The self-driving network: Can you really trust AI to take the wheel?

A new era of autonomy

Just as cars have evolved from manual systems to computer-assisted operations to self-driving vehicles, networks are following a similar trajectory. Now, with advances in agentic AI, self-driving networks are becoming a reality. It's an exciting shift, but one that also begs the question: When the network has become more business critical than ever, can you really trust AI to take the wheel?

What are self-driving networks?

Self-driving networks are advanced, AI-native networks that can, when authorized, automatically optimize themselves with minimal to no human intervention. It's the difference between a network reacting when something breaks and one that stays alert, anticipates issues, and fixes them before anyone notices.

But self-driving networks aren't human-less networks. They don't eliminate the role of IT teams or assume full autonomy overnight. Instead, they replace manual, reactive work with predictive, autonomous operations, so your IT staff can focus on more strategic initiatives like architecture, experience, and business alignment. And the level of autonomous operations is always set by humans.

Benefits of self-driving networks include:

— **Greater efficiency and performance:** AI-driven workflow automation proactively detects and resolves issues, improving reliability and reducing downtime.

— **Improved scalability:** Automated provisioning reduces onboarding and configuration time.

— **Better security:** AI algorithms quickly identify and mitigate threats before they impact operations.

A real-world self-driving moment

A global pharmaceutical company faced a sudden surge in Wi-Fi demand when employees gathered for an unplanned all-hands meeting. Their self-driving network automatically detected a wireless spike and instantly opened more capacity, shifting devices onto 5 GHz and 6 GHz bands.

The system also detected some access points running outdated software that blocked access to 6 GHz, and automatically upgraded them, assuring full performance so the meeting could continue without disruption.

How trust is built in autonomous systems

Until recently, many people had reservations around self-driving vehicles, yet today they are a common mode of transportation in some cities. What changed? Trust built as self-driving cars became more commonplace, as people began to understand the technology behind them, and as their safety was proven over time.

In a similar way, turning your network over for AI to drive takes time. It's a process of incremental trust that requires transparency, explainability, and a continuous demonstration of safety. Breaking the journey to a self-driving network into stages is a great way to build trust in the technology and to help network teams adjust as their role changes from reactive troubleshooting to proactive strategy and implementation. Our suggested process involves five steps.
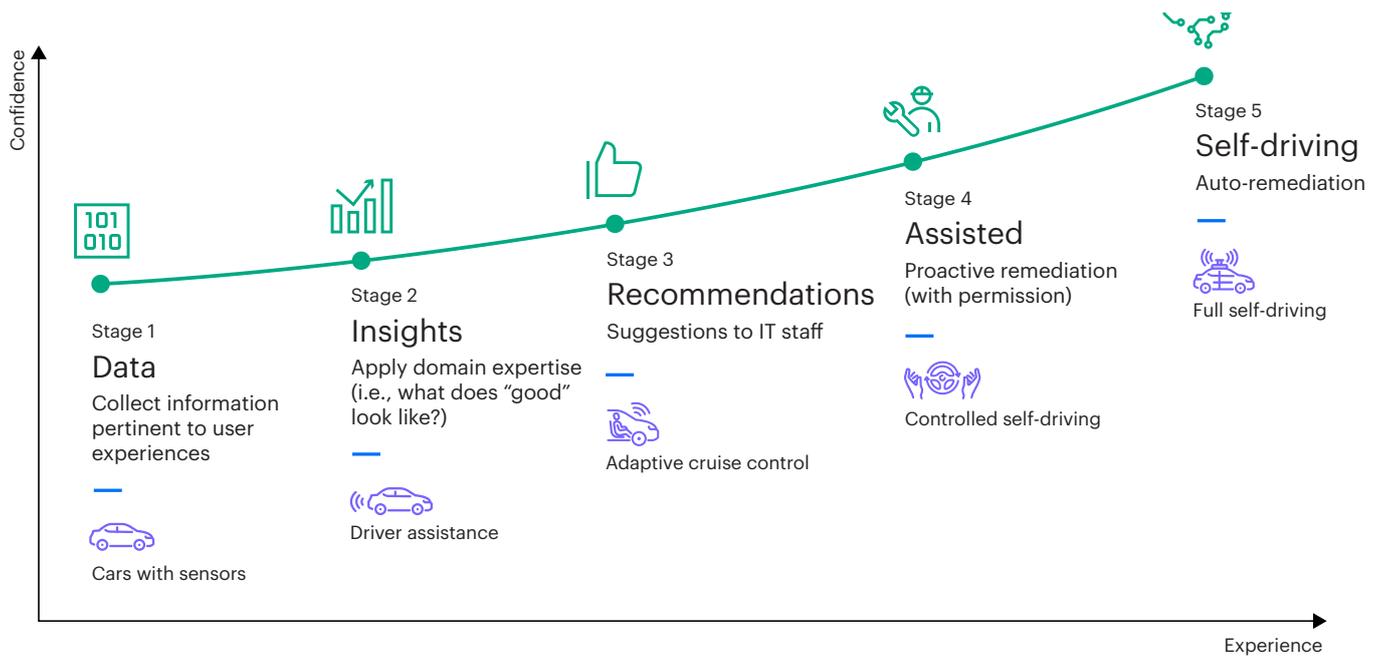
Figure 1. Journey to self-driving

Watch out for AI washing

In a market saturated with AI claims, distinguishing real innovation from AI washing is crucial. AI washing happens when vendors over-label, overpromise, or lightly repackage existing features as AI-powered. To avoid it, look for solutions that are:

1. Explainable
AI must make its reasoning visible. Explainable AI (XAI) tools and transparent root-cause analysis show why a recommendation or automated action was taken and how the AI improved over time. Understanding what's happening behind the scenes provides clarity and assurance.

2. Mature
AI systems are only as good as the data they are trained on. This is why vendor time in market, data volume, and data science expertise matter. Mature solutions offer quality data and battle-tested outcomes from real customer implementations, including the vendor themselves. Vendors who don't trust their own AI are a red flag.

3. Purpose-built for AI
A self-driving network can't be built by bolting AI onto a legacy system. It requires an AI-native architecture designed to observe, decide, and act continuously. This foundation is what makes autonomy dependable rather than fragile or unpredictable.

4. Human centered, not human replacing
Every trustworthy autonomous system is built to augment, not eliminate, IT expertise. Teams remain in control, deciding where automation applies and when to allow the network to self remediate.

Under the hood of HPE's self-driving network

HPE's philosophy centers on delivering real self-driving capabilities, grounded in transparency, rigorous data science, and AI-native architecture. Our proven solutions are here to help you along every step of the self-driving journey, built upon an AI-native native architecture.

— **Right data:** Full-stack telemetry collected at scale to fuel accurate, context-rich decision-making. Our data lake is the world's largest, offering both depth and accuracy.

— **Right expertise:** Continuously improving models based upon real world patterns developed by our data science teams in conjunction with our customer support staff.

— **Right architecture:** Purpose-built for self-driving operations, not retrofitted into legacy solutions.

— **Proven in our own operations:** We use our own AI internally for diagnostics and support workflows.

The road ahead: From "Can I trust it?" to "How far will it go?"

A self-driving network builds trust the same way self-driving vehicles do—through transparency, maturity, and repeated proof it can improve everyday operations safely. When the underlying architecture is explainable, purpose-built, and grounded in real data, autonomy stops feeling risky and becomes a practical advantage. The result is a network that reduces complexity, strengthens security, and frees IT teams to focus on higher-value work. At that point, the question becomes not whether to embrace autonomy, but how quickly its benefits can accelerate your business forward.

Learn more at

HPE.com/networking

Visit HPE.com

Chat now

HEWLETT PACKARD ENTERPRISE

hpe.com