NETWORK TRANSFORMATION:

PRIORITIES, CHALLENGES & MEASURABLE IMPACT

Across all sectors and organisation sizes, enterprises are navigating sustained digital acceleration. The drivers are both internal and external – the need for strategic improvements and accelerated growth, as well as market competition and supply chains demanding a digital first approach, all in the face of global uncertainty and complexity.

These forces mean that the enterprise network is no longer a background utility, but a digital platform that directly influences revenue, customer experience, operational continuity, and risk exposure. As a result, network transformation has become a board-level priority.

It means network transformation is now a strategic imperative. Recent enterprise surveys show that a significant majority of IT leaders view modern networking as foundational to enabling cloud, AI, IoT, and digital experience initiatives. At the same time, network outages remain financially damaging, with large enterprises reporting that even a single major disruption can result in substantial revenue loss and productivity impact (such as Jaguar Land Rover).

In parallel, cybersecurity is a key requirement for transformation - hybrid workforces and cloud adoption have dissolved traditional perimeters, so security must now protect users, devices, data, and applications, wherever they reside.

THE CHALLENGE: FRAGMENTATION IN HYBRID NETWORKS

Most global enterprises now operate hybrid networks that combine on-premise, public cloud, SaaS and remote users and sites. However, networking and security have typically been managed as separate domains, resulting in a fragmented approach that has added complexity and structural inefficiencies:

- Multiple vendors and contracts
- Disparate management consoles
- Inconsistent security policies across regions
- Limited end-to-end visibility
- Slower troubleshooting and change management

As complexity increases, so does risk. Configuration drift, policy misalignment, and visibility gaps can create exposure – such as security policies becoming misaligned across different vendor solutions, and not enforcing necessary permission controls. Operational teams often spend significant time correlating data across tools rather than focusing on strategic improvements. With increasingly complex cyber threats, attackers often exploit multiple vulnerabilities. An inability to correlate anomalous behaviour and link IoC (Indicators of Compromise) from different alerts and signals increases the risk of a potential breach.

For CIOs balancing performance and protection, this separation between networking and security is increasingly unsustainable.

CONVERGENCE AS A STRATEGIC ENABLER

The solution to addressing the complexity and risk that arises from fragmentation is to move towards a more converged approach. More organisations are consolidating their technology stack through a move towards platforms, where unified solutions offer greater integration and fewer vendors to work with. Removing complexity and extracting more value from their technology investments, is key to delivering genuine transformation.

One of the most significant shifts in this approach is the move toward converged networking and security models, in particular with SASE (Secure Access Service Edge). This approach was designed to address the challenges of legacy networking and security architecture, and is seeing growth of 26% annually. The benefits of SASE extend beyond product features, providing IT teams with operational efficiencies, and the ability to leverage data and intelligence more effectively.

Let's look into the key advantages of a converged solution,
that deliver a stronger security posture as well as improved business outcomes.

1 Unified Insights and End-to-End Visibility

When networking and security telemetry exist in separate systems, troubleshooting becomes reactive and time-consuming. A performance issue might require investigation across multiple tools and dashboards.

Many disparate security solutions also lack key contextual insights, such as East/West traffic, while over 70% of network breaches involve lateral movement. With integrated alerts from the network, security insights in a SOC could be missing critical IoCs.

A converged model provides a single data plane and unified analytics layer, enabling:

- Real-time visibility into application performance
- Correlated network and security events
- Faster root cause analysis
- Proactive detection of anomalies

For distributed enterprises, unified insights dramatically reduce mean time to resolution (MTTR) and improve service continuity.

2 A Single, Consistent Security Policy

Hybrid environments often suffer from inconsistent policy enforcement. Branch offices may operate under different configurations. Remote access controls may not align with internal network policies.
A unified architecture enables a single, centrally managed security policy applied consistently across:

- Branch and campus locations
- Cloud environments
- Remote users
- Third-party access

This consistency reduces the risk of misconfiguration and simplifies compliance reporting. It also aligns with Zero Trust principles by ensuring that access controls and inspection policies are enforced uniformly, regardless of user location.

3 Reduced Complexity and Operational Overhead

Operational complexity carries both direct and indirect costs. Multiple vendors mean multiple SLAs, support processes, renewal cycles, and integration challenges. Hardware-centric architectures require patching, lifecycle management, and periodic upgrades.

A simplified, converged approach reduces this sprawl by:

- Consolidating vendors and contracts
- Minimising hardware dependencies
- Centralising management and orchestration
- Standardising deployment across geographies

For mid- to large enterprises expanding into new markets or integrating acquisitions, this simplification accelerates site rollout and reduces integration friction.

FROM INFRASTRUCTURE TO BUSINESS PLATFORM

For organisations looking at SASE to support network transformation, there are key metrics they can use to measure definable business results:

- **Improved User and Customer Experience:** Through improved network performance from SASE, employees are more productive, while customers experience fewer service delays or disruptions
- **Stronger Resilience:** With built-in redundancy and failover from better connectivity, increased uptime lowers business risk
- **Lower Total Cost of Ownership:** Reducing multiple point solutions, a SASE solution also reduces time spent on troubleshooting or managing multiple dashboards
- **Clearer ROI:** Long-term savings are coupled with the ability to scale the network alongside business growth

In a business landscape defined by digital interdependence, the modern network must do more than connect locations. That's why GCX and Cato Networks partner to provide a simplified, secure, and resilient foundation capable of sustaining growth, innovation, and trust across every geography in which the enterprise operates.

Together, we enable enterprises to:

- Simplify complex global network and security infrastructures
- Reduce security risks associated with traditional point solutions
- Improve uptime and application performance for distributed workforces
- Free internal IT resources to focus on strategic initiatives rather than point-product firefighting
- Align with modern digital business requirements across verticals, including retail, hospitality, manufacturing, automotive, and legal services

In a world where digital transformation is a competitive imperative, the partnership between GCX and Cato Networks offers a practical, secure, and simplified blueprint for success.