

The Network Has Become a Business Platform

It's Time We Started Treating It Like One



By Bhavin Barbhaya

*Enterprise Networking
Practice Head, Black Box*



India perspective:

Why secure, autonomous, consumption-based networking is becoming a business priority, and how Black Box and Nile bring the model to life.



A Personal Observation

One of the privileges of my role is the opportunity to work with organizations across a remarkably diverse range of industries and markets. In India, whether I am speaking with CIOs in Mumbai and Bengaluru, technology leaders in financial services, manufacturers digitizing their operations, or enterprises scaling across multiple cities and locations, the conversations are strikingly consistent.

They rarely begin with routers, switches, or the latest networking specifications. Instead, leaders are asking much bigger, strategic questions:

- How do we support AI without creating more operational complexity?
- How do we enable business growth without continually driving up IT costs?
- How do we strengthen cyber resilience when users, devices, and threats keep multiplying?
- How do we give our IT teams the capacity to innovate instead of simply keeping the network running?

Those conversations point to a fundamental change. For years, the network was treated primarily as infrastructure. Today, it is one of the most critical business platforms an organization owns. It is also one of the most important foundations for growth, security, resilience, and innovation.

What's Changing in India?

Across India, AI is moving from experimentation into production. Employees expect seamless digital experiences wherever they work. Customers expect always-on services. Enterprises are adding branches, offices, plants, campuses, cloud environments, and connected devices at greater speed. The network must keep pace with all of it.

At the same time, boards and business leaders are asking tougher questions about cyber risk, operational resilience, technology costs, and return on investment. These challenges are deeply connected. They all depend on a network that is secure, scalable, continuously available, and ready to adapt without another disruptive infrastructure cycle.

Unfortunately, many organizations are still trying to meet tomorrow's expectations with yesterday's network operating model.

The Network Is Now a Business and Security Issue

A decade ago, networking conversations rarely extended beyond the IT department. Today, they are part of discussions with CEOs, CFOs, COOs, CISOs, and boards because network performance directly influences strategic priorities.

For Indian enterprises, the network affects how quickly a new branch, plant, campus, or customer location can come online. It shapes employee productivity, customer experience, application performance, and business continuity. It also determines how effectively the organization can apply security policies across a growing number of users and devices.

In the AI era, network performance becomes business performance. AI models and digital applications can deliver value only at the speed, resilience, and responsiveness of the network connecting users, data, applications, and distributed locations. A network that is difficult to scale, secure, or operate will eventually become a constraint on business ambition.

That is why leadership teams need to stop viewing the network as back-end infrastructure and start treating it as a core business and security capability.

Where Organizations Get Stuck

Technology itself is rarely the only problem. Most organizations have access to capable networking hardware and software. The real challenge is the operating model around it.

Too much time is still spent managing hardware lifecycles, coordinating multiple suppliers, maintaining complex VLAN and network-access-control environments, responding to incidents, and planning disruptive refreshes. In large, distributed Indian environments, that burden grows quickly.

Traditional security approaches can add another layer of complexity. As more users, devices, and locations connect, policies become harder to manage consistently and a compromised device can create wider exposure across the network.

Every hour an experienced engineer spends maintaining legacy infrastructure is an hour not spent enabling AI, improving customer experiences, strengthening security, or delivering new digital services. That is becoming an increasingly expensive trade-off.

A Better Way to Measure Network Success

When I meet customers, I encourage them to judge their network against four business-focused questions:



Is it helping the business grow?

Can you bring new branches, offices, plants, campuses, and digital services online quickly? Can the network adapt to acquisitions, new applications, or changing capacity needs without months of complex work?



Is it optimizing investment?

Can you reduce unpredictable capital spending, avoid disruptive refresh cycles, improve cost visibility, and consume networking in line with business requirements?



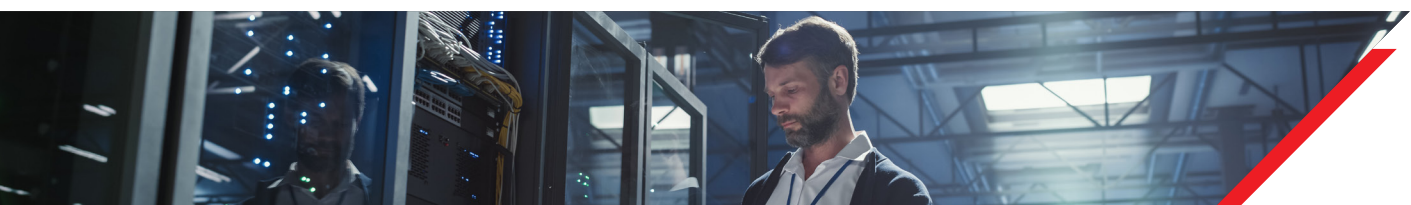
Is it protecting the business?

Can the network enforce security consistently at the user and device level? Can it help limit lateral movement and reduce the potential impact of a compromised endpoint?



Is it freeing people to innovate?

Are skilled IT teams focused on strategic initiatives, or are they consumed by monitoring, troubleshooting, supplier coordination, and routine network operations?



Why Secure Network as a Service, and Why Now?

This is why interest in Network as a Service is growing among organizations in India. The value is not limited to replacing capital expenditure with operating expenditure. The bigger opportunity is to change how the network is secured, operated, and continuously modernized.

A secure NaaS model brings infrastructure, software, security, lifecycle management, and ongoing operations together as a service. Instead of managing separate technologies and refresh cycles, organizations consume a defined networking outcome with clearer accountability for performance and support.

The strongest models also embed security and automation into the network itself. Native identity-based controls and device-level isolation can help contain threats and reduce dependence on complex legacy segmentation. AI-driven monitoring, predictive analytics, and automated remediation can identify and resolve common issues faster, often before users are affected.

The result is not simply a more modern network. It is an operating model designed to provide greater resilience, predictable consumption, stronger security, and more capacity for IT teams to focus on business priorities.

What Black Box and Nile Bring Together

For India, Black Box is bringing this model to market through Secure Network as a Service powered by Nile.

Nile provides a cloud-native Secure NaaS platform with identity embedded into the network fabric, Segment-of-One isolation, autonomous operations, and optional, financially backed performance guarantees. These capabilities are designed to simplify access control, help limit lateral movement, reduce operational complexity, and deliver a continuously modernized network through a utility-based model.

Black Box brings the enterprise integration and service capabilities required to turn that platform into a business outcome. Our teams assess the existing environment, design the target architecture, manage deployment and migration, integrate the network into the broader enterprise landscape, and provide ongoing support and managed operations.

Together, Black Box and Nile give organizations one accountable path from network strategy to implementation and ongoing performance. The technology is important, but the real value lies in the outcome: a secure, resilient, scalable network that evolves with the business.

Looking Ahead

The next few years will place even greater demands on enterprise networks. AI adoption will accelerate. Cyber threats will become more sophisticated. Organizations in India will expect technology to support faster expansion, distributed operations, stronger security, and lower operational overhead.

The organizations that succeed will not necessarily be those that own the newest technology. They will be the ones with an operating model that allows their technology to evolve as quickly as the business itself.

That is why I believe it is time we stopped asking whether our network is modern enough. We should ask a more important question: Is our network helping the business become what it wants to be, securely, reliably, and at the speed required?

If the answer is not a confident yes, the conversation should not begin with the next hardware refresh. It should begin with rethinking how the network is delivered, secured, and operated.

Black Box Secure Network as a Service, powered by Nile.