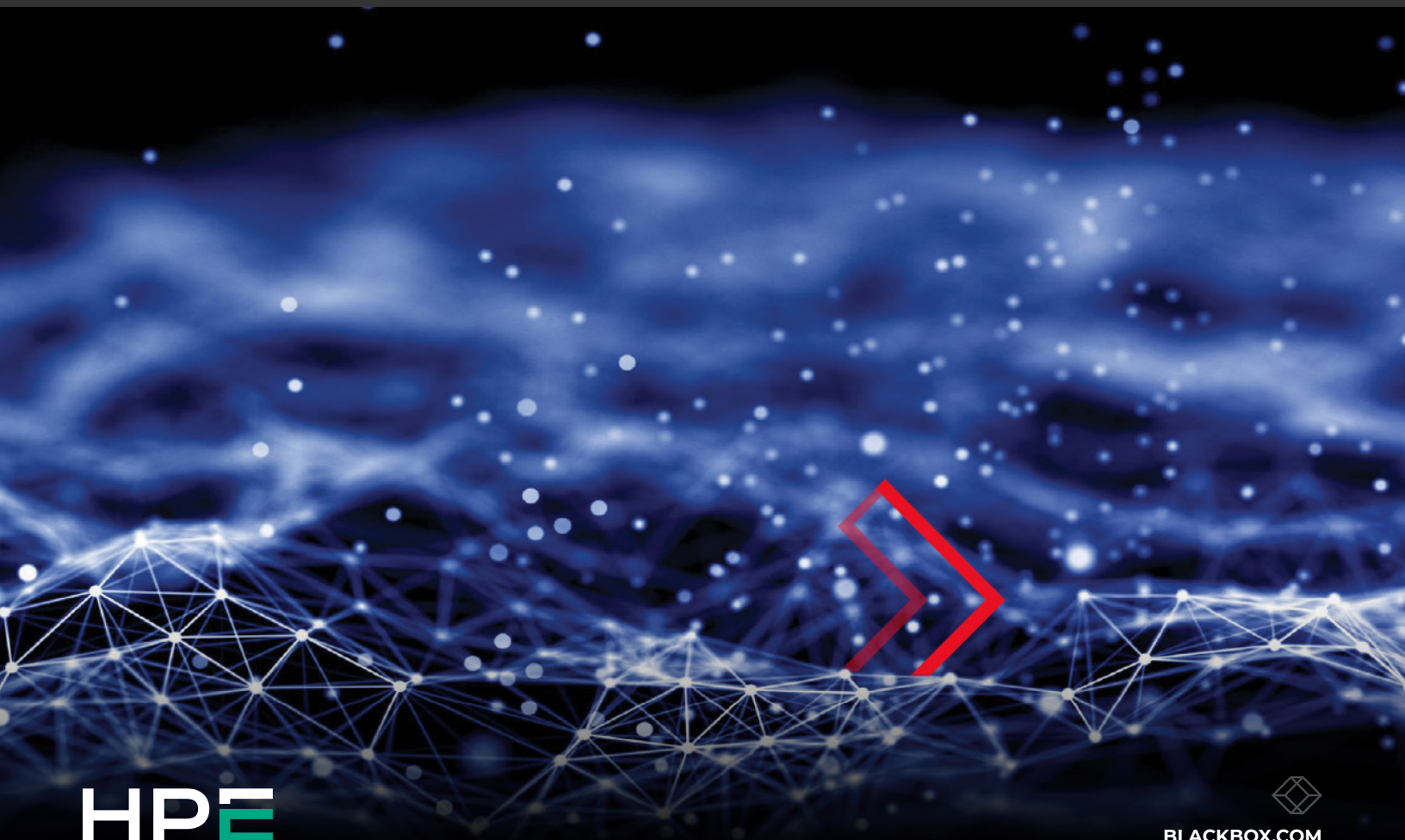
BLACK BOX®

Why Self-Driving Networks **Aren't Science Fiction**



HPE

BLACKBOX.COM

TABLE OF CONTENTS

INTRODUCTION

Self-Driving Networks Are Already Here (and So Are the Costs of Not Adopting)

Businesses across Australia and New Zealand (ANZ) are part of a broader global tension between legacy network capacity and accelerating digital demand.

Virtualised networks, AI-automated processes,complex cloud architectures, work from anywhere expectations and a greater demand for seamless connectivity are now the norm. While we're looking forward to automated AI networking, where security, adaptability and scale are standard, enterprise networks regionally are slow to adapt. The resulting challenges manifest as digital project delays, rising costs and inefficient resource allocation across organisations.

Self-driving network solutions systematically address these challenges, combining automation, telemetry and AI-driven decisions to optimise performance in real time - all with minimal human intervention. These solutions are the next generation of architecture that will keep ANZ enterprises productive and future-ready.

Here, we explore what self-driving networks are, why they matter for enterprises across Australia and New Zealand, and which practical solutions organisations can deploy now to move from reactive maintenance to proactive and autonomous networking.

The State of Enterprise Networks in ANZ

Cloud native access, mobile workforces and a growing demand for seamless, frictionless experiences have rewritten what businesses and end-users expect from their networks. However, existing and emerging barriers are slowing organisational capacity to adapt.

In New Zealand, while governance is strong in terms of network readiness, the people and technology required to deploy is lagging, with AI talent concentration among the weakest indicators. In Australia, where people and technology indicators are marginally stronger, the trend remains the same.

Gartner predicts that 85% of organisations heavily reliant on legacy systems will struggle to fully execute their digital strategies. This reliance on critical infrastructure nearing end of life can lead to missed opportunities, decreased productivity and increased risk during transformation projects.

For IT leaders, these signals and the realities behind them create a tension between technology needs and business priorities: should they keep investing in small fixes that buy time, or move to modern architectures that scale and optimise themselves?

So, what's causing this divide?

Modernisation Introduces Network Complexity and Visibility Challenges

Over the past decade, we have witnessed a convergence of mobile, cloud, the Internet of Things (IoT), edge computing, private 5G and now, AI. Technological evolution requires more complex and higher-volume data transfer, adding complexity and visible blind spots to enterprise networks. This is especially the case as companies transition toward hybrid and multi-cloud architectures. Notably, 86% of Australian business leaders acknowledge that their existing network infrastructure is insufficient to leverage new technologies fully.

Region-wide Skills Gaps

Both Both Australia and New Zealand have experienced sustained constraints in skilled talent availability. The latest Australian Computer Society's (ACS) Digital Pulse report estimates that an additional 230,000 tech workers will be required by 2030 to sustain the sector's continued growth. The widening regional skills gap, coupled with retention challenges, is creating pressure for organisations to secure the talent they need to engender meaningful digital transformation.

User Expectations

Users expect to work seamlessly from anywhere, reshaping how enterprises design and secure their networks. As mobility increases, users no longer need to be "inside" a physical network perimeter. They expect to move fluidly between corporate, campus, and external networks without disruption. At the same time, secure access must be ensured regardless of location. As a result, centralised corporate networks that only permit access from within the office are largely obsolete.

Further, distributed access points increase the risk of breaches, while higher volumes of video conferencing, cloud collaboration and remote logins strain existing architecture. This means more endpoints to manage, more blind spots in visibility and higher expectations for reliable connectivity, all while ensuring consistent and secure access across a fragmented workforce.

Policy Pressures

New Zealand's digital priorities emphasise heightened cybersecurity, closing the tech skills gap, accelerating technology adoption and widening digital inclusion. Meanwhile, in Australia, the focus is on cybersecurity, digital infrastructure and skills investments.

Organisations face pressure not only to modernise and meet user expectations for smart, AI-driven experiences, but also to comply with emerging regulations - particularly in cybersecurity and AI governance.

Closing these gaps requires shifting from legacy, manual and siloed networking to platforms that deliver visibility, automation and secure performance. However, with ongoing and varied pressures, technology leaders are faced with prioritisation paralysis, as many are left firefighting with little internal bandwidth to modernise.

The Value Self-Driving Networks Offer ANZ Enterprises

Self-driving networks are automated, AI-native and self-healing networking solutions that deliver value across five practical layers. For ANZ organisations, where end-user expectations and agility demands are rising, these benefits translate into measurable outcomes.

Frictionless Experience

Self-driving networks remove everyday friction for employees and other endusers. By identifying and remediating issues before they affect users, the networks deliver consistent connectivity across sites, reducing session drops and speeding up authentication. This results in fewer support interruptions and steadier app performance, offering a more frictionless experience from the ground up.

Cloud Native Access

Global advancements in connectivity technology mean that centralised corporate networks, where users operate "inside" the office, are no more fit for purpose. It's no longer just about connecting sites. Networks must now securely and consistently connect users to applications wherever they are, rather than being constrained by a traditional network edge.

Security Embedded in the Network

Traditional perimeter security doesn't work when your workforce is distributed and SaaS-heavy. To create the security, zero-trust access, and cloud integration required for this new reality, Secure Access Service Edge (SASE) must combine with:

- Self-driving networks and SD-WAN.
- Cloud security.
- Cloud Access Security Broker (CASB).
- Secure web gateways.
- Zero-trust policies.

Mobile workforces need complex policies that span cloud and on-premises environments. SASE provides centralised visibility and control without forcing traffic back through a corporate network.

Enhanced Productivity

AI-driven networking automates diagnostics and remediation, reducing time to repair, ticket volumes and skilled talent workloads. Self-driving networks have achieved 70% faster Mean Time to Resolution through automating diagnostics. Teams can run critical backups in hours, not days; meanwhile, simplified network operations and increased service reliability naturally lead to higher productive outputs. Beyond operational benefits, self-driving networks simplify threat detection and protection with a zero-trust, threat-aware network.

Additionally, network automation controls the proliferation of connected devices, offering the agility to scale. Freed from constant issue resolution, IT teams can focus on projects that drive productivity and value.

Future-Ready Foundation

At scale, the network becomes a strategic asset rather than a cost centre. Self-driving capabilities enable automatic scaling, policy consistency and rapid support for cloud, edge and IoT workloads thereby lowering technical debt and accelerating innovation. Coupled with local expertise and support, organisations gain agility, regulatory assurance and a platform that adapts as their business needs evolve.

It's not just a game of catch-up; ANZ organisations have critical opportunities to leapfrog global competitors and position themselves as future-ready.

The Cost of Staying Legacy

Holding on to legacy network infrastructure is becoming a growing liability. In fact, according to IDC predictions, Global 2000 businesses will experience two to three network outages each year due to legacy systems that significantly affect their business agility. When engineers and help desks spend disproportionate time on issue identification, troubleshooting and incident response, less bandwidth is allocated to innovation, growth and broader productivity goals.

Network downtime and service interruptions impact revenue and end-user experience, and the resulting invisible costs include higher support volumes and longer recovery windows. Further challenges include:

Increased exposure:

Siloed legacy stacks also widen the attack surface. Notably, the Australian Cyber Security Centre (ACSC) identifies that legacy network infrastructure increases security vulnerabilities as it can enable attackers to gain access to more modern systems. Furthermore, fragmented visibility and patchy telemetry weaken issue detection, increasing exposure and regulatory risk as compliance demands rise across ANZ.

Stalled innovation:

Adding capacity to old architectures often means significant upgrades or temporary workarounds that introduce vulnerability. As cloud-native workloads, AI services and IoT endpoints proliferate, legacy networks struggle to deliver the predictable performance and quality of service guarantees that modern solutions offer. Rather, they create friction for the initiatives meant to drive growth.

Inefficient resource allocation:

Legacy networks that fail to handle the workloads required to keep businesses secure, connected and innovative pose a measurable risk, including unplanned downtime, missed SLAs and delayed projects. For technical teams, the symptoms include poor visibility into network traffic, lengthy time-to-resolution, ballooning support tickets and backups that take hours instead of minutes. The outcome is wasted senior talent - a challenge further exacerbated by limited supply.

Delaying modernisation converts a one-time investment into a recurring cost. Automation and the shift toward Network-as-a-Service (NaaS) and SDN are essential pathways for businesses seeking to reduce operational overhead, tighten their security posture and utilise automated, private network connections.

Looking Ahead to the Next 3–5 Years

Moving forward, networks will likely cease to be a tool and become the control plane for digital business. Over the next three to five years, networking infrastructure will sense, decide and act autonomously to protect performance and optimise cost.

Here are the key trends to watch:

1. **Network Security and Scalability will Remain Priorities for Enterprises**

   Organisations continue to prioritise network security and scalability. From real-time AI threat detection to zero-trust architecture and securing IoT devices, adopting advanced technology is crucial to achieving scalable and secure tech foundations.

2. **The Rise of Autonomous Systems**

   Autonomous systems are transitioning from pilot projects toward practical applications. These systems are integral to a future where technology is required to be more adaptive and collaborative, learning and executing tasks autonomously.

3. **AI-powered Networking Readiness to Boost Collaboration**

   Although many companies are exploring AI's potential, expectations often fall short of the reality of implementation. Successful AI adoption will require closer collaboration between technology and business decision-makers to assess infrastructure and align expectations in a strategic direction.

4. **AI-based Attacks and Threats Emerge as a Challenge**

   While AI offers practical benefits, the associated security vulnerabilities require increasingly attentive management - particularly in light of emerging Gen-AI-based attacks. Network architecture will need water-tight security to protect data and operational processes.

5. **Intensified Regional and National Competition**

   Global competition in the critical tech realms is intensifying. This drives countries and corporations to invest in sovereign infrastructure, where self-sufficiency and localised tech development may reduce geopolitical risk.

   For ANZ businesses already playing catch-up with global counterparts, early adoption of self-driving capabilities now buys time, competitive advantage and operational simplicity later. In this sense, selfdriving networks are the start, rather than the finishing line.

Black Box + HPE Networking: The Partnership Driving Change

The collaboration between Black Box and HPE Networking delivers the self-driving network: a paradigm shift in network management that leverages AI to automate and optimise operations.

Its AI-native design transitions network management into a proactive, rather than a reactive process, continuously monitoring, learning and improving network efficiency. Based on HPE Mist, this system simplifies and automates network operations across wireless, wired and Wide Area Network (WAN) environments.

Task automation and self-healing capabilities detect and resolve issues from devices to the cloud, significantly reducing manual troubleshooting and downtime. While IT engineers and support teams gain back time to focus on innovation and growth initiatives, self-healing offers end-users a seamless network experience.

The Marvis Virtual Network Assistant utilises a conversational interface to deliver data-driven responses and recommended actions. Client-to-cloud visibility and AI-native zero-trust security provide consistent policy enforcement across the entire infrastructure.

Meet the Partners:

The partnership brings together Black Box, a global leader in system integration and managed services, and an Elite Plus HPE Networking partner, with HPE Networking's AI-native platform, HPE Mist. With a global scale, local expertise across 35+ countries and an ANZ presence spanning 20+ years, Black Box's partnership with HPE Networking supports enterprises with custom, outcomes-focused networking solutions.

Leveraging deep expertise in highly regulated industries, this partnership offers end-to-end services, from strategy, design, deployment and support, ensuring organisations achieve tangible, real-world outcomes with comprehensive network solutions.

Case Study

Transforming WAN Performance and Security through Black Box and HPE Networking Innovation

See how Black Box and HPE Networking strengthened network resilience for a leading NZ construction supplier.

Problem:

The business struggled with unreliable failover links, poor visibility into network traffic and inconsistent support from its former provider. These issues slowed productivity, causing weakened security and delayed resolution

Solution:

Black Box redesigned the WAN with AI based SD-WAN and AI driven virtual firewall. Enhancements included fibre upgrades, 4G failover, dynamic VPN and identity-based policy controls to improve visibility and security.

Outcomes:

The business gained a more reliable connectivity with faster troubleshooting and real-time visibility via HPE Mist dashboards. In the first quarter following deployment, support tickets were reduced to zero. Ultimately, the solution reduced ongoing costs and enabled a scalable, future-ready network.

Beyond Legacy: Time to Modernise is Now

Enterprises in ANZ can no longer afford to treat networking as a background utility or wait for the right time to modernise. The costs of legacy architecture are compounding, while self-driving networks are available now.

Together, Black Box and HPE Networking bring local expertise with a global footprint to deliver a proven partnership that transforms networking complexity into automated, visible and secure connectivity at scale.

Learn how Black Box and HPE Networking can help you move beyond legacy and into a future-ready network, starting now.

READY TO GET STARTED?

Visit **blackbox.com** today.

Black Box is a global leader in digital infrastructure solutions, delivering network and system integration, managed services, and technology products to Fortune 100 and top global enterprises. With a presence across the United States, Europe, India, Asia Pacific, the Middle East, and Latin America, Black Box serves businesses across financial services, technology, healthcare, retail, public services, and manufacturing.