Guide

The road to **AI-readiness**

Why it's time to re-evaluate your network and how to plan for success.





Key takeaways

- AI is putting unprecedented pressure on networks. Legacy infrastructure may not have the capacity, speed or resilience to support emerging AI workloads.
- Network failure is a major business risk. Downtime can disrupt operations, damage customer trust and create significant financial costs.
- Business resilience depend on visibility, governance and security. Organizations are using zero trust approaches to give visibility and control over users, AI agents, devices and data flows across their networks.
- Network transformation for the AI era should be phased and flexible. Prioritize critical systems, automate operations and build adaptable, diverse infrastructure with a step by step process and key questions for the network as AI becomes business as usual.

Table of contents

When the network fails, everything fails 3

Network outage: The usual suspects 4

Five foundations for an AI-ready enterprise 5-9

The roadmap for network resilience 10

Key questions 11

How Verizon can help 12



When the network fails, business stalls: The new challenges of the AI era

As businesses are increasingly built on their networks, a breakdown can have serious consequences. Websites crash. Booking systems fail. Orders aren't registered. Payments stall. Communications stop, production lines stop. In fact, everything that's digitally connected can be impacted. And that can have serious consequences, both financially and for your company's reputation.

"I've never known customers put such focus on the availability of their network," says Colin Wilson. an Enterprise Architect at Verizon Business. "For today's businesses, the network is an absolute imperative, just like electricity and water."

But as organizations place a growing reliance on artificial intelligence (AI), IT leaders have to deal not only with vastly increasing volumes of data but also an ever-evolving set of challenges and cyber risks.

Breakdown prevents take-off

Take the case of Alaska Airlines. A series of IT outages in 2025 forced the company to cancel hundreds of flights, causing travel disruption for thousands of customers. Not only did it cost the company an estimated $40 million,[1] it also impacted its customer service and damaged brand loyalty. And while outages like this are considered relatively rare, they're a real and near-term threat that all businesses need to be prepared for.

Keeping an eye on AI

Much of the conversation around cyber risk recently has centered around AI. The news cycle is inundated with reports of AI agents going rogue,[2] escaping users' control, ignoring instructions and hacking into websites. The case of OpenAI models circumventing controls designed to isolate them from the internet so they could breach Hugging Face's systems is certainly of concern. Indeed, AI firms themselves are urging companies[3] and nations to enhance their cyber defenses before AI grows powerful enough to override them.

AI overload

But it's not just rogue agents that can create potential problems. With more businesses investing in AI, and running more AI-heavy workloads, this shift is driving increased network demand, which puts extra strain on the network and data centers. That strain is leading to a rise in outages caused by IT and networking issues. In 2026, they made up 23% of impactful outages.[4] And these AI workloads are only going to increase, creating even bigger demand, which means that strain will grow, too.

Of course, while AI is clearly a concern, it's not the only potential cause of outages. Indeed, there are many potential weaknesses that organizations need to be aware of. But what exactly are they? How damaging can they be? And how can businesses fortify their network infrastructure to mitigate these potential issues – both known and unknown?

> "For today's businesses, the network is an absolute imperative, just like electricity and water."
>
> **Colin Wilson**
> Enterprise Architect
> at Verizon Business

Network outage: The usual suspects

It's no overestimation to say that digital downtime for a business can be devastating. In fact, research from Cisco and Oxford Economics[5] suggests that the average cost of downtime has reached $15,000 per minute.

While we're often quick to blame cyberattacks or bad actors for IT blackouts, they're really only one part of the problem and outages can be triggered by a variety of factors, from human error to bugs, software glitches or equipment failures. Similarly, outages can just as easily be created by applications, and the network is seen as guilty until it's proven innocent. As AI usage grows, radically changing the demand being put on networks, the likelihood of problems will continue to increase.

Typical causes of an outage

Human error:
- Someone makes a mistake while configuring a network, updating software or fixing system issues.

Infrastructure not built for AI:
- The network, servers, storage, power or cooling systems weren't designed to handle the extra demand of AI workloads leading to a breakdown.

Unpredictable AI workloads:
- AI suddenly creates large, unexpected spikes in demand, overloading the system.

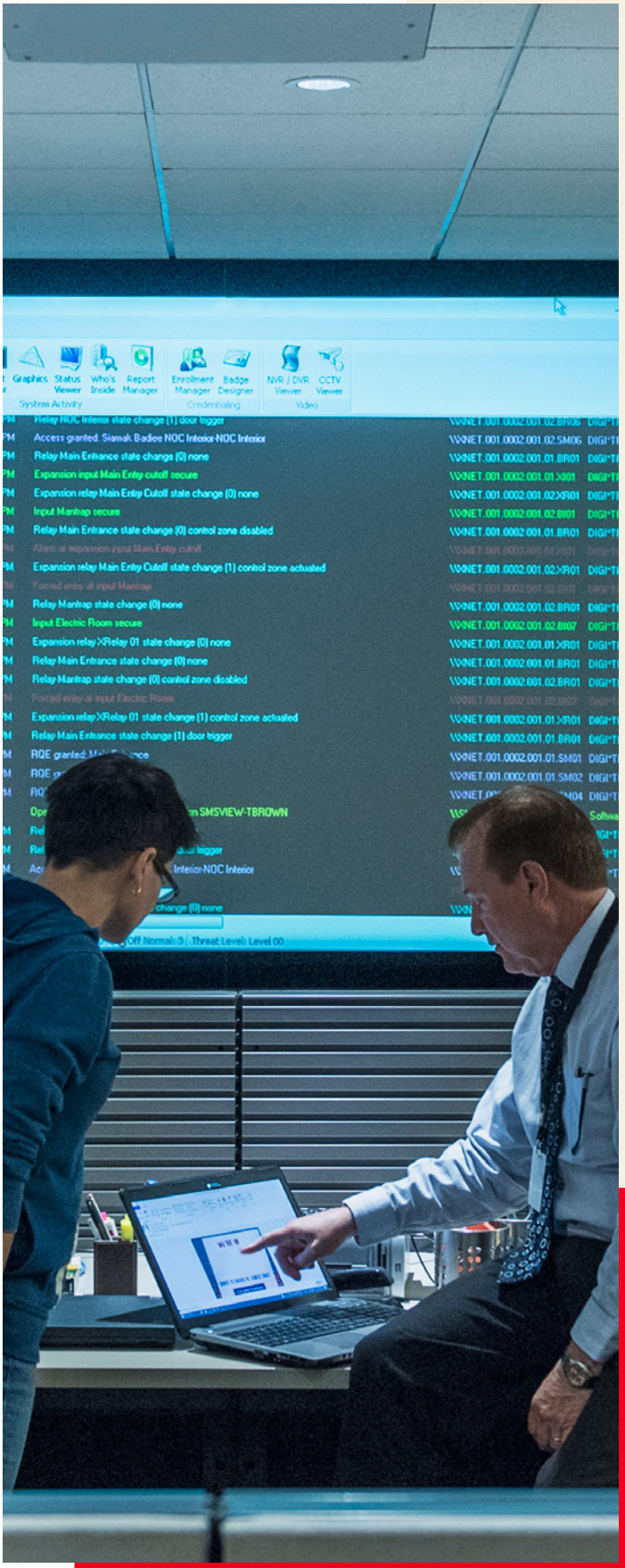
Hardware failure:
- Servers, storage equipment, power supplies or cooling systems fail. Or a physical event, such as a fire, damages a facility. While these aren't technically 'network issues,' the result is still the same.

Software bugs and glitches:
- A programming error or defective software update causes a crash.

Third-party failures:
- A cloud provider, telco, software supplier, data center or internet service provider (ISP) has a failure leading to a systems crash.

Cyberattacks:
- Bad actors use methods such as ransomware or distributed denial-of-service (DDoS) to infiltrate the network and cause harm.

Some of these network challenges are possible to anticipate through standard risk management. But others less so. To truly mitigate the risk of potential failure, it's essential to re-examine the network, fortifying your defenses and enhancing your capabilities, to ensure you have all the safeguards required and are set up for success.





Preparing your network for the AI era

The five foundations for a resilient AI-ready backbone

To reduce as many of the risks outlined above, and to future-proof your networks for the new age of AI-heavy workloads, IT and business leaders should focus on five key considerations.

Consideration 1: AI readiness

Businesses need to assess their network, ensuring it has the flexible architecture to handle the high data volumes and computer requirements of AI workloads. With the average modern enterprise running numerous scattered datasets and large numbers of disparate AI models across multicloud environments, there's a real risk of encountering severe latency bottlenecks and high network congestion.

"Say you have 20 different sets of data around the world and 20 different AI models that need to see that data," Wilson says. "When the first AI model processes an output, it may become an input for model two, thus these AI workloads are talking to each other. It's a latency and capacity nightmare for the network."

There's also an issue when it comes to the different types of AI on the network. On one hand, you have public large language models (LLMs) like Copilot and Gemini. On the other you have domain-specific AI which is trained on proprietary information.

The way the network handles and secures each type needs to be different. It helps to distinguish between standard tools that are commonly used within the business and those bespoke model-building workloads used for specific tasks, like drug discovery.

The proliferation of the Internet of Things (IoT) is another factor to consider. As well as new AI tools for human workers, businesses also have to deal with an explosion of data coming from non-human sources, like AI agents, robots, machines, sensors and gadgets. With the work created to manage all this data, it also creates extra vulnerabilities.

While organizations might previously have had to manage the security of, say 10,000 employees having access to the network, they're now having to deal with maybe hundreds of thousands or a million devices all connected – some of which may have been installed by business users, not IT experts. In some cases, IT and IT security teams might not even be aware of their presence on the network. Even with robust monitoring, IoT devices can be harder to verify and may not meet industry standards for security. So, increased governance is crucial. You need a robust strategy for all AI tools, and a framework to control how much capacity any model or agent can have.



What's the approach for AI readiness?

As your business embraces AI on a larger scale, you'll see a profound impact on your network requiring low latency, business-critical performance, and an increase in bandwidth needs. To be truly AI-ready, you should:

- Implement dedicated AI-ready network/Wide Area Network (WAN) alongside your corporate and operational networks
- Enhance your network's flexibility, visibility and governance
- Separate high-performance, east-west AI training/inference traffic from standard north-south enterprise traffic using dynamic network slicing to eliminate system overload
- Establish a different set-up for the huge data in the training phase of enterprise-specific AI

Consideration 2: Visibility and governance

When you're managing multicloud environments from different vendors, you could experience blind spots. Many organizations use AI to carry out tasks that might previously have had to go to different departments or processes to gain approval to do so. With AI removing that layer of oversight, it's possible that actions are carried out with little or no visibility. That can lead to governance issues, and it can have a damaging effect on the network.

It's essential, therefore, to make sure you can monitor every data flow continuously, giving you greater visibility and helping you mitigate issues before they lead to broader system outages. It also helps reduce anxiety around maintaining compliance and meeting regulatory requirements.

What's the approach for visibility and governance?

Maintaining visibility over all your data is crucial not only to ensure you understand the kind of pressures your network is under, it also helps you spot issues before they become problems. To do this, you can:

- Integrate multicloud cross-domain data into a single-pane-of-glass dashboard. This helps you keep on top of everything in one place. Configuring through a self-service portal and APIs can help you keep pace with rapid, constant change.
- Enhance your network visibility and resilience to meet mandatory compliance under the EU Digital Operational Resilience Act (DORA). This can help you stay ahead of problems, and avoid hefty penalties, which can reach up to €20M or 10% of global annual turnover.

"Most national enterprises are going to be captured under those regulations," says Wessel Blom, Head of Solutions, Verizon North Europe. "That includes diagrams that show how fiber routes are mapped out. They also need to consider backup systems for networks and power. When you put in your satellite link or your mobile backup, how do you ensure that's on a different power grid going to a different country?"



Consideration 3: Zero trust protection

With agentic AI systems autonomously querying databases, making API calls and transferring data between clouds at lightning speeds, traditional IT security approaches simply can't keep up. They can't inspect these ultra-fast transactions without creating crippling latency. So, either these workloads are not adequately secured, or the network will grind to a halt trying to secure them. Plus, with unmonitored desktop AI agents repeatedly querying backend APIs, networks and systems can easily become overloaded, affecting genuine business workloads.

"We're in a new world, where machines can target vulnerabilities and start doing lateral movement in seconds," says Alistair Neil, Managing Director of Advanced Solutions, International at Verizon Business. "How do you change the architecture of your business so that you're not preventing people from using the tools they want to, but at the same time, you're protecting the infrastructure you've got?"

By implementing a zero trust framework across the entire network – which includes all your IoT sensors and devices, AI agents, and automated operators – you can ensure that autonomous AI agents are only able to access authorized applications and data pipelines.

What's the approach for security in the AI-ready network?

By building consistent, robust security protocols into your network, you can keep on top of security and prevent AI agents from doing things they're not supposed to, or tying up bandwidth. To do this, you should:

- Embed zero trust controls directly into the transport layer so you can authenticate non-human machine identities without negatively affecting network performance
- Establish strict rate limits, access scopes, and cryptographic identity verification for automated agents

> "There are lots of sensors and devices of all sorts sending data. You need to understand what they are. What data are they sending? Where are they sending it? Have you got a proper security wrapper, so they're not sending data the wrong way or being used to compromise the network? You need some rules around what AI tools are able to do and what systems they can access."
>
> **Colin Wilson,**
> Enterprise Architect,
> Verizon Business

Consideration 4: Edge and data sovereignty for hybrid cloud

With companies increasingly using AI for different purposes – from customer service to fraud detection, to simplifying processes or managing factory operations – these AI models require access to customer and operational data. The problem is that this data might be housed in different locations around the world and subject to national data sovereignty laws (e.g. EU Data Boundary, General Data Protection Regulation (GDPR), and local banking regulations) that strictly forbid the transfer of sensitive data across borders. Where, then, should compute operations take place?

If located at the edge, you don't need to send as much data back and forth to different locations, so you can improve your ability to meet regulatory compliance and achieve lower latency. But you won't be able to scale as easily. On the other hand, if you store and compute all data in one centralized location, you can scale more easily, but it's more of a regulatory and latency problem. And a failure there could affect your operations everywhere.

Take the example of a retailer that's slowly increasing their number of AI functions. They're also increasing the amount of tasks they're processing locally and getting to the point where the edge compute function isn't big enough anymore. What do they do? Upgrade the server in every store to boost local computing? Or move the compute to the cloud? The cloud is certainly more scalable but this shift has significant implications for the network architecture. Not only does the network need to be sized to handle the additional traffic but the 'availability' of connectivity is suddenly of critical importance because the business can't afford the connectivity to go down. They need a better way.

Meeting increasing data regulations

Another thing to consider is that global enterprises are likely to see increased regulation to keep data within national or regional boundaries. This will be almost impossible if you're using the public internet as your backbone. And it will be even more complex if you're not sure which AI systems are using your data, and what those AI systems are doing with it.

What's the approach for managing AI data sovereignty?

For a truly AI-ready, compliant network, you should create a decentralized network estate, which will help you enhance operational survivability by eliminating the risk of single point of failure and facilitating compliance with data protection laws. With this kind of distributed architecture, you can:

- Keep sensitive data and computing capacity in the location it's needed
- Run AI models locally
- Maintain backup systems in multiple locations
- Transfer data between regions only if needed
- Maintain central governance keeping all the data in the same place





Consideration 5: Network automation and efficiency

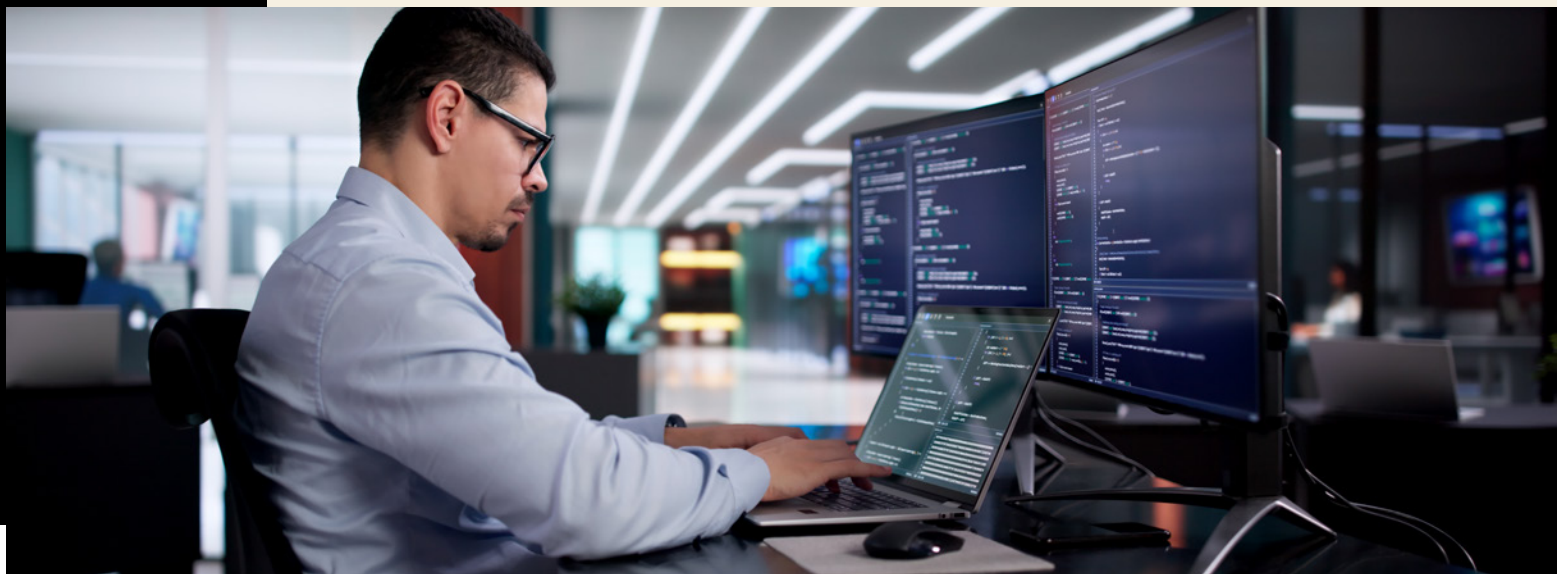
IT departments in many organizations spend far too much time manually configuring their firewalls, troubleshooting problems and alarms, and managing the complexities that come with legacy hardware. It's not a great use of their time. And it prevents them from focusing on other business-critical operations. However, by using intelligent automation to simplify the network infrastructure, you can set it up to handle growing amounts of data without extra manual intervention. That means IT teams can spend less time on maintenance or repetitive tasks and more time focusing on growth and innovation.

What's the approach for integrating intelligent automation?

Adopting intelligent automation can help you reduce unnecessary layers and tasks. To achieve this, you can:

- Shift from manual maintenance to autonomous AI operations where AI monitors the network automatically
- Adopt one central system to manage network and security functions and rules, freeing up budget and resources to invest in launching new products, opening new sites and bringing services to market sooner

"Agility is the hallmark of the digital economy," Wilson says. "Enterprises need to be quick and agile. When the business wants to do something – from opening a new store, to spinning up a new production line, or entering a new market – IT needs to respond quickly. Intelligent automation is a powerful tool in enabling them to do that."



The roadmap for network resilience

Many organizations are now realizing the need to look at their networks again. The key question is how can they move from their existing legacy stack without tearing everything down or causing disruption. “There are so many aspects to review,” Wilson says. “Edge vs cloud compute? Upload vs download traffic patterns? Where’s my data going to be processed? They’re worried about data integrity and how they secure their network.”

This roadmap has been devised to help businesses manage the transformation.

Step 1: Establish strict governance

- Audit exactly what is connected to your network. Assign clear ownership for every user, AI agent and IoT device so you can manage or deactivate them instantly if an issue arises.

Step 2: Pinpoint high-capacity hubs/locations

- Identify the core data centers and cloud environments that will bear the brunt of AI workloads to ensure they have sufficient, scalable bandwidth.

Step 3: Prioritize system criticality

- Categorize which applications demand 100% uptime vs those that can tolerate brief outages. Continuously reassess this hierarchy as your business needs evolve.

Step 4: Establish a governance layer with Secure Access Service Edge (SASE) and implement zero trust protocol

- SASE and zero trust frameworks give you the tools to cap AI agent bandwidth, prevent unauthorized access, and assign clear ownership to the massive influx of connected IoT devices.

Step 5: Ensure network architecture matches business needs and priorities

- Avoid a purely cost-focused mindset during migration. Choosing the cheapest short-term option could create wider operational vulnerabilities and higher long-term expenses.

Step 6: Maintain architectural flexibility

- Build in the ability to rapidly shift bandwidth or change geographic routing in case geopolitical shifts or new regulations/sovereignty laws suddenly restrict access to specific cloud environments.

Step 7: Plan migration pathways for automated bots to replace manual processes

- Modern infrastructure is far better suited to automations and often uses agentic capabilities ‘out of the box.’ Big bang switch overs are hard though, so run legacy and new infrastructure side-by-side to catch issues and guarantee zero operational downtime during transition.

Step 8: Implement backup systems planning

- Effective BCDR (business continuity and disaster recovery) planning ensures true path diversity (primary, secondary and tertiary links) that don’t rely on the same underlying infrastructure, such as shared subsea cables or regional power grids.

Key questions

Before starting any network transformation, ask yourself these questions:

1. Network challenges:

What caused your last three major network incidents, and were they external cyberattacks or internal issues?

2. Network segmentation:

Do you have the policies and processes as well as the technology in place that will allow you to segment your network to accommodate rapidly increasing AI traffic volumes?

3. Scalability:

How are you measuring the network impact of pilot AI models to ensure you have the capacity to scale them enterprise-wide without causing congestion?

4. AI agentic operations:

How do you authenticate AI agents making thousands of cross-cloud API calls per minute, and does that create latency bottlenecks?

5. Visibility of automation:

How do you manage the release of new automations and how do you monitor and control the autonomous actions of AI agents and IoT devices on your network?

6. Edge and center:

What's your balance of edge and centralized compute? How does your network provide the resilience and capacity that you're going to need?

7. Regulatory resilience:

If an AI workload triggered a major network overload, could your reporting mechanisms satisfy EU Digital Operational Resilience Act (DORA)/network and information systems (NIS2) regulatory timelines within 24 hours?

8. Flexibility:

How quickly and autonomously can your network adapt, reroute traffic or scale bandwidth if a primary connection fails or a sudden disruption occurs?

9. Data sovereignty:

Do your multicloud AI pipelines comply with local data sovereignty regulations, or is raw customer data crossing borders to reach centralized AI models?

10. IT ops automation:

How much time do your IT staff spend on routine maintenance compared with focusing on scaling new digital capabilities?





How Verizon Business can help

Understanding the potential network risks of this new age of data-heavy, AI-powered workloads is one thing. Having a robust plan to fortify your network so you can safeguard operations and guarantee network availability is another. But even then, getting started and staying on course through that transformation can be a huge, complex, time-consuming undertaking. That's why you need a partner that not only understands the complexity of everything involved, but also lives and breathes it on a daily basis.

Verizon can help you transform your network to create a resilient, manageable foundation to fully embrace the age of AI without worrying about outages, loss of capacity, or other issues that negatively impact your business.

Build on a strong foundation

Verizon owns and operates a global Tier-1 network backbone that spreads throughout 180 countries. It gives you a strong physical foundation, with private IP backbone, and the kind of built-in survivability you need to run and manage mission-critical AI workloads. You get a strong base upon which to build your AI and digital services.

"We own the foundational layer," Wilson says, "which is the big network that sits at the center. We then build our managed services around it, adding the technologies that exactly match our customers' needs."

Simplified management

With the pace of change only increasing, we provide a single, unified policy framework that encompasses your multi-vendor environments to make things simpler. Rather than managing separate tools for connectivity, cloud access and security, you get a more unified framework. You can apply consistent policies, maintain visibility over your whole architecture, ensure zero trust security and manage vendors more easily.

AI-enhanced operations

Find faults and resolve them faster with AI automation monitoring your network. With automatic evaluation of any upgrades or change requests, you can spot potential issues before they happen, preventing complications. The AI constantly monitors to identify problems and turn data into valuable business insights.

World-class consulting

Our consulting, transition and project management office (PMO) teams are experts in their fields, working with leading organizations every day. We work with you to make sure you have the expertise, resources and guidance to deliver a seamless transition from high-risk legacy environments to high-performing cloud-based operations.

Simpler business

We help you eliminate the headache of managing a complex, fragmented spiders' web of providers, suppliers, contracts and regulatory requirements. We make things much simpler by bringing everything together under one managed service contract, tailored to meet your specific needs.

The age of agentic AI offers promise like we've not seen before. Businesses that truly embrace it are sure to drive innovation, efficiency, productivity and business growth, and might even find new ways to change the world and society. But the pace of growth, change and urgency to adopt AI are also moving at lightning speeds. The organizations that take the time now to ensure they're fully prepared for the future will be the ones who ultimately flourish. Connect with our enterprise strategy team for an in-depth discussion about your network's AI readiness.

Find out more

Learn more about how Verizon can help you explore and adopt AI in your networks and enterprise. verizon.com/business/en-en/solutions/adaptive-networks/



1. Alaska, 2025. Alaska Airlines' statement on IT outage.
2. The Guardian, 2026. Sharp rise in incidents of AI escaping users' control, research finds.
3. BBC News, 2026. Time is running out for cyber security, warn top tech firms.
4. Networkworld.com, 2026. Network outages, power failures strain data center resiliency.
5. Cisco, 2026. The $600 Billion Wake-up Call: New Splunk Research Reveals Downtime is a Systemic Business Crisis.

© 2026 Verizon. This content was created with the assistance of artificial intelligence and validated by humans. OGSB1350423