GTT Greater Technology Together

White paper

# HOW ENTERPRISES APPROACH NAAS AND MNS TO BUILD RESILIENT, FUTURE-READY NETWORKS

gtt.net


# INTRODUCTION

**The network has become the new battleground for enterprise IT because it's the layer where cloud complexity, distributed work and rising security demands all converge. Enterprises are responding to that complexity by focusing on the network layer. Specifically, how to combine two approaches to network management that were long seen as competing choices: Network as a Service (NaaS) and managed network services (MNS).**

NaaS is a consumption-based model that delivers network connectivity and capabilities on demand without the need to own or manage physical infrastructure. It's built for flexibility and rapid deployment. With MNS, a third-party provider takes responsibility for the ongoing operation, monitoring and management of the network. Organizations use this approach when reliability, consistency and service assurance cannot be compromised.

Last year's research, published in GTT's *Cloud Usage and Management Trends: Where is the Money Going?* found that enterprises were overwhelmed by multi-cloud complexity and turning increasingly to managed services to regain control. This year's research picks up where that left off, showing how enterprises are now combining NaaS with MNS to address the complexity that multi-cloud, distributed work and rising security demands have placed on their infrastructure. The debate over which model to choose is largely over; **78%** of enterprises are already running both and **89%** are expected to within the near future.

The enterprises that provided feedback in this study have committed to this combined approach, evaluating NaaS the way they would evaluate any long-term strategic partnership: on a five-year TCO, not a short-term cost. Enterprise commitment is one thing. Running combined NaaS and MNS well is another. Based on the results provided, four friction points show up consistently across the enterprises in this study and each one carries real consequences if left unaddressed:

1. **Observability gaps**
2. **Rising security and compliance demands**
3. **Cost volatility**
4. **Talent shortages**

This paper is based on an analysis of GTT sponsored original research from Hanover Research, conducted among 300 senior technology and business leaders across the US, UK, France and Germany, of enterprises with $200 million or more in annual revenue. It is written for the technology and business leaders who are accountable for getting networking management right. Each friction point is examined in depth, including where they come from; what the financial commitment behind networking looks like in light of them, how they play out differently across industries and what enterprises need from a provider to address these friction points.

# THE MARKET HAS DECIDED: NAAS AND MNS CONVERGENCE IS THE DEFAULT

**NaaS and MNS have moved from competing options to complementary ones faster than most expected. Even among enterprises planning new deployments over the next 24 months, 57% expect to split NaaS and MNS equally, and another 28% expect to run mostly NaaS with some MNS. Pure plays in either direction are increasingly rare.**

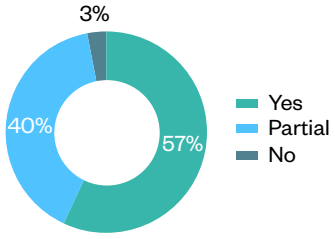
GTT proposed moving a manufacturer of agricultural products to a Managed SD-WAN solution to achieve reliable, secure, scalable service. SD-WAN is a cloud-based centralized network infrastructure which offers network connectivity across a wide area, built-in security features to protect the data moving across the entire network and reduces capital investment.

GTT implemented its Managed SD-WAN solution into test sites, delivering a network that was 10 times faster and much more cost efficient, exceeding expectations. The company described the technology as a "game changer"

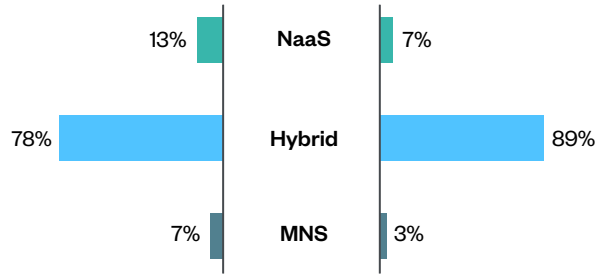
A rollout across all its sites was approved and the company is now now benefiting from cross-company performance improvements, cost savings and better analytics delivered via GTT EnvisionDX, the observability and network management portal. They are able to map and monitor traffic across the network and move computing power to the parts of the business that need it most from a single portal and in real time. No more truck rolls to make updates in far-flung locations, every site updates at the same time.

## HYBRID ADOPTION DOMINATES AS ORGANIZATIONS SEE NAAS AND MNS CONVERGING

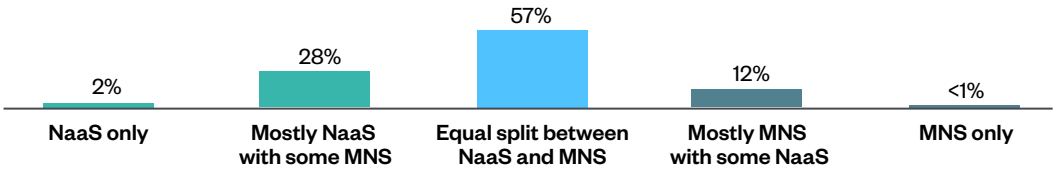
### Perceived Convergence Between NaaS and MNS




### Current Usage / Future Use Consideration




### Expected Service Model to Dominate New Developments in 24 Months



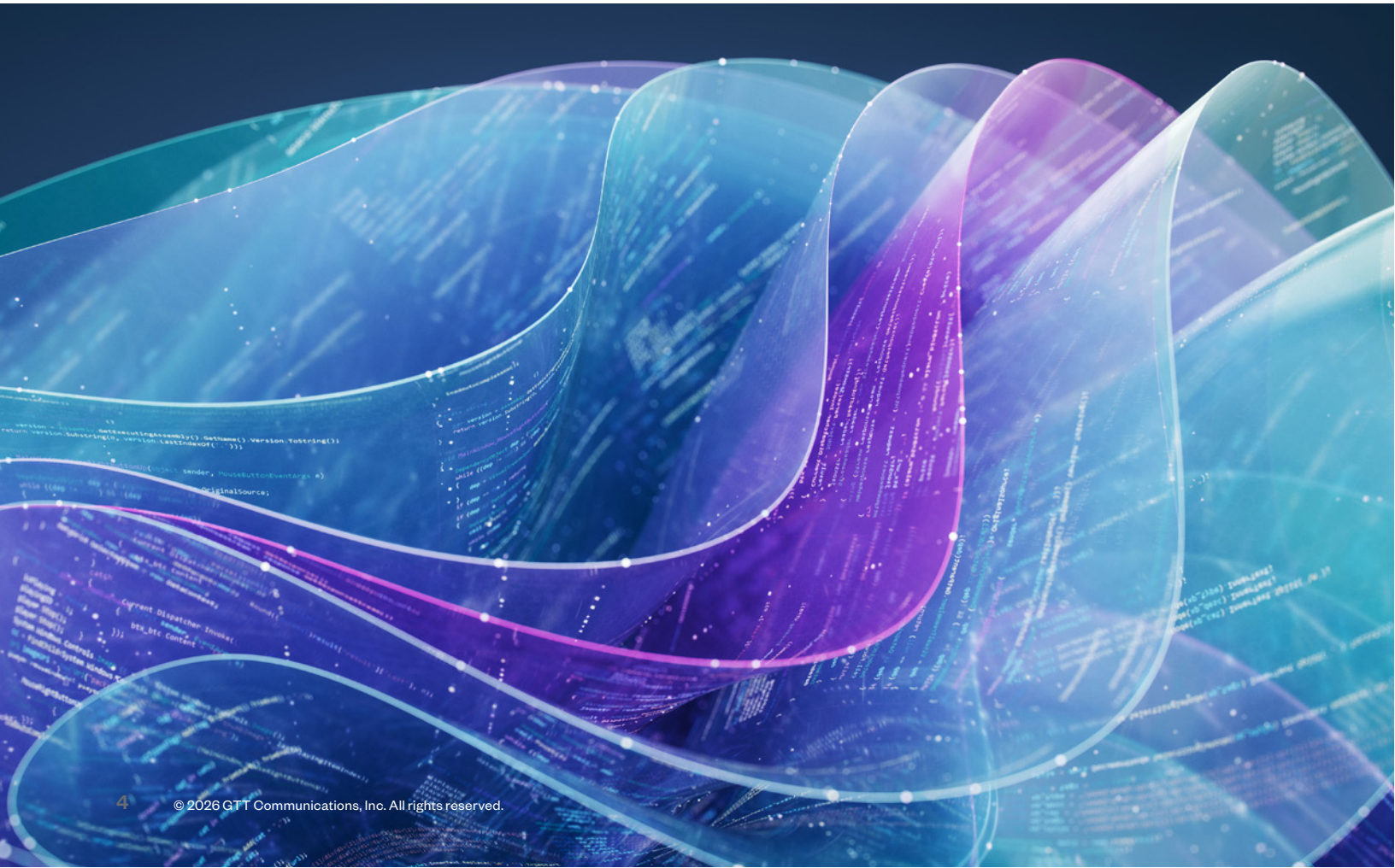
What makes this notable is that NaaS and MNS were pitched and understood as opposing strategies: two different bets on how to run a network, each with its own advocates and its own logic. Now, **57%** of enterprises say they see the two converging, because each one solves a problem the other doesn't.

| | NaaS | MNS |
|---|---|---|
| **Best suited for** | New deployments, distributed work, cloud-native environments | Environments where reliability, compliance and service assurance can't be compromised |
| **Core strength** | Flexibility and speed | Reliability and assurance |
| **What it enables** | Fast provisioning and easy scaling as the business grows or shifts | Consistent performance and audit-ready controls in complex, regulated or mission-critical environments |

**NaaS** is used when the business needs to move fast. **Scalability, technology adoption and business continuity** each rank as very or extremely influential NaaS adoption drivers for **90%** of organizations using or planning to use it, priorities that point to growth and operational flexibility as the core NaaS use case.

**MNS** is used where the cost of getting it wrong is too high to risk. Among organizations remaining MNS-only, reliability ranks as the top driver, cited by **93%**, a signal that **consistency and assurance, not speed,** are what MNS is being asked to deliver.

The result is a network that looks less like a single architecture and more like a portfolio, with NaaS and MNS each playing to its own strengths.



# WHAT MATTERS INTERNATIONALLY

| | United States (n=145; 48%) | United Kingdom (n=55; 18%) | Germany (n=55; 18%) | France (n=45; 15%) |
|---|---|---|---|---|
| **Convergence between NaaS and MNS [% Yes]** | 56% | 56% | 53% | 64% |
| **Current Model** | Hybrid 79% | Hybrid 85% | Hybrid 58% | Hybrid 89% |
| **Likely Future Model** | Hybrid 86% | Hybrid 89% | Hybrid 95% | Hybrid 96% |
| **Top NaaS Driver [Top 2]** | Scalability 90% | Simplified Network Management 91% | Business continuity; Scalability; Tech adoption 96% | Cloud-native integration 98% |
| **Financial Metric used to Justify NaaS** | 5-Year TCO 63% | 5-Year TCO 49% | 5-Year TCO 58% | 5-Year TCO 69% |
| **Observability Barrier [% Yes]** | 76% | 51% | 93% | 78% |
| **Required Level of Audit & Compliance [Top 2]** | 90% | 91% | 84% | 98% |

## Key takeaways by country

### United States

- Most mature current hybrid usage: The US shows **79%** current hybrid adoption and **86%** future consideration.
- Scalability is the headline driver: The top reason to integrate or migrate to NaaS is scalability (**90%**).
- Board justification is financially led: The main metric used to justify NaaS to the board is 5-year TCO (**63%**).
- Observability remains a concern: **76%** cite lack of observability as a barrier — high, though below Germany and France.

## United Kingdom

- High hybrid adoption and future demand: **85%** currently use a hybrid model and **89%** are considering it for the future.
- Operational simplicity is the lead message: The UK's top driver for NaaS adoption is simplified network management (**91%**).
- Strong compliance expectations: **91%** require high or very high audit/compliance evidence from providers.
- Lower observability friction: The UK has the lowest observability barrier among the four, at **51%**.

## Germany

- Biggest growth gap/opportunity: Germany has the lowest current hybrid adoption among the four at **58%**, but the highest future consideration at **95%** — a strong indicator of upside.
- Top drivers are unusually broad: Germany ties across business continuity, scalability and technology adoption at **96%** each.
- Observability is the biggest barrier: Germany has the highest concern around lack of observability, with **93%** citing it as an obstacle to NaaS adoption.
- Lower convergence perception: Germany is the least likely of the four to say NaaS and MNS are converging (**53%**).
- Regulatory pressure is a major story: The research flags NIS2 as especially significant in Germany, affecting about 29,000 entities, with potential fines up to €10 million or 2% of global revenue, plus board-level liability.

## France

- Highest future hybrid interest: **96%** are considering a hybrid NaaS + MNS model in the future, with **89%** already using a hybrid model today.
- Cloud-native integration stands out: France's top driver for NaaS adoption is cloud-native integration (**98%**).
- Strongest compliance expectations: France shows the highest requirement for high/very high audit and compliance evidence from network providers at **98%**.
- Highest perceived convergence: France is the most likely to say NaaS and MNS are converging (**64%**).

## Cross-country takeaways

**United States**
Strongest case for scale, TCO and scalability

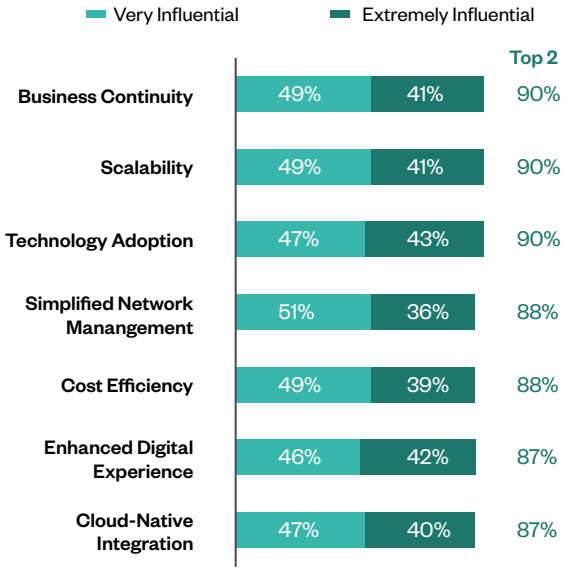
**United Kingdom**
Strongest case for simplified management and cyber resilience

**Germany**
Biggest growth opportunity, but also biggest observability/ regulatory challenge

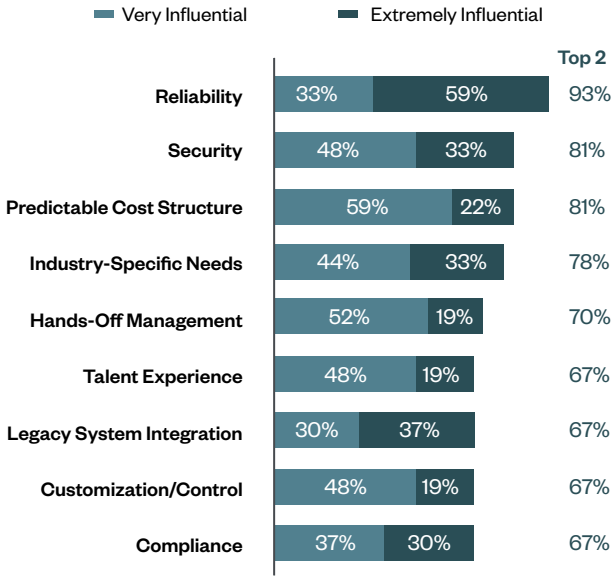
**France**
Strongest compliance and cloud-integration story

## ORGANIZATIONS APPEAR TO SELECT NAAS FOR OPERATIONAL ENABLEMENT AND MNS FOR ASSURANCE NEEDS

### Influential Factors in NaaS Adoption




### Influential Factors in MNS Adoption



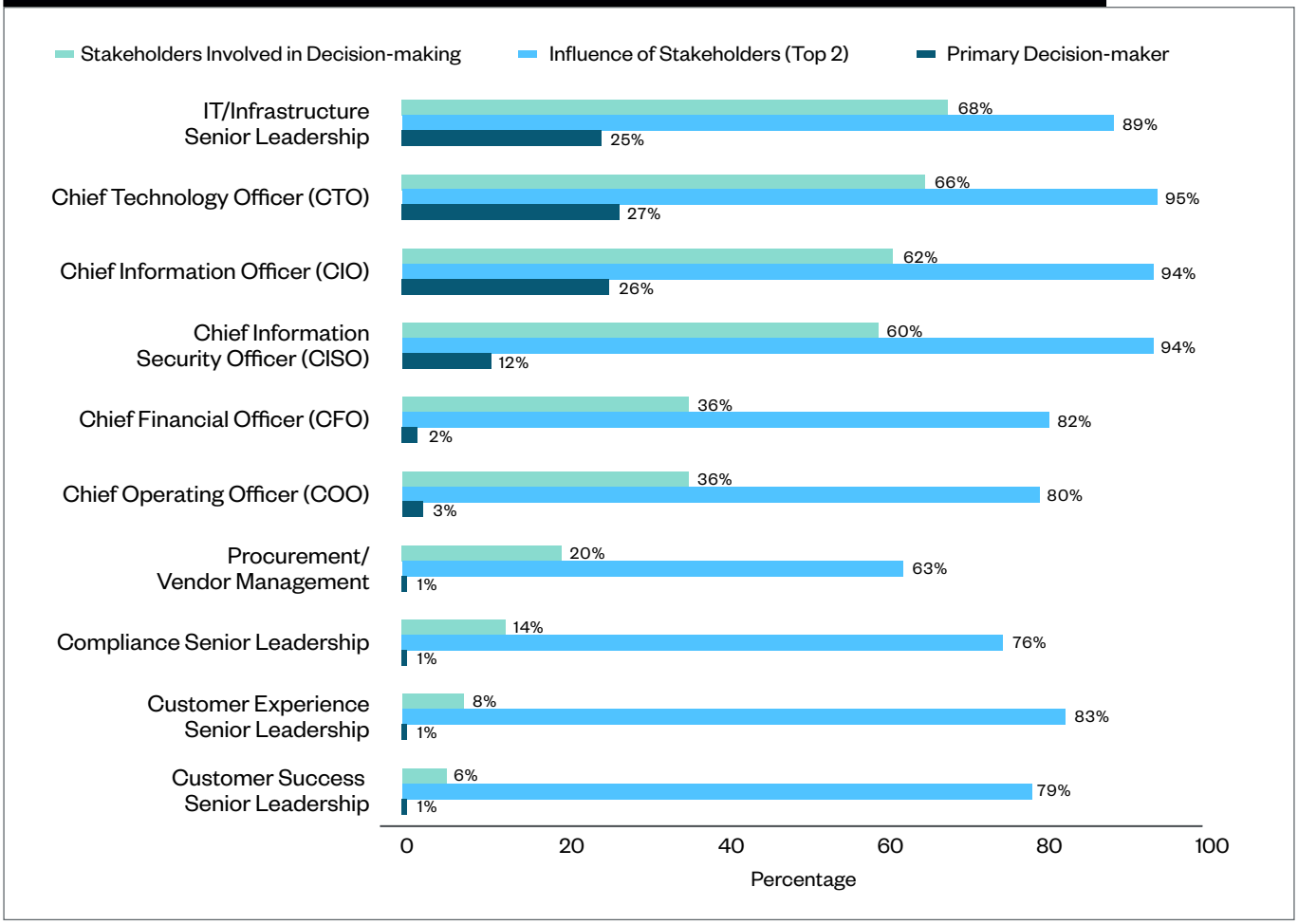

## The Network Has a New Constituency

Network decisions have moved well beyond IT. CTOs, CIOs and CISOs still make the final call; the CTO is the primary decision-maker in **27%** of organizations, the CIO in **26%** and the CISO in **12%**. But the circle of influence has widened significantly. CFOs and COOs are each involved in **36%** of decisions and compliance and legal leadership are involved in **14%**.

"Managed network services can help organizations significantly lower IT capital expenditures, reduce the need for staff scaling and training and mitigate risks for companies undergoing multi-cloud and NaaS migrations.

***KENN D WALTERS***
***LEAD ANALYST & EXECUTIVE ADVISOR, ISG***

## NAAS AND MNS DECISIONS ARE LED BY TECHNOLOGY LEADERSHIP WITH INFLUENCE EXTENDING BEYOND THE PRIMARY DECISION-MAKERS




A notable addition to that group is customer experience leadership, however though, customer experience leaders represent the smaller faction of the leadership invited to the decision making table.

This makes sense because a network affects how quickly a customer gets served, how smoothly an employee can do their job and how reliably a digital product performs. Any one of those breaking down shows up immediately as a customer experience problem, regardless of whether the root cause sits in the network.

The compliance-driven stakeholders follow their own logic. Mandates like DORA, PCI, GDPR and HIPAA increasingly attach dollar figures and audit consequences to network performance and security posture. Once a network failure carries a quantifiable financial or regulatory cost, finance and legal stop being downstream stakeholders and become participants in the decision itself.

Between the customer-experience stakeholders and the compliance-driven ones, the bar for what the network needs to deliver has never been higher. That's what makes the friction points explored in the next section so consequential: they're points of exposure for a much wider set of executives than IT alone.

> "Delivering a great customer experience for us means making sure our customers know with absolute certainty what we offer, where it is and when it will be in their hands
>
> ***CIO OF A MAJOR ELECTRICAL COMPONENTS DISTRIBUTOR***

# THE FRICTION POINTS

**Hybrid solves the strategic question of whether to run NaaS and MNS together. It doesn't make the day-to-day work of running that combination easy. Four friction points show up consistently across the enterprises in this study and each one carries real consequences if left unaddressed.**

## **Friction Point 1:** Observability

Observability refers to an organization's ability to monitor, understand and act on what is happening across their network environment in real time, looking at performance, security and compliance with immediate troubleshooting.

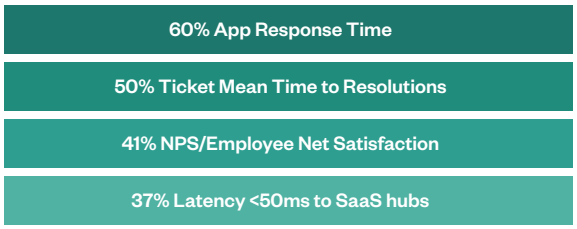
**Seventy-five percent** of enterprises say observability has been a barrier to NaaS adoption. **18%** of responders say it has stopped adoption more than once. That's not surprising once you consider what hybrid actually requires; visibility into two different environments, often built by different providers with different tooling, that need to be monitored and understood as a single system.

Without that visibility, troubleshooting becomes guesswork. An outage could originate in the NaaS layer, the MNS layer, or the handoff between them. Without unified observability, finding out which one adds time directly onto the outage itself. The longer it takes to identify where the problem lives, the longer it takes to fix and the more it costs in lost productivity or missed SLAs.

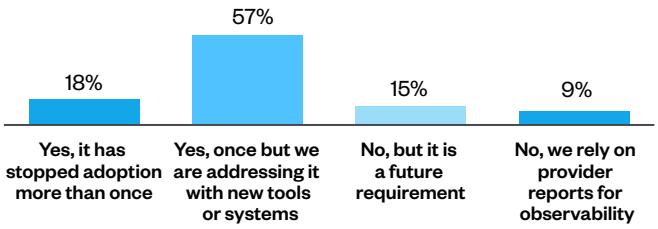
The same blind spot creates compliance exposure. Auditors expect clear proof of what happened across the network, regardless of where the data resides. If the same visibility gap that slows troubleshooting also prevents an organization from producing that evidence on demand, observability stops being an operational challenge and becomes a compliance risk waiting to be exposed.

**ORGANIZATIONS APPEAR TO SELECT NAAS FOR OPERATIONAL ENABLEMENT AND MNS FOR ASSURANCE NEEDS**

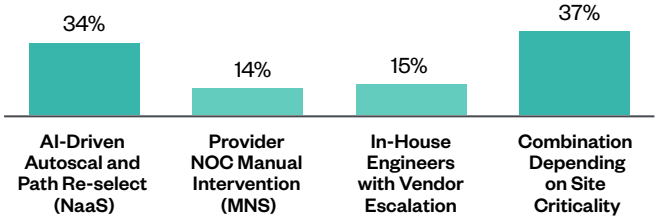
### Top Digital Experience KPIs for Internal Users




### Observability Barrier to NaaS Adoption




### Preferred Network Performance Remediation




### Key Observability Concerns in NaaS

## **Friction Point 2:** Security and compliance

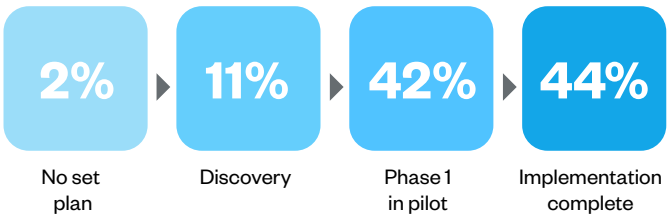
Zero trust implementation is well underway across the market, with **44%** of enterprises having completed it and another **42%** actively piloting it. But policy enforcement is not the same as protection. The bar for proof keeps rising even where zero trust is already deployed. **Ninety percent** of enterprises require high or very high audit evidence from their network providers. The evidence needed goes beyond high level reports or provider certifications, but detailed activity records that can withstand scrutiny. Immutable logs that cannot be altered after the fact are considered valuable or extremely valuable by **94%** of respondents. The compliance question is no longer "are you secure?" but "can you prove it and can you prove it holds?"

Encryption key management adds another layer of complexity. **Forty-five percent** of enterprises want full control over their own keys, while **46%** prefer a shared responsibility model where they own the keys but the provider stores and manages them. Only **7%** are willing to hand key management over to the provider entirely. The message is consistent across both camps: customers expect to retain meaningful control. Providers that don't offer that flexibility are increasingly disqualified before the conversation starts.

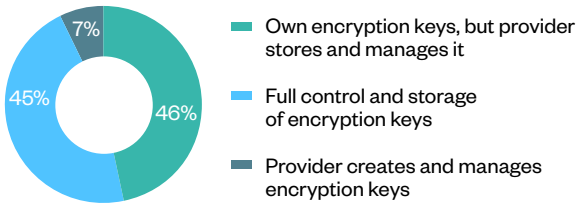
The compliance landscape itself is also shifting and the network sits at the center of most of it. Over the next 24 months, enterprises expect the biggest regulatory impact to come from resilience requirements around ransomware and supply chain attacks (**56%**), data residency and sovereignty mandates (**48%**) and Environmental, Social and Governance (ESG) related IT practices (**48%**).

**SECURITY EXPECTATIONS ARE HIGH AS MOST ORGANIZATIONS ARE ADVANCING ZERO TRUST AND REQUIRE STRONG AUDIT EVIDENCE**

### Current Stage of Zero-trust Implementation

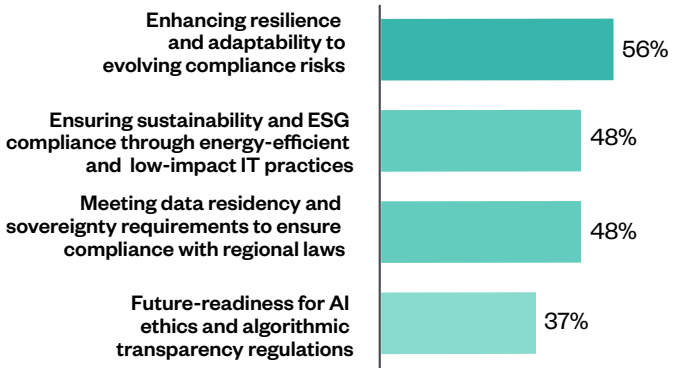



### Preferred Model for Encryption Key Management

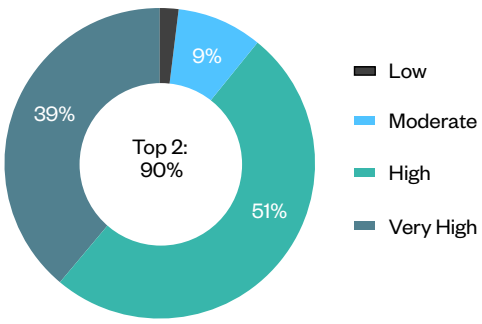



## Compliance and Audit

### Expected Compliance Regulation Impact Areas




### Required Level of Audit and Compliance Evidence from Network Providers



# *FOUR COUNTRIES, FOUR SECURITY REALITIES*

## United States

### Delivered Outcomes, Shared Responsibility

The US is the second most advanced market, with **47.6%** reporting Zero Trust complete. It leans toward a shared-control model, with **51.7%** preferring customer-owned but provider-managed encryption keys. US buyers respond to managed models when accountability and ROI are clear.

## United Kingdom

### Furthest Along, Most Protective of Control

The UK leads the survey in Zero Trust maturity, with **60%** reporting implementation complete. It is also the most control-oriented market: **65.5%** prefer to store encryption keys themselves and **100%** of UK MNS-only respondents cite security as a top reason to stay there

## Germany

### Cautious by Design, Not by Default

Germany is the most methodical market. It has the **highest discovery rate (18.2%)** and **49.1%** in pilot, showing momentum but measured execution. With NIS2 pressure and strong sovereignty expectations, the cost of getting security wrong is high.

## France

### Moving Fast, But Trust Must Be Earned

France has the **highest pilot rate (57.8%)**, showing strong Zero Trust momentum, but only **31.1%** report completion. Security and compliance are also strong reasons to remain MNS-only and buyers expect resilience plus proof of control.

## Bottom Line

**United States**
Pragmatic and outcome-led

**United Kingdom**
Mature and control-first

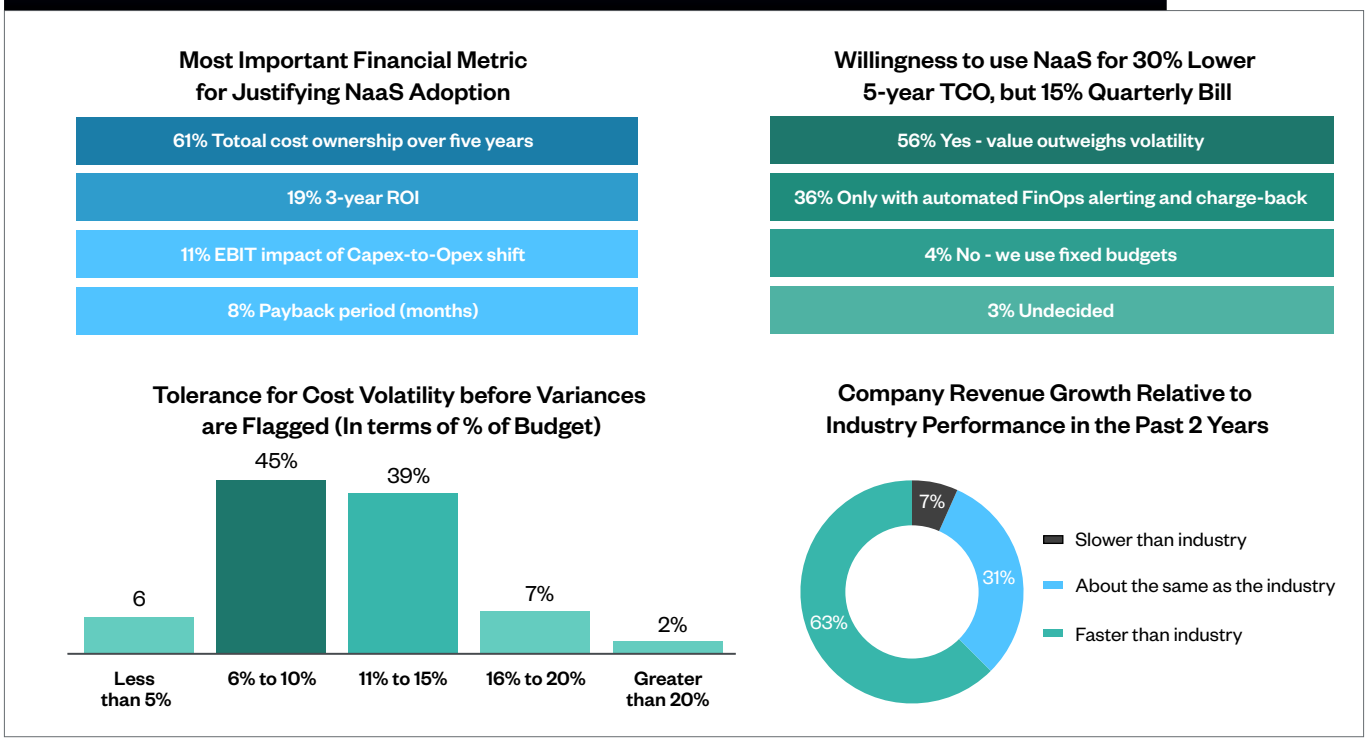
**Germany**
Deliberate and compliance-driven

**France**
Active in rollout, but trust-sensitive

## **Friction Point 3:** Cost volatility

The market has largely settled on an acceptable tolerance for cost volatility. Nearly half of enterprises (**45%**) flag variances once they reach **6 to 10%** of budget, while another **39%** draw the line at **11 to 15%**. Within those ranges most enterprises absorb fluctuations without escalation. Beyond them, finance becomes involved and without the right visibility and controls in place the conversation shifts from network strategy to explaining the spend. Decisions slow down, approvals take longer and strategic initiatives can lose momentum.

**NAAS ADOPTION IS EVALUATED THROUGH A LONG-TERM COST LENS WITH DEFINED LIMITS ON VOLATILITY**




## **Friction Point 4:** Talent shortage

The talent gap in NetOps and SecOps isn't new. **Thirty-seven percent** of enterprises cite it as the top external trend shaping their next network update cycle, more than any other factor. It appears as a consistent theme across every GTT-commissioned study, which suggests it's a structural condition of the market rather than a temporary staffing cycle.

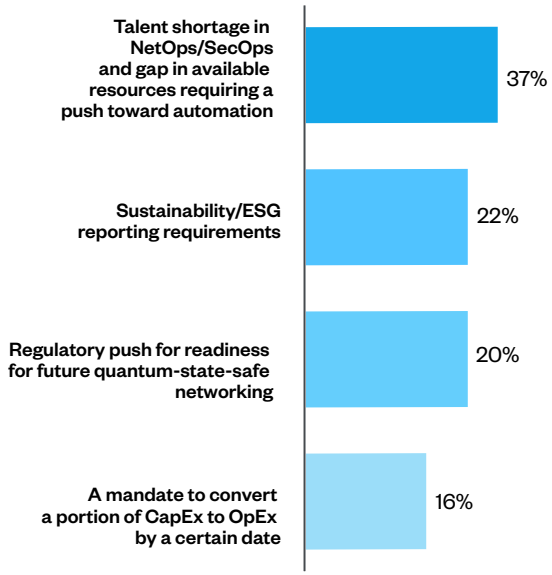
Enterprises can't hire their way out of it fast enough, so they're automating and outsourcing instead. Plans for network API and self-service skew toward portal-based models, with fewer organizations pursuing full end-to-end automation. **37%** prefer AI-driven automated remediation when network performance issues arise signalling that enterprises are engineering around the talent gap rather than waiting to fill it. The consistent growth in hybrid adoption points in the same direction: when internal teams can't cover the operational burden, managed services fill the gap.

"The GTT team works as an extension of our in-house IT team. We have effectively collaborated to ensure the integrity of the solution and are continuously making sure the solution aligns with our business goals.

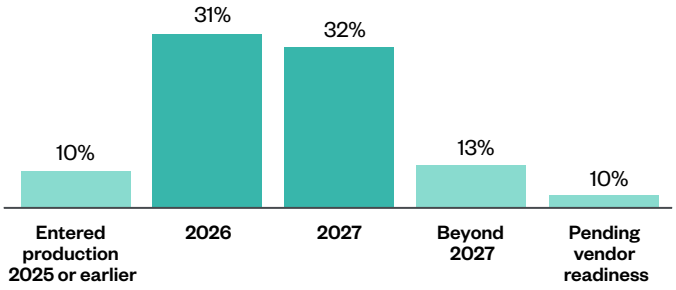
***CIO OF A LEADING GLOBAL CONFECTIONERY MANUFACTURER***

## NAAS ADOPTION IS EVALUATED THROUGH A LONG-TERM COST LENS WITH DEFINED LIMITS ON VOLATILITY

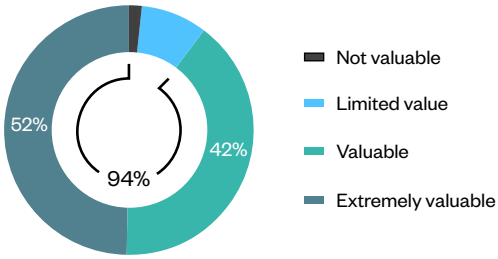
### External Trends Influencing the Next Network Update




### Target Date for First Production Post-Quantum VPN Tunnel




### Value of Immutable Audit Logs



# THE FINANCIAL CASE

**The friction points in the previous section are significant and expensive to address. But enterprises aren't pulling back from hybrid networking because of them. If anything, the financial data shows organizations making longer, more deliberate commitments to get it right.**

## The 5-year TCO lens

The most telling signal is the financial metric enterprises use to make the case to their boards. **Sixty-one percent** cite five-year total cost of ownership as the primary metric for justifying NaaS adoption. This is well ahead of three-year ROI (**19%**), EBIT impact of a CapEx-to-OpEx shift (11%) and payback period (**8%**). When **nearly two-thirds** of enterprises are taking a five-year view to justify a network decision, they're evaluating NaaS the way they'd evaluate any long-term strategic partnership.

A five-year TCO lens also extends to the provider, the support model and the management layer that sits on top of it. Enterprises are not just asking whether the platform is the right one today, but whether the provider will evolve alongside them over the life of the commitment. With 37% of enterprises citing talent shortages as the top external trend shaping their next network update, the question of how the network will be managed over that five-year horizon is an important part of the TCO calculation.

**93% of enterprises willing to absorb meaningful short-term volatility for long-term savings.**

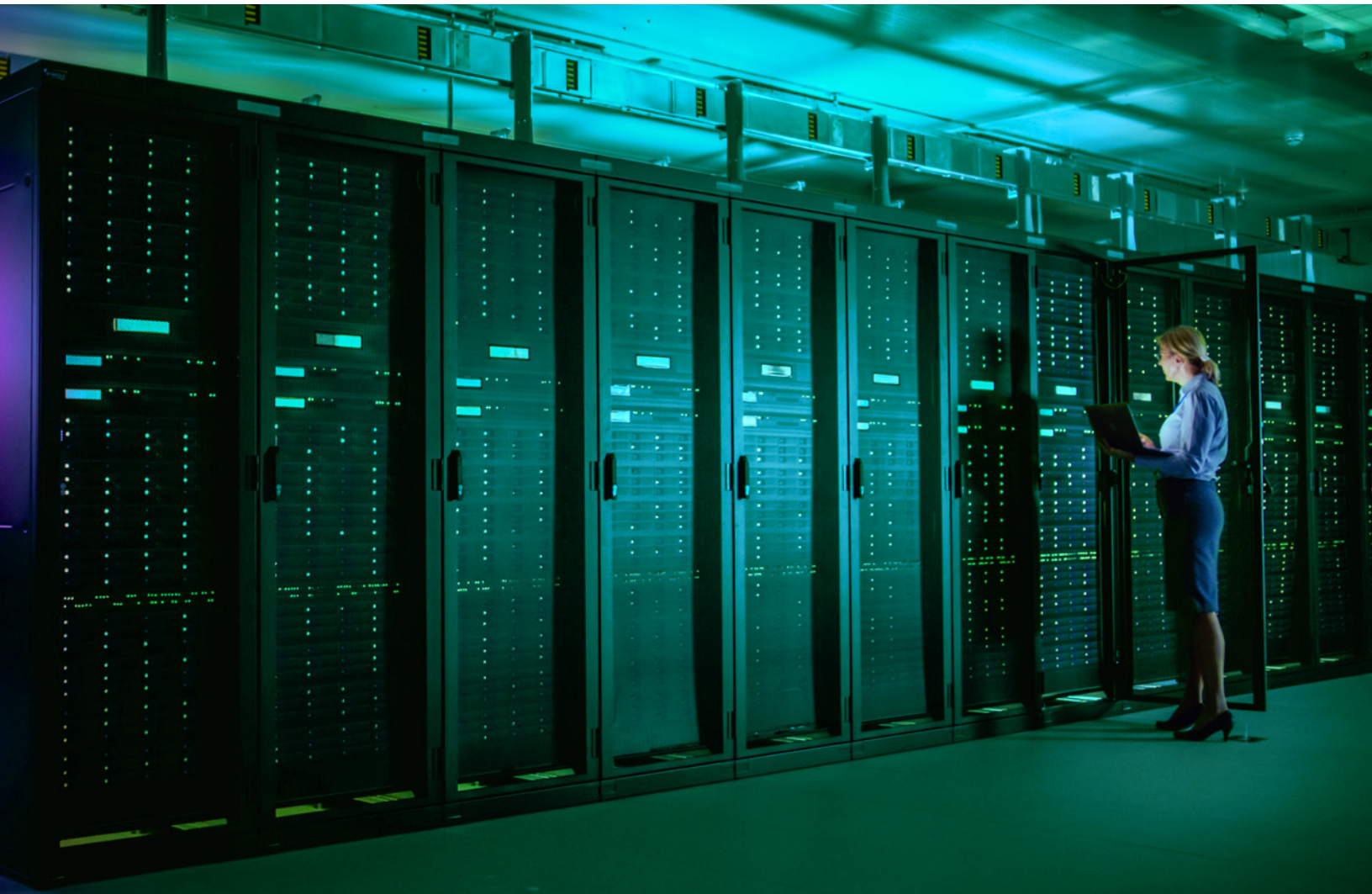
## How much volatility they'll accept and why

Committing to a five-year horizon doesn't mean enterprises are willing to absorb unlimited cost swings along the way. But what's notable is how far enterprises will stretch that tolerance when the long-term value case is strong enough. Fifty-six percent say they would accept up to **15%** quarterly bill swings in exchange for a **30%** reduction in five-year TCO. Another **36%** would accept the same tradeoff, provided automated FinOps alerting and chargeback mechanisms in place. Together, that's **92%** of enterprises willing to absorb meaningful short-term volatility for long-term savings.

That gives providers a clear mandate: the value case must be demonstrable over five years and the tools to manage short-term variability must come with it. Sixty-three percent of enterprises report their revenue growth has outpaced their industry over the past two fiscal years. For growing organizations, the network has to keep pace. New markets, new sites, new workloads and new users all land on the network first.

> "The network decisions you make in the next few years will be harder to reverse than you think. The enterprises that get this right will be the ones who chose their platform and partner with the same rigor they'd apply to any other long-term strategic commitment."

***FLETCHER KEISTER***
***CHIEF PRODUCT AND TECHNOLOGY OFFICER, GTT***



# *HYBRID IN PRACTICE: HOW INDUSTRIES ARE GETTING THERE*

**Hybrid is the default, but how organizations are getting there and what's driving urgency, differs significantly by industry. That variation often comes down to the type of problem being solved and who gets pulled into the room to solve it.**

Where compliance and security are the primary stakes, the CISO plays a central role. Where operational continuity is what's at risk, the teams responsible for operational continuity hold effective veto power over any network change that slows operations or output. Where cost structure and capital efficiency drive the conversation, the CFO is involved from the start. The decision maker shifts because what's at stake shifts. What's at stake shifts because each industry is running a different version of the hybrid problem.

What follows is how that plays out across four sectors where the dynamics are clearest.

## Manufacturing

Manufacturing presents one of the more complex decision-making environments in the dataset. Manufacturing organizations are especially likely to involve the CIO, but the teams responsible for keeping production lines running hold effective veto power over any change that could cause downtime. The dynamic shapes everything about how hybrid adoption unfolds in this sector.

Uptime and supply chain reliability are the dominant concerns, setting a high bar for any modernization initiative. Manufacturing organizations flag cost variances at **6-10%** of budget at a rate of **40%**, tighter than Healthcare (**25%**) and second only to Financial Services (**61%**). This is consistent with a sector where any unplanned cost requires justification against the operational priority of keeping production running. A network transition that introduces even temporary instability in a production environment carries hard costs and lost revenue that may far outweigh the operational benefits of moving faster. The result is a sector that moves deliberately because the consequences of getting it wrong are immediate and measurable in ways they aren't in other industries.

That caution isn't a barrier to hybrid adoption but it is a constraint on how hybrid gets implemented. NaaS is evaluated on whether it can be introduced without disrupting the environments that can't afford disruption. MNS anchors the parts of the network where reliability is non-negotiable. The transition happens, but on a timeline and in a sequence that keeps production risk off the table.

**Manufacturing organizations flag cost variances at 6-10% of budget at a rate of 40%, tighter than Healthcare (25%) and second only to Financial Services (61%).**

## Retail

The retail sector presents an interesting split. On one hand, retailers are significantly more likely than Financial Services and Technology firms to report running NaaS only — **26%** versus **6%** and **10%**, respectively — the highest NaaS-only rate of any sector in the dataset. On the other hand, the majority of retail organizations are still taking a combined approach or using MNS and for good reason.

Retail operates across hundreds or thousands of distributed sites, with fast provisioning, easy scaling and cloud-native integration all making NaaS a natural fit for new deployments. But distributed may also mean leanly staffed. When something goes wrong at a store location, there often isn't a local IT person to fix it. That's what makes managed services the operational layer that keeps retail stores running. The **26%** running NaaS only are getting the flexibility benefits of the model, but without managed services in place, reliability is difficult to sustain.

**26% of retail respondents run NaaS only. While they are getting the flexibility benefits of the model, without managed services in place, reliability is difficult to sustain.**

## Financial Services

Financial Services carries the strictest cost controls in the dataset. Organizations here are significantly more likely than Healthcare, Manufacturing or Retail to flag cost variances at **6-10%** of budget (**61% vs. 25%**, **40% a**nd **39%**, respectively). Financial Services organizations are also the most likely of any sector to include the CISO in NaaS/MNS decisions, reflecting an industry where security and compliance risk sit at the center of every infrastructure conversation.

Financial Services firms are planning to sunset legacy infrastructure faster than any other sector, with most targeting a 1-2 year timeline. Compliance pressure is a key driver, with **48%** of enterprises overall citing data residency and sovereignty requirements as a top compliance concern over the next 24 months. Financial services organizations do face some of the most prescriptive mandates in that space. DORA and PCI set specific requirements around operational resilience, data sovereignty and audit evidence that aging infrastructure may not be able to meet.

The combined approach here is also the clearest: always-on workloads like core banking and trading favor MNS reliability, while distributed branches and digital banking tiers are well-suited to NaaS flexibility.

**48% of financial services respondents cite data residency and sovereignty requirements as a top compliance concerns. Aging infrastructure may not be able to meet strict requirements such as DORA and PCI.**

## Healthcare

Healthcare networks are under more pressure than most. The shift to telehealth, the explosion of medical imaging data, and the growth of distributed and pop-up care models have placed demands on infrastructure that was built for text-based records and centralized facilities. The network has had to expand faster than most healthcare organizations planned for, in directions they didn't anticipate.

That expansion has made hybrid a necessity rather than a strategic preference. NaaS provides the flexibility and reach that distributed care models demand. MNS anchors the environments where reliability and compliance are non-negotiable. Patient data security under HIPAA and other mandates requires audit-ready controls, consistent performance and the kind of service assurance that a purely consumption-based model can't guarantee on its own.

Healthcare organizations are also thinking further ahead on security than their legacy transition timelines might suggest. They are the most likely sector to target 2026 for their first production post-quantum VPN tunnel, ahead of Financial Services, which is significantly more likely to target 2027. That's notable given that healthcare tends toward longer legacy transition timelines overall, with most organizations expecting a 3–5-year sunset horizon compared to 1-2 years for Financial Services and Technology.

**Healthcare networks are under more pressure than most. The network has had to expand faster than most healthcare organizations planned for and in directions they didn't anticipate.**

## The fastest-growing organizations in this study run their networks differently from their slower-growth peers. That gap shows up across several dimensions.

While five-year TCO is the dominant board metric across the full sample, the fastest-growing companies are more likely to make the case to their boards on EBIT impact, arguing that moving from CapEx to OpEx improves earnings directly, not just long-term costs. **Twenty-one percent** of faster-growth companies use EBIT impact as their primary metric, compared to just **5%** among slower-growth peers. That financial orientation tracks with how they're actually running the network. Faster-growing organizations are significantly more likely to rely exclusively on NaaS today and significantly more likely to be planning full end-to-end network automation with no manual intervention.

Organizations that favor NaaS aren't necessarily less risk-averse; they're often optimizing for speed, flexibility and operational modernization. Meanwhile, organizations that lean toward MNS are typically optimizing for operational assurance, compliance and accountability. The emerging trend is not NaaS versus MNS, but using both in the places where each delivers the greatest business value.

| Organizations leaning more toward NaaS | Organizations leaning more toward MNS |
|---|---|
| Prioritize agility and speed | Prioritize operational assurance |
| Comfortable with self-service and automation | Prefer provider-led management |
| Focus on rapid deployment and innovation | Focus on compliance, governance and predictability |
| Optimize for flexibility | Optimize for reliability |

# WHAT GOOD LOOKS LIKE

**Every friction point identified in this report has a provider-side answer. What enterprises need from a network provider maps directly onto where hybrid gets hard.**

## On observability

The observability requirement is straightforward: full visibility across both the NaaS and MNS layers, treated as a single environment rather than two separate ones. That means real-time traffic monitoring that doesn't stop at the boundary between providers and AI-driven automated remediation that can identify and respond to performance issues without waiting for a human to locate the source.

Thirty-four percent of enterprises already prefer AI-driven auto-scale and path reselection as their primary remediation approach for performance dips and another 37% use a combination of approaches depending on site criticality. The direction is clear: enterprises want remediation that moves faster than manual intervention allows.

## On security and compliance

The security and compliance requirement has three distinct components.

1. **Audit-ready evidence**
   This means detailed activity records that can stand up to close inspection. Ninety percent of enterprises require high or very high audit evidence from their providers and **94%** consider provider-maintained immutable logs valuable or extremely valuable.
2. **Encryption key management**
   Enterprises expect to retain meaningful control over their own keys. **Forty-five percent** want full ownership and **46%** want a shared responsibility model where they own the keys but the provider manages them.
3. **Post-quantum readiness**
   **Sixty-three percent** of enterprises are targeting 2026-2027 for their first production post-quantum VPN tunnel. Providers that aren't on that roadmap are already falling behind a significant portion of their customer base.

## On cost volatility

Enterprises have a clearly defined cost variance tolerance of 6-15% of budget. What they need from providers is the tooling to stay within it.

Automated FinOps alerting that flags variances before they escalate and chargeback mechanisms that give finance teams real-time visibility into consumption against budget are the practical controls that make cost volatility manageable. Thirty-six percent of enterprises say they would only accept the TCO tradeoff of hybrid if automated FinOps controls are in place.

## On talent shortage

The talent gap in NetOps and SecOps isn't something enterprises expect to solve internally. Thirty-seven percent cite it as the top external trend shaping their next network update cycle. The growth in automation investment suggests most have stopped waiting for the hiring market to catch up. Automation covers only part of the gap.

What enterprises need from a provider is operational coverage for the parts automation can't yet handle: managed services that absorb the day-to-day burden their internal teams don't have capacity for and expertise in NetOps and SecOps that would take years and significant investment to build in-house.

# THE PATH FORWARD

**The findings in this report show that hybrid networking is where enterprise network strategy has landed. The organizations managing it well have moved past the question of whether to run NaaS and MNS together and are focused on how to run the combination well. That means a deliberate architecture that puts each model to work on the problems it is best suited to solve.**

The friction points in this report—observability gaps, rising compliance demands, cost volatility and talent shortages—do not have to slow you down. What separates the enterprises managing hybrid well is a provider that delivers unified visibility across both environments, audit-ready security controls, the financial transparency to keep cost variance within tolerance and the operational expertise to cover what internal teams can't.

So, what are the next steps? Take the friction points covered here and pressure-test your current environment against them. Take the **What Good Looks Like** section and hold your provider against it. The gaps you find are your starting point.

GTT works with enterprises at every stage of this journey. If you'd like to benchmark your environment or explore what a hybrid networking roadmap looks like in practice, contact us at **gtt.net.**

GTT is a leading networking and security as a service provider for multinational organizations, simply and securely connecting people and machines to data and applications — anywhere in the world. We serve thousands of organizations, bringing together the right people, partners and technology to reduce the burden on IT teams and solve the most pressing networking and security challenges. Built on our top-ranked global Tier 1 network, GTT Envision is a single global technology platform to connect, orchestrate, virtualize and automate enterprise networks, enabling customers with consumable solutions to achieve business missions and meet ongoing demand when, where and how needed. Our portfolio includes SASE, SD-WAN, security, internet, voice and other connectivity options, complemented by a suite of professional services and exceptional sales and support teams in local markets around the globe. We partner with our customers to deliver Greater Technology Together. For more information, visit gtt.net

GTT Greater Technology Together



ManServ_NaaSvMNSWtPaper_GGMCM-4172_v1_07102026