T Business

What's next for networks

Manage performance and reclaim sovereignty: how IT and security leaders can reduce costs



Connecting your world.

Table of Contents

Executive Summary 3

Introduction 4

The reality in 2026: Three challenges to master 5

Consolidate, don't stack: LAN, WAN, and security as one 6

Cloud connectivity—an underestimated cost driver 7

Why integrated platforms (SASE) are still recommended 8

Network-level security: Control where traffic originates 9

From observation to implementation: Developing architecture strategically 10

Create clarity, not perfection 10

A few principles, rigorously implemented 10

Develop the architecture in stages 11

Make progress measurable 11

Putting sovereignty in context: Choose control over ideology 12

Regulation as an opportunity: A pragmatic approach to NIS2 13

Secure networking with Deutsche Telekom: Single-source networking and security 14

More tools is not the solution: Successful transformation strategies 15

Conclusion: Less effort, more control 16

Sources 16

Executive Summary

Most companies don't see the problem until it gets expensive. New AI applications don't react fast enough, security policies no longer apply consistently, cloud costs rise unexpectedly, and security audits keep revealing vulnerabilities. This shows how digitalization rarely fails for want of technology. Instead, it fails because organizations can no longer manage what they have built. What connects these symptoms is not the individual application or service in most cases, but rather the way they are connected. The network resembles a system that has grown over the years: functional, but increasingly difficult to keep track of.

In many companies, network and security landscapes are the result of countless individual decisions. Different solutions exist side by side, each one sensible on its own yet, in their entirety, difficult to manage. Teams can only see parts of the picture at a time, responsibilities are distributed, and every change carries risk.

The growing use of cloud services and distributed applications has exacerbated the situation. Data no longer moves along clear structures, but flows dynamically between sites, clouds, and users. If organizations cannot see and steer the environment from a central location, understanding how performance, risks, and costs relate to one another becomes difficult.

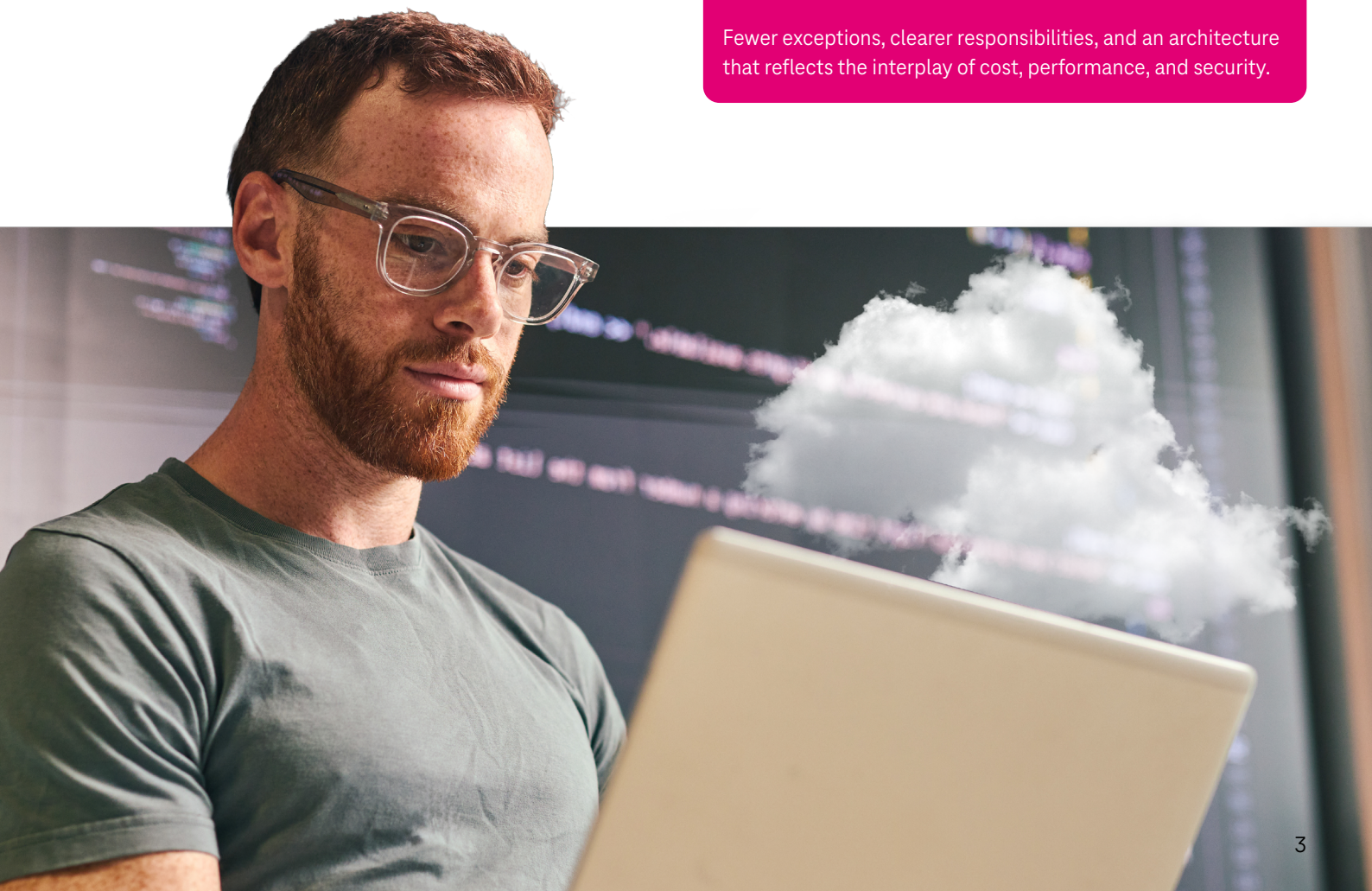
Under these circumstances, networking, security, and the cloud can no longer be considered in isolation. What matters is building the architecture in such a way that it remains controllable as an integrated whole. In this context, consolidation does not primarily mean reduction, but rather integration by bringing together functions, platforms, and control logic.

Companies that make progress in this regard take one step at a time. They follow a few clear principles and evolve their infrastructure during live operations rather than rethinking it in isolated projects.

This white paper draws on real-world experience to show how you can reduce complexity and regain control.

The result is a controllable network

Fewer exceptions, clearer responsibilities, and an architecture that reflects the interplay of cost, performance, and security.



Introduction

When applications slow down or cloud costs rise unexpectedly, the cause is often not an individual aspect but rather the overarching system. In many companies, it's not an individual tool causing problems, but rather the entire legacy network infrastructure straining under its own complexity. Technology is not the bottleneck. The ability to manage and control the infrastructure is.

This situation is the result of a fundamental shift. Corporate networks have evolved from clearly bounded structures into distributed architectures. Cloud services, mobile applications, and hybrid work have dissolved fixed organizational boundaries and fragmented IT across different geographic locations.

This has also changed the logic of network traffic and security. Connections now run between clouds, sites, and users rather than along clearly defined paths. Security that only focuses on a few select areas is no longer sufficient; it must cover the entire architecture.

As a result, the network takes on a new role. It no longer handles only transport, but rather the central control and enforcement layer for performance, cost, and security policies. Architecture decisions directly shape governance and operations.

For CIOs, CISOs, and CTOs,
this raises a critical question:

How do you design a distributed, dynamic environment that stays visible and controllable as a single system?



The reality in 2026
Three challenges to master

IT leaders are currently facing multiple pressures simultaneous that directly shape how organizations design networks and implement security strategies.

Costs

Budgets are stagnating or shrinking as IT systems become more complex. Departments now compete for scarce funds, and investments go primarily to more immediate business needs (such as AI projects) rather than “invisible” foundational technology. At the same time, cloud costs are exploding, in particular due to data-intensive AI and multi-cloud deployments. Cloud providers namely charge large sums for outbound traffic (egress), resulting in expenses that are difficult to predict.



People

Small and mid-sized IT teams are managing heterogeneous IT estates with legacy dependencies. Qualified professionals are scarce, and the expertise that exists is fragmented across a multitude of tools and isolated point solutions. A significant share of the available time goes into day-to-day operations and routine networking and security tasks. With resources tied up this way, there is little room to automate consistently or to push IT projects with higher value and direct business relevance. As a result, architectures have, in many cases, not evolved fast enough to keep up with the strategy.

Regulations and reporting obligations

Regulations such as EU NIS2 and DORA are pushing cybersecurity onto the board’s agenda. Companies must analyze risks in depth, document their processes thoroughly, and produce evidence of compliance. A fragmented architecture with many point solutions increases the amount of work involved several times over: disparate reporting tools, scattered logs, and unclear ownership make it harder to keep track of all the moving parts and show who is accountable for what. NIS2 explicitly assigns risk management and responsibility to the organization’s leadership. Without integration, this bar is impossibly high.

All three pressures share a common blind spot: the network. Historically, the corporate network has blended into the background of day-to-day operations because it appears stable. Yet all the organization’s data come together here with implications for costs, security, and performance. Without a comprehensive network strategy, inefficient parallel structures arise. Costs spiral out of control (for example through cloud traffic), and resilience suffers. The next section looks at a central pattern that successful companies use to meet these challenges.

Consolidate, don’t stack
LAN, WAN and security as one

Consolidating the network and security landscape is a key lever for gaining efficiency and control. Successful companies are moving away from siloed thinking and viewing LAN, WAN, and security not as separate objects but as a unified architecture.

For comparison: in other areas of the company, consolidation has long been standard. Consider integrated ERP or CRM systems that used to consist of dozens of individual solutions. In contrast, network and security infrastructures have grown fragmented at many companies. A consolidated approach brings tangible benefits:

Cost reduction

Fewer different vendors and individual products mean lower license and maintenance costs. Duplicate spending can be avoided, and a consolidated approach cushions current price increases.

Reducing the burden on IT teams

With fewer tools, operational complexity decreases. Automation is more effective across a unified platform, and the team can focus squarely on a consolidated environment, instead of getting lost in countless specialized tools.

Greater transparency

With an integrated network security platform, all data flows and policies are available consistently. Blind spots disappear because you no longer need to monitor multiple systems at once. Documentation and audit work (for NIS2, etc.) decreases because compliance is consistently visible.



Organizations that treat networking, security and cloud connectivity as a unit unlock potential that cannot be attained through isolated projects. Transitioning from piece-meal optimizations to a coherent architectural approach has a tangible impact on costs, operations, and security. What matters is less the specific integration philosophy than whether the available platforms can actually live up to that ambition in practice.

The underestimated cost lever
Cloud connectivity

The cloud bill goes through the roof and no one knows why—an all-to-common scenario. Workloads are stable, usage remains constant, and yet costs spike unexpectedly. Companies often look for the causes in instances or storage, while the actual driver remains invisible: traffic between clouds and company sites.

For a long time, internet connectivity was considered good enough from a cost perspective. Network costs hardly mattered. But this assumption is quickly losing its validity. Because the fundamental rules of the game are changing.

Spiking egress fees

With AI workloads, multi-cloud architectures, and huge data lakes, outbound traffic between clouds and sites is surging. Analysts observe that egress and data transfer fees account for a significant and frequently underestimated share of total cloud costs, especially once data storage, processing, and use are geographically decoupled. As a result, many companies see their cloud costs spike due to data transfer charges.

Cloud on-ramp decisions affect both cost and performance

These additional costs frequently surface on the cloud bill—most notably through rising egress charges for outbound data transfer. As data volumes grow and organizations adopt multi-cloud strategies and AI workloads, the choice of cloud connectivity becomes increasingly consequential. Beyond access over the public internet, cloud providers also offer dedicated connectivity options that can affect both performance and cost efficiency.

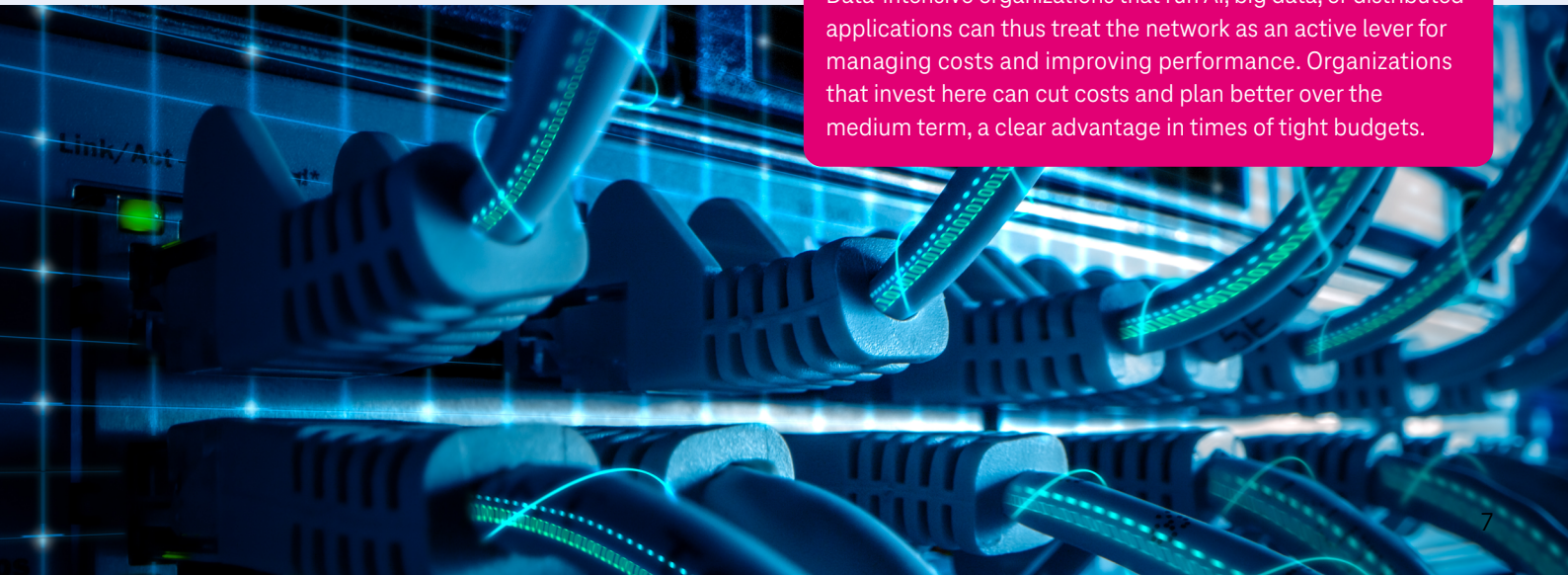
Cloud on-ramps—the many paths to the cloud

Cloud providers such as Deutsche Telekom, Microsoft and AWS offer dedicated connections in addition to access via the public internet. Deutsche Telekom and AWS, for example, call this service *Direct Connect.* To implement these connections, cloud providers work with certified connectivity providers that establish the link between the corporate network and the cloud.

Predictable costs, improved performance

Private cloud connectivity provides dedicated access to the cloud that isn't shared with other tenants. This delivers stable latency, guaranteed bandwidth, and higher availability—particularly for data-intensive applications and AI workloads. While this access incurs additional costs from both cloud and connectivity providers, the investment can pay off technically and economically in scenarios involving high data volumes or stringent performance and availability requirements.

Data-intensive organizations that run AI, big data, or distributed applications can thus treat the network as an active lever for managing costs and improving performance. Organizations that invest here can cut costs and plan better over the medium term, a clear advantage in times of tight budgets.



Why integrated platforms (SASE) are still recommended

Having more security tools no longer equates to better security. The opposite is in fact true at many companies. Every additional specialized solution makes integration harder, increases operational risk, and slows response times. Policies are applied inconsistently, and visibility is fragmented across multiple consoles.

This is precisely why the market is shifting. Integrated platforms bundle network and security functionality in a shared operating model with central management. SASE (Secure Access Service Edge) is emblematic of this approach: not a new technology, but a coherent consolidation of proven building blocks, namely SD-WAN with network-based security. The three developments below reinforce this consolidation trend.



Vendors expanding their portfolios

Networking vendors are investing heavily in security features while security vendors are integrating technologies such as SD-WAN, routing, or Wi-Fi into their offerings. This is giving rise to platforms that offer a broad range of capabilities.

Suite offerings with broad coverage

Many integrated solutions now cover a very wide functional scope ranging from connectivity to access control. Numerous specialized tools can be eliminated without creating a critical gap.

Pragmatic 90 percent solutions

Integrated platforms deliver sufficient protection and performance for most use cases. Not every organization needs the best possible specialized solution if a simplified overall platform meets roughly 90 percent of security requirements and remains operable in the process. The remaining 10 percent of specialized needs can often be addressed specifically, without making the architecture significantly more complex.

Adding more tools does not equate with progress. What does is a well-orchestrated mix of the right tools. Integrated platforms eliminate gaps between networking and security, because it is precisely those gaps that cause most of the vulnerabilities and problems in practice.

Network-level security
Control where traffic originates

Security today is no longer achieved at isolated points, but across the entire flow of data. In modern network architectures, controls must be applied where data originates and where it is processed. This covers everything from endpoints, LANs, WANs, and cloud connectivity.

In contrast to conventional perimeter security, the architecture no longer concentrates security at a few perimeter points but instead anchors it throughout the distributed environment. This makes it possible to enforce policies regardless of the workload's location. This shift also changes the control logic. The focus is no longer on individual components, but rather on the interplay of connections, identities, and policies throughout a distributed environment.

Modern network architectures have these central principles in common

- **Zero Trust Network Access (ZTNA)**
  Access decisions are made based on context, not granted across the board.
- **Segmentation and micro-segmentation**
  These techniques structure networks to limit dependencies and keep the impact of disruptions manageable.
- **Secure cloud access**
  Security policies apply regardless of where processing takes place, including for cloud services.
- **Encryption with visibility**
  Encryption combines with carefully defined visibility mechanisms.
- **Central analysis of security telemetry**
  This involves aggregating operational data and preparing it for analysis to gain a coherent picture of the security situation.

These principles show how you can use architecture to integrate security with the ability to manage the environment. However you choose to define them, the most important thing is their rigorous implementation in existing environments.



From observation to execution
Developing architecture strategically

Successful companies no longer treat networking and security architecture as a purely technical undertaking, but rather as a responsibility of company leaders. If you treat the network as a strategic lever to optimize cost, performance, *and* security, you can reduce complexity and build resilience without overwhelming the organization with large-scale projects.

Effective strategies have this in common: instead of constantly adding new tools, they concentrate on the architecture—step by step, pragmatically, with a consistent focus on control.

Create clarity, not perfection

The starting point is not an elaborate full audit, but rather a purposeful shift in perspective. Key questions to ask include following.

- Which data flows are critical for production or the business?
- Where do exceptions arise, and why?
- Which dependencies are we consciously accepting?

What matters is relevance, not completeness. The goal is direct visibility into the areas where it's possible to have a direct impact on costs, risks, and outages. This creates the basis for an architecture that not only protects systems, but also influences how they operate.

Explore real-world examples

Discover how organizations are successfully modernizing their network and security architecture.

A few principles, rigorously implemented

Regardless of industry or starting point, these are the principles successful businesses follow.

- **First the policy, then the tool**
  Rules are clearly defined and enforceable—independent of the technology used.
- **Segmentation to simplify**
  Segments limit complexity and make networks more easier to manage.
- **Identities instead of network boundaries**
  The architecture controls access based on context and identity, not mere network membership.
- **Resilience sets the bar**
  Failure scenarios are planned for, not assessed after the fact.
- **Make sovereignty measurable**
  Dependencies and exceptions are transparent and manageable.
- **Application-specific**
  The network prioritizes traffic according to application.

These principles create clear guide rails for architecture and operations, which is especially important when resources are limited.

Develop the architecture in stages

Instead of going for a big bang, successful companies rely on a staged approach. The following four-phase process has proven effective:

Phase 1: Create transparency

Make data flows, exceptions, and responsibilities visible

The goal: *Clarity about the current state and gaps in control*

Phase 2: Establish control

Implement initial segmentation, enforce policies close to the network, and implement basic logging

The goal: *Make uniform policies effective where traffic originates*

Phase 3: Anchor resilience

Establish fallback mechanisms and redundancies, rehearse emergency operations

The goal: *Maintain the ability to respond even under stress.*

Phase 4: Standardize and automate

Unify the architecture, automate routine processes, optimize the operating model.

The goal: *Fewer exceptions, more scalability and repeatability*

This iterative approach delivers rapid successes without creating an operational burden. Each stage makes the environment easier to manage and creates the foundation for the next.

Make progress measurable

You can can't manage what you don't measure. Successful teams rely on a few meaningful KPIs that both IT teams and management can understand. Examples include the following.

- **Exception rate**
  Number of active policy exceptions (and their average duration)
- **Segment coverage**
  Share of critical data flows passing through defined segment boundaries
- **Policy consistency**
  Share of sites/cloud connections with an identical baseline policy
- **Time-to-isolate**
  Time to isolate a compromised segment (in the event of an incident)
- **Compliance scope**
  Number of systems in the audit scope (and its trend over time)
- **Dependency index**
  Number of identified single points of failure along the central communication paths (provider, identity, DNS, etc.)

KPIs like these translate technical reality into visibility for management. They make progress (or gaps) tangible and create a shared understanding of success across the organization.

Putting sovereignty in context
Choose control over ideology



Discussions about *digital sovereignty* are often ideologically loaded. In practical terms, the topic comes down to **a few key questions**:

Who operates the network—and from where?

Do trustworthy teams or contractually bound service providers operate all critical network components? Do those operators run the system within a clearly defined jurisdiction and according to specified requirements such as site requirements or background checks? Sovereignty here means operations and responsibilities are clearly governed and fully traceable, regardless of whether they are handled internally or externally.

Who has access to keys and policies?

Is authority over cryptographic keys, certificates, and policy stores retained in-house or transferred to third parties? A sovereign network keeps control over critical security control components, in particular over key material and policies.

Are paths, dependencies, and exceptions visible?

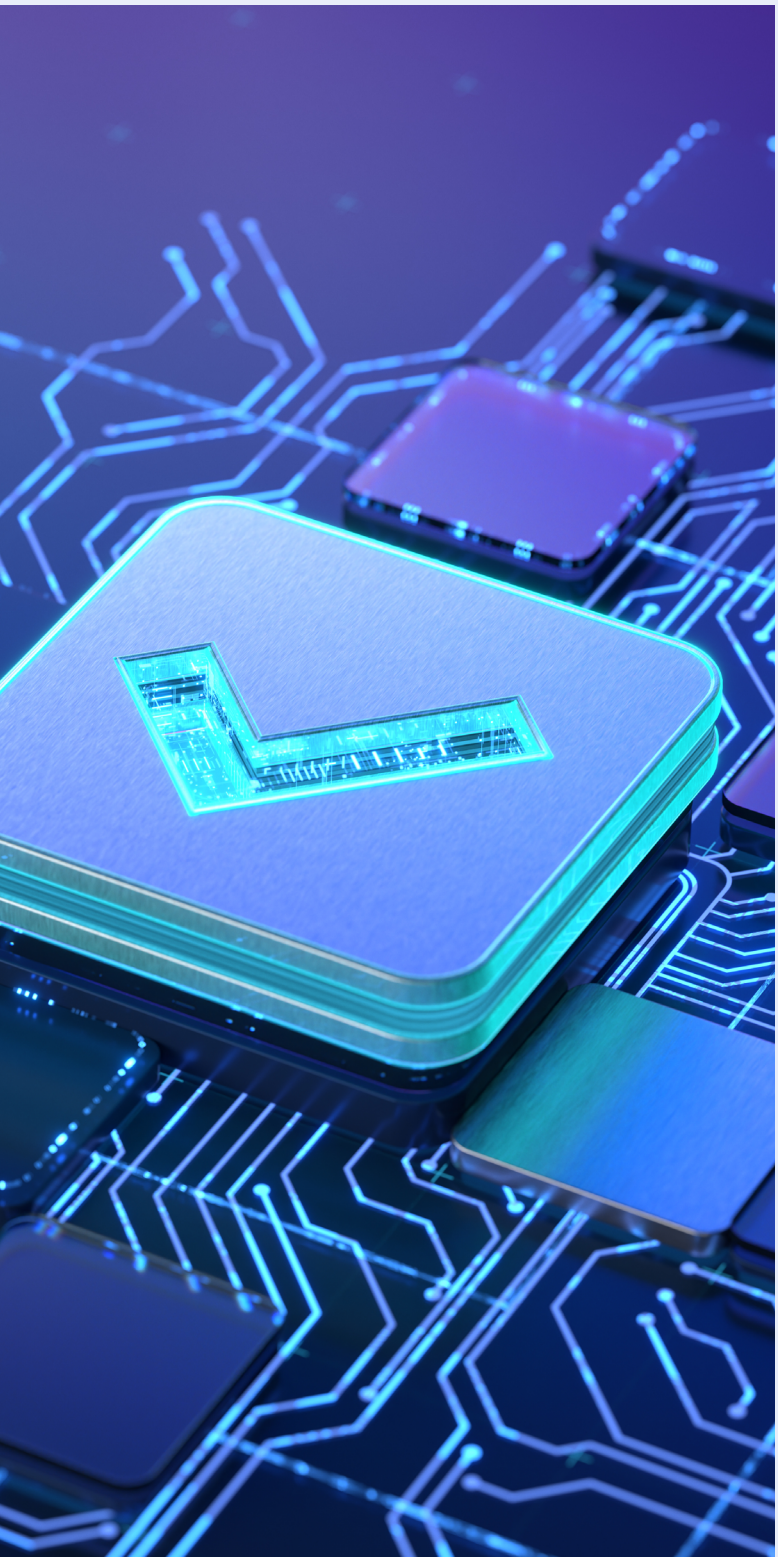
For every connection, can you trace which providers, countries, and systems it passes through? Can you further minimize single points of failure? Are deviations from defined security policies fully documented, approved, and temporary? Visibility into dependencies is essential. Without it, organizations cannot govern their environments and truly achieve sovereignty.

These are main pragmatic aspects of sovereignty. It is not about complete independence, but about control and choice. A sovereign network architecture puts the organization in the driver's seat.

Regulation as an opportunity
A pragmatic approach to NIS2

Regulations often appear to be burden. But organizations can also use them to drive improvements. The EU's NIS2 directive, for example, mandates a thorough cyber strategy review.

Organizations can channel that momentum to drive internal change rather than treating NIS2 as just a source of regulatory pressure. A consolidated secure networking approach directly addresses several NIS2 obligations:



Easier documentation

Fewer heterogeneous systems means less time spent on reporting. A consolidated platform makes it much easier to document network and security policies, changes, and incidents as well as present them to auditors.

Clear accountabilities

NIS2 requires clear responsibilities and reporting lines. In an integrated architecture, network and security responsibilities remain distinct. It's possible to name the specific people who are responsible for data flows and policies while monitoring compliance.

Traceability and control

Central telemetry and monitoring grant companies complete visibility across all communication paths and security controls. Metrics such as policy compliance that cover all sites or time-to-detect for incidents are available on demand. Central telemetry and monitoring thus transform compliance into a management tool: you gain control, not just a bunch of compliance check boxes.

An integrated secure networking strategy turns the equation on its head. More challenging requirements can be met with less overall complexity because integration boosts efficiency. Regulation no longer holds back progress, becoming instead a driver of sound architectural decisions.

Secure Networking with Deutsche Telekom
Single-source networking and security

Today's biggest operational risks arise not within individual technologies, but at their interfaces. Network security gaps and incomplete integration of cloud and operations complicate governance and increase risk. This is exactly where integrated secure networking comes in.

Deutsche Telekom combines network operations and security services in a unified operating model. While many providers deliver connectivity and security separately, Deutsche Telekom integrates security functions directly into the network. These are not add-ons, they're integral network services.

The portfolio covers access networks, WAN, cloud connectivity, central security, and compliance capabilities. Connections and policies work in concert and follow clear responsibilities, rather than requiring coordination across multiple systems.

Others recognize the value of this integrated approach as well: The IDC MarketScape "Worldwide Managed SD-WAN Services 2025" vendor assessment recognizes Deutsche Telekom as a Leader and specifically highlights the combination of global connectivity, SD-WAN management, and integrated security.

Thinking about networking and security as one proves its worth both operationally and in the market.



More tools is not the solution
Successful transformation strategies

Now let's take a look at how pioneering companies have approached this. Their transformation projects follow a surprisingly similar trajectory, breaking sharply with conventional "invest more" and "add more tools" strategies:

End-to-end instead of silos

Successful IT teams view data flows end-to-end. They make decisions about cloud, WAN, LAN, and security with an awareness of how these domains interconnect. This produces architectures with significantly fewer system boundaries and breaks in continuity, making the environment both more secure *and* easier to steer.

Fewer tools, more integration

Instead of layering new products on top of existing ones, these companies deliberately reduce the number of components. They consolidate capabilities into integrated platforms. Every interface eliminated means fewer potential mistakes and less operational effort. Even small teams can maintain full visibility this way.

Develop the architecture in stages

None of the successful organizations reached its target architecture with a single big bang. What they share is an iterative approach in manageable stages. They first obtain a clear picture of the status quo; then they make the underlying architecture choices (segmentation, enforcement points, identity-based control). After that, they layer in resilience mechanisms piece-by-piece before standardizing and automating so everything scales. This *learn-as-you-go* approach keeps the company agile and delivers tangible improvements fast instead of bogging it down in multi-year transformation projects.

Observe, don't dictate

The above methods are grounded in real-world practice, not academic theories. The implicit message is: take your blueprint from successful architectures and don't blindly follow whatever hype happens to be trending. This is how Deutsche Telekom's consulting practice works, too: recommendations are always anchored in best practices.



Conclusion
Easier to manage with less effort



Technological capabilities will continue to expand, while budgets, people, and time remain limited. Success therefore depends not on the number of solutions deployed but on how well solutions can be managed. The decisive lever lies not in adding further components, but in reducing complexity and making interdependencies manageable.

Secure networking describes an architectural approach to this challenge: organizations design network, security, and cloud as one interconnected system. The goal is not to maximize functionality, but to make the environment transparent, assign clear responsibilities, and maintain control of operations. Consolidation, above all, means less fragmentation and a clearer picture of how data flows, access, and costs relate to one another.

Key takeaways

- **Consolidation facilitates management and lowers costs**
  Fewer platforms and specialized solutions reduces both expenditures and the complexity of day-to-day operations while cutting the amount of time teams spend coordinating.
- **Integration creates stable operating models**
  Uniform processes and clear responsibilities take pressure off teams and form the basis for consistent governance.
- **Networks evolve from transport to management layer**
  Through visibility and deliberate connectivity choices, the network can help to actively manage performance, cost, and resilience.
- **Architecture over security**
  when organizations design networking and security as a unified whole, control over data flows and access is structurally anchored, not an afterthought.

This moves the focus away from piecemeal optimization and toward an establishing clearly-defined strategies that make the architecture easier to manage. Rethinking networking means recognizing it as an integral part of your governance and security strategy.

The result is not more complexity, but a more coherent architecture

Fewer exceptions, clearer responsibilities, and a system that actively manages costs and risks – rather than reacting to them.

Sources:
Cloud Costs & Cost-Effectiveness
- Wasabi
- Gartner Magic Quadrant for Cloud Financial Management Tools

Network & SASE Market
- Gartner Magic Quadrant for SASE Platforms 2025
- IDC MarketScape Worldwide Managed SD-WAN Services 2025

Transformation & Target Architecture
- Gartner Strategic Roadmap for SASE Convergence 2025

Contact us for a personal consultation.

Contact
Go to contact form
www.geschaeftskunden.telekom.de

Publisher
Deutsche Telekom
Geschäftskunden GmbH
Landgrabenweg 149
53227 Bonn, Germany

Connecting your world.

Deutsche Telekom GmbH | 06/2026