theCUBE Research Whitepaper

Seven Keys to Building a Self-Driving Network:

Why AI-Native Operations are Becoming Foundational to the Future of Enterprise Networking

Date: May 2026 **Author:** Bob Laliberte

Executive Summary

Enterprise networks are becoming increasingly critical to business operations as organizations expand hybrid work, cloud-native applications, AI initiatives, and distributed digital experiences. At the same time, operational complexity continues to rise, placing pressure on IT teams to deliver higher levels of performance, resiliency, and security with limited operational resources.

theCUBE Research data reflects this shift clearly, with 94.6% of organizations reporting that the network is more or much more important to achieving business goals than it was two years ago. As networks evolve into platforms for business outcomes, traditional operational models built around manual processes, siloed tools, and reactive troubleshooting are becoming increasingly difficult to sustain.

This is driving growing interest in self-driving networks, AI-native networking platforms capable of continuously observing operational conditions, correlating telemetry across domains, identifying issues proactively, and autonomously recommending or executing remediation actions.

However, achieving meaningful autonomy requires more than adding AI features to existing management platforms. It depends on architectural consistency, shared operational intelligence, integrated security, and trusted automation frameworks that can operate across the distributed enterprise.

Achieving meaningful progress toward autonomous networking requires organizations to address both the operational realities driving complexity and the architectural foundations necessary to support AI-native operations at scale. HPE Networking's Seven Keys to a Self-Driving Network provide a framework for evaluating this transition, focusing on AI-Native Architecture (Not Bolt-On AI), Continuous, Experience-First Telemetry, Agentic AI That Can Observe, Decide, and Act, End-to-End Intelligence Across the Distributed Enterprise (Client to Cloud), Built-In, Policy-Driven Security, Intelligence Beyond Networking, and Human-Guided Autonomy. Together, these principles reflect the broader shift from reactive operations toward intelligent, experience-driven, and increasingly autonomous network operations.

The Network's Expanding Role in Business Outcomes

The enterprise network has evolved from a supporting utility into a critical platform for business execution. Digital transformation initiatives, AI adoption, hybrid work, edge computing, and increasingly experience-sensitive applications have elevated the network's importance well beyond traditional connectivity.

theCUBE Research data reflects this shift clearly. Nearly 95% of organizations report the network has become more important to achieving business goals over the past two years, with almost two-thirds describing it as "much more important."

SURVEY QUESTION

How important is the role of the network in your organization's ability to meet its business goals compared to two years ago?

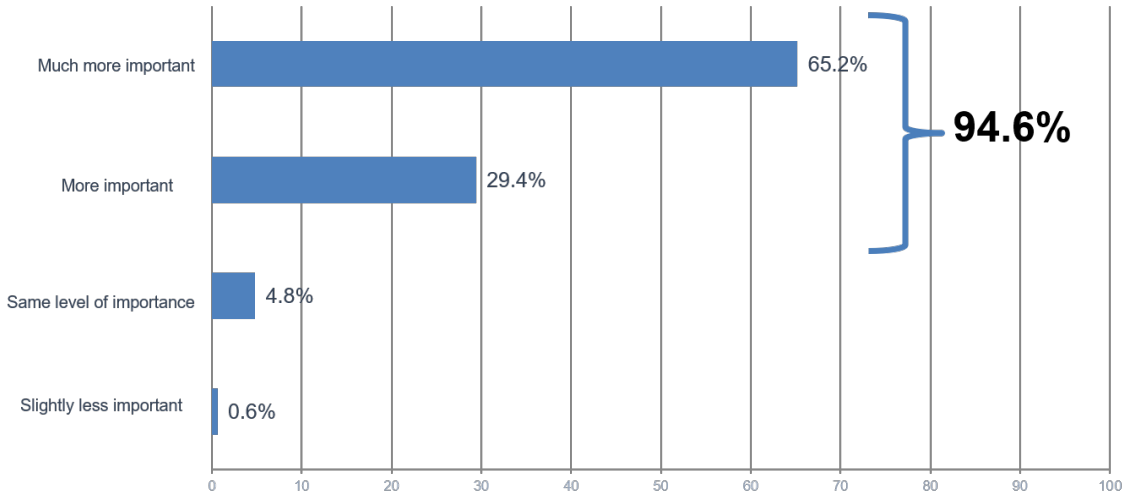

Figure 1 – The Role of the Network to Business Goals– Source: theCUBE Research

This growing dependence on the network is being accelerated by several converging trends.

Organizations are operating in increasingly distributed environments where users, applications, and data exist across campuses, branches, home offices, public clouds, edge locations, and AI infrastructure. At the same time, collaboration platforms, real-time analytics, and AI inferencing workloads are placing far greater demands on network consistency, latency, and resilience than traditional enterprise applications.

As AI becomes more deeply integrated into enterprise operations, the network is also becoming increasingly important to the secure movement of data, the orchestration of workloads, and the delivery of digital experiences. This is particularly evident in AI environments, where organizations report growing operational pressure related to traffic growth, east-west data flows, and latency-sensitive applications.

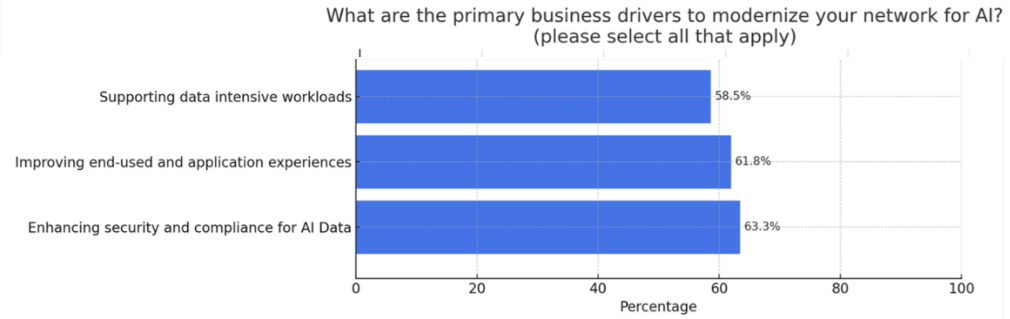

Figure 2 – Business Drivers to Modernize Network– Source: theCUBE Research

The operational challenge is that traditional networking models were not designed for this level of dynamism or scale. This is why organizations are moving beyond simple automation and exploring AI-native operational models capable of delivering continuous intelligence and autonomous operations.

Why Traditional Network Operations Are Struggling to Keep Pace

Despite years of investment in automation and network management tools, operational complexity continues to grow faster than most organizations can absorb. Enterprise networks now span private data centers, public clouds, branch locations, home offices, edge environments, and increasingly AI-enabled infrastructure, dramatically increasing operational scale and interdependency.

At the same time, AI workloads are introducing new traffic patterns and performance sensitivities that traditional operational models were not designed to manage effectively. East-west traffic growth, distributed inferencing, GPU-intensive workloads, and increasingly experience-sensitive applications require far greater operational visibility, responsiveness, and coordination across environments.

This complexity is compounded by fragmented operational models. Many organizations still manage LAN, WLAN, WAN, security, and cloud environments through disconnected tools and siloed operational teams. As a result, troubleshooting often requires manual correlation across multiple domains, slowing remediation and limiting operational agility. theCUBE Research findings continue to show that organizations struggle with fragmented visibility, operational complexity, and aligning networking infrastructure to support AI-driven operations.

While first-generation AIOps platforms have improved visibility and introduced automation into networking operations, most were not architected to support continuous intelligence or autonomous decision-making across highly distributed enterprise environments. Many continue to rely on infrastructure-centric telemetry rather than end-to-end user and application experience data, limiting their ability to prioritize issues accurately or automate remediation safely.

Organizations also face important operational and organizational challenges as they move toward self-driving networking models. Trust remains a significant factor, as most enterprises are not prepared to immediately allow AI systems to make autonomous operational changes without transparency, explainability, and governance controls. Security integration presents additional complexity, particularly in environments where networking and security operations remain operationally separate. Autonomous systems require shared telemetry, coordinated policy enforcement, and integrated intelligence across domains to operate effectively.

Finally, operational readiness and organizational culture play a critical role. Transitioning toward autonomous networking requires IT teams to evolve beyond reactive administration and increasingly focus on orchestration, governance, policy management, and AI-assisted operations.

What organizations increasingly require is not simply more automation layered onto legacy operational models, but a more fundamental shift toward AI-native operations built around shared intelligence, continuous telemetry, integrated security, and human-guided autonomy.

HPE Networking's Seven Keys to a Self-driving Network

To enable organizations to overcome those challenges and accelerate the adoption of Self-driving Networks, HPE has outlined seven key attributes to ensure success. They include:

1. AI-Native Architecture (Not Bolt-On AI)

The foundation of a self-driving network begins with architecture. AI capabilities layered onto legacy platforms often struggle to deliver the responsiveness, scalability, and operational cohesion required for autonomous operations.

AI-native architectures built around cloud-scale microservices allow intelligence, telemetry, and automation to evolve continuously rather than through infrequent platform upgrades.

This architectural approach enables:

- Continuous operational learning
- Distributed intelligence
- Real-time analytics
- Faster innovation cycles
- Operational resiliency through service isolation

HPE Networking's convergence of Aruba Networking Central and HPE Mist reflects this architectural strategy. Rather than focusing solely on feature consolidation, HPE is aligning platforms around shared microservices, common operational frameworks, and reusable intelligence services designed to support long-term autonomous operations.

This architectural consistency becomes increasingly important as enterprises pursue more autonomous and distributed operational models.

2. Continuous, Experience-First Telemetry

A self-driving network requires more than infrastructure visibility. It requires continuous telemetry that reflects actual user and application experiences across the distributed enterprise.

Traditional networking operations often relied heavily on device-centric monitoring and indirectly inferred user impact. Modern autonomous systems require richer operational context.

Experience-first telemetry focuses on:

- End-user experience

- Application performance
- Connectivity quality
- Cross-domain operational context
- Continuous validation of outcomes

This operational model enables AI systems to prioritize issues based on actual business impact rather than isolated infrastructure alerts.

HPE Networking's Large Experience Model (LEM) approach then correlates telemetry across wired, wireless, WAN, security, and cloud domains to understand how operational conditions affect user experience and application performance in real time.

As AI-sensitive applications continue to expand, this level of contextual telemetry becomes increasingly foundational to operational assurance.

3. Agentic AI That Can Observe, Decide, and Act

Many AI-driven networking platforms can generate insights or recommendations. Far fewer can execute reliable closed-loop operations.

HPE Networking's third key focuses on the evolution from advisory AI toward agentic AI systems capable of observing operational conditions, reasoning across multiple data sources, taking action, and validating outcomes autonomously.

Unlike static automation workflows, agentic AI introduces adaptive operational intelligence capable of:

- Goal-oriented behavior
- Autonomous planning and execution
- Context-aware remediation
- Continuous learning and refinement

This capability becomes particularly important in distributed environments where operational conditions can change faster than human operators can respond manually.

HPE's Marvis AI assistant and Marvis Actions capabilities illustrate this progression toward closed-loop operations by combining telemetry correlation, automated troubleshooting, remediation workflows, and continuous validation.

Importantly, explainability remains central to building trust in these systems. Organizations increasingly expect visibility into why actions are being taken and what operational impact they produce.

4. End-to-End Intelligence Across the Distributed Enterprise (Client to Cloud)

Self-driving networking cannot operate effectively within isolated operational silos. User experiences span wireless access, campus infrastructure, WAN connectivity, cloud environments, security systems, and increasingly AI-enabled applications and services.

This requires end-to-end intelligence capable of correlating telemetry, policies, and operational context across the full client-to-cloud environment.

As enterprises expand AI-driven workloads and distributed operations, the ability to maintain consistent operational visibility across domains becomes increasingly important.

HPE Networking's architectural strategy emphasizes unified operational visibility and coordinated intelligence across networking domains rather than isolated operational tooling. This shared context allows operational systems to reason holistically rather than reacting independently within individual infrastructure silos.

This becomes especially important in highly distributed environments where operational issues frequently traverse multiple infrastructure layers simultaneously.

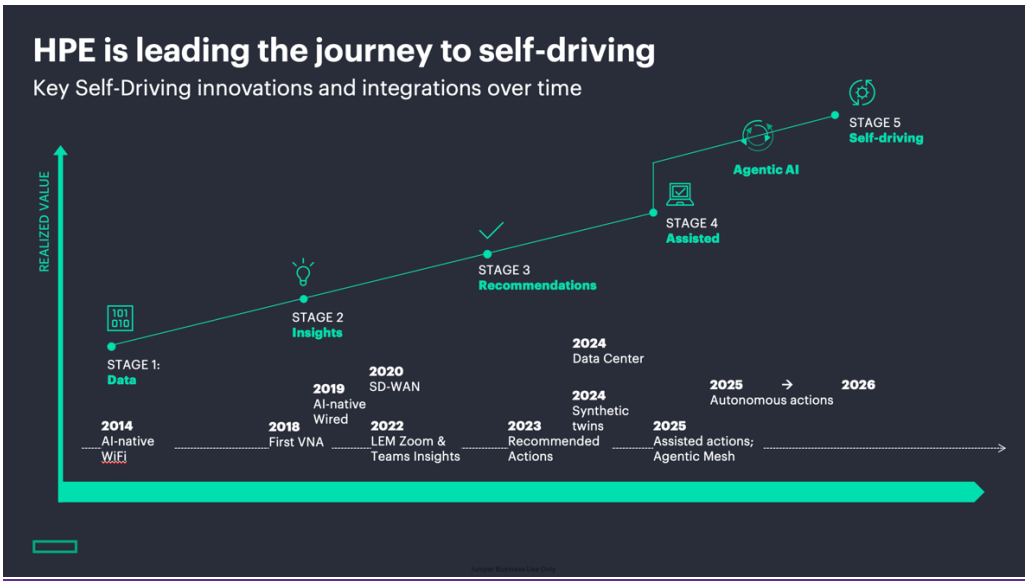

Figure 3 – HPE Self-driving Journey – Source: HPE Networking

5. Built-In, Policy-Driven Security

Security cannot function as a disconnected operational layer in autonomous environments.

A self-driving network requires security policies, visibility, and enforcement mechanisms to operate cohesively with networking intelligence.

This includes:

- Dynamic policy enforcement
- Identity-aware networking
- Integrated threat visibility
- Coordinated remediation
- Shared operational context between NetOps and SecOps

As networks become more autonomous, the ability for security decisions to move at machine speed alongside networking decisions becomes increasingly important.

HPE Networking's integration of security capabilities,including SRX firewalls, SASE, and policy orchestration,within its broader AI-native operational framework reflects this convergence of networking and security intelligence.

This integrated approach helps reduce operational friction while improving consistency and resiliency across distributed environments.

6. Intelligence Beyond Networking

The future of autonomous operations extends beyond networking infrastructure alone.

User experiences depend on interactions across:

- Applications
- Cloud services
- Compute infrastructure
- Storage systems
- Virtualization environments
- Security operations

As a result, self-driving networking increasingly requires intelligence capable of operating across broader IT domains.

HPE Networking's strategy reflects this broader vision through integrations with:

- Morpheus for cloud and application orchestration
- OpsRamp for IT operations visibility
- Security platforms
- Open agentic frameworks and standards

This extensibility allows organizations to move toward more coordinated operational intelligence across the enterprise while protecting existing investments and maintaining operational flexibility.

Long term, this evolution points toward the broader concept of a self-driving enterprise rather than isolated autonomous networking domains.

7. Human-Guided Autonomy

Perhaps most importantly, self-driving networking is not a binary operational state. It is a progression built around operational trust.

Organizations want:

- Visibility before automation

- Recommendations before remediation
- Explainability before autonomy
- Governance before full operational delegation

HPE Networking's seventh key, Human-Guided Autonomy, recognizes that autonomous operations must evolve gradually through demonstrated efficacy and operational transparency.

This progression typically begins with visibility and AI-assisted troubleshooting, followed by guided remediation, selective automation, and, where appropriate, autonomous operations.Importantly, this "time-to-comfort" model aligns closely with how enterprises are realistically approaching AI adoption more broadly.

Trust is ultimately built through measurable operational outcomes, transparency, and continuous validation rather than through automation alone.

Our ANGLE

Enterprise networks are becoming increasingly central to business operations as organizations expand AI initiatives, distributed applications, hybrid work, and experience-driven digital services. At the same time, operational complexity continues to outpace traditional management approaches built around manual processes and siloed tools.

Self-driving networking represents an important evolution toward more intelligent, adaptive, and experience-focused operations. However, achieving meaningful autonomy requires more than incremental automation. It depends on AI-native architecture, continuous telemetry, integrated security, shared operational intelligence, and trusted operational governance.

HPE Networking's Seven Keys to a Self-Driving Network provide a practical framework for organizations navigating this transition. By focusing on AI-native operations, experience-first intelligence, agentic AI, client-to-cloud visibility, built-in security, cross-domain intelligence, and human-guided autonomy, HPE is aligning its networking strategy to the operational realities enterprises increasingly face.

Ultimately, the value of self-driving networking will be measured not simply by automation itself, but by its ability to simplify operations, improve digital experiences, strengthen resiliency, and help organizations operate more effectively in increasingly distributed and AI-driven environments.