Cloudflare Zero Trust offerings delivered by Kyndryl.

Together, Cloudflare and Kyndryl help businesses:

Streamline multi-cloud and direct-to-Internet strategy and transition networks in confidence.
Enterprises have moved data to the cloud and use SaaS applications, but are leveraging hardware as their network. Cloudflare and Kyndryl have teamed up to deliver network services to the enterprise market. Cloudflare is the technology platform and Kyndryl is the services provider that guides customers through this journey.

Reduce spend on private network links and appliances while saving IT teams from manual work.
We provide enterprises with leading networking and edge security capabilities needed for flexible work environments, including reduced technical debt and traditional architecture. Kyndryl advises and assists in managing the IT infrastructure as organizations evolve their networks and transfer workloads into Cloudflare's platform.

Accelerate digital maturity and network modernization.
Flexible cloud networking expertise with managed Cloud-Centric WAN enables networks to respond to evolving IT needs and stay equipped for what's ahead.

Extend network security to offices and data centers by replacing traditional WAN.
Complete enterprise cybersecurity tackles risks and attacks from every location and vector. This includes your WAN. Managed WAN allows organizations to convert all their resources to cloud-native solutions and retire expensive traditional hardware.

Learn More

To learn more about the Cloudflare and Kyndryl partnership, please visit cloudflare.com or kyndryl.com.

1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com