T Business

Netze weiterdenken

Performance steuern und Handlungsfähigkeit zurückgewinnen: Wie Verantwortliche für IT und Security Kosten senken können



Connecting your world.

Inhaltsverzeichnis

Executive Summary 3

Einleitung 4

Die Realität 2026: Drei Herausforderungen, die es zu meistern gilt 5

Konsolidieren statt Addieren: LAN, WAN und Security zusammendenken 6

Der unterschätzte Kostenhebel: Cloud Connectivity 7

Warum integrierte Plattformen (SASE) heute empfehlenswert sind 8

Netznahe Sicherheit: Kontrolle die dort greift, wo Traffic entsteht 9

Von der Beobachtung zur Umsetzung: Architektur gezielt weiterentwickeln 10

Klarheit schaffen – nicht Perfektion 10

Wenige Prinzipien, konsequent umgesetzt 10

Architektur in Etappen entwickeln 11

Fortschritt messbar machen 11

Souveränität richtig einordnen: Kontrolle vor Ideologie 12

Regulierung als Chance: NIS2 pragmatisch nutzen 13

Secure Networking mit der Telekom: Netzwerk und Sicherheit aus einer Hand 14

Noch mehr Tools ist nicht die Lösung: Erfolgreiche Transformationsstrategien 15

Fazit: Weniger Aufwand – mehr Steuerbarkeit 16

Quellen 16

Executive Summary

Die meisten Unternehmen erkennen das Problem erst, wenn es teuer wird: Neue KI-Anwendungen reagieren nicht schnell genug, Sicherheitsregeln greifen nicht mehr konsistent, Cloud-Kosten steigen unerklärlich oder Security Audits zeigen immer wieder Schwachstellen. Dann zeigt sich, dass Digitalisierung selten an fehlender Technologie scheitert, sondern an fehlender Steuerbarkeit. Was diese Symptome verbindet, ist meist nicht die einzelne Anwendung oder der einzelne Service – sondern die Art, wie sie miteinander verbunden sind. Das Netzwerk gleicht einem System, das über Jahre gewachsen ist – funktional, aber zunehmend schwer zu überblicken.

In vielen Unternehmen sind Netzwerk- und Security-Landschaften das Ergebnis zahlreicher Einzelentscheidungen. Unterschiedliche Lösungen existieren nebeneinander, jede für sich sinnvoll, in Summe jedoch schwer zu steuern. Transparenz entsteht nur fragmentarisch, Verantwortlichkeiten sind verteilt, und Änderungen werden zum Risiko.

Mit der zunehmenden Nutzung von Cloud-Services und verteilten Anwendungen hat sich diese Situation weiter verschärft. Daten bewegen sich nicht mehr entlang klarer Strukturen, sondern wandern dynamisch zwischen Standorten, Clouds und Nutzern. Ohne zentrale Sicht und Steuerung wird es schwer, Performance, Risiken und Kosten im Zusammenhang zu verstehen.

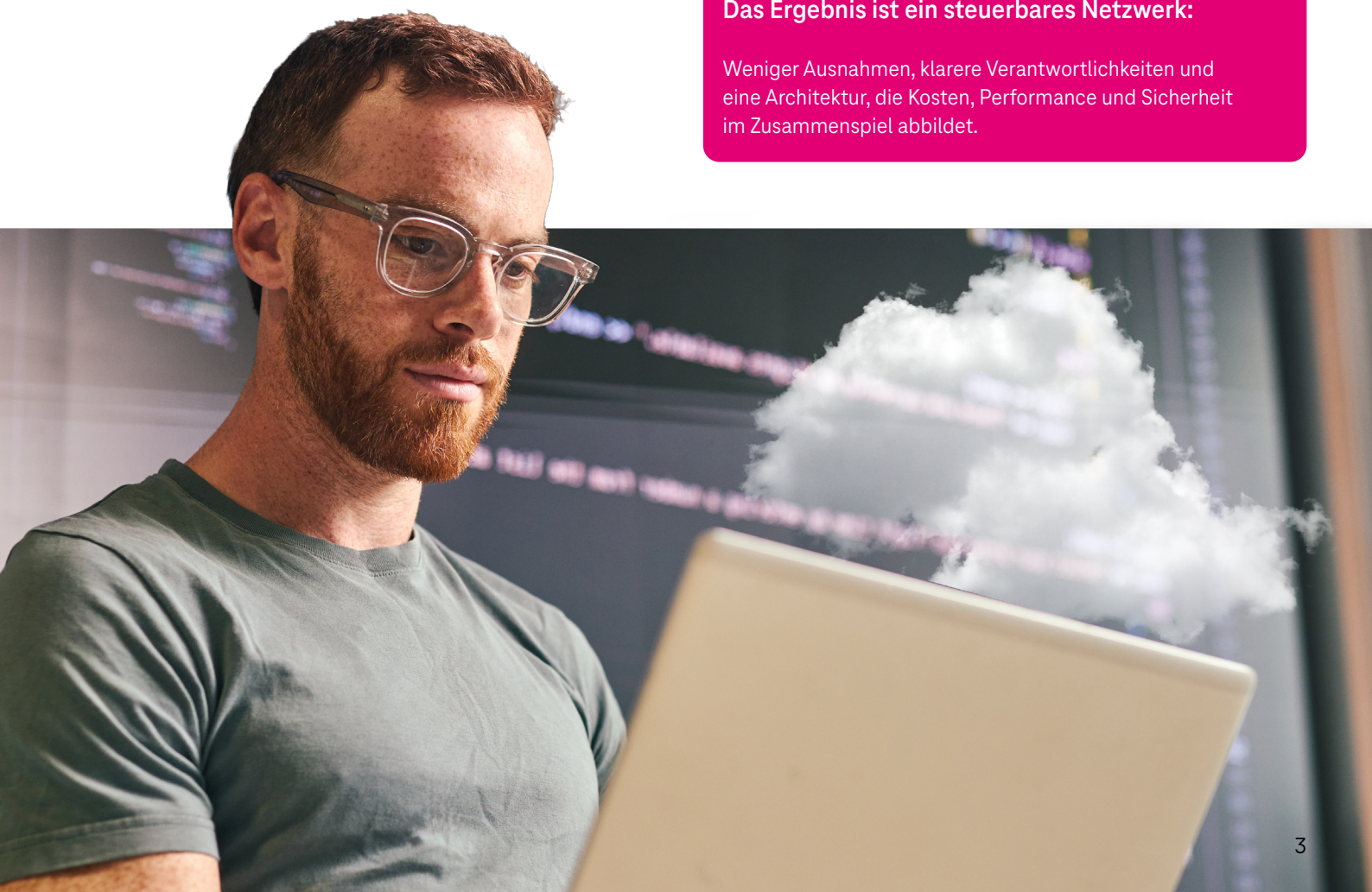
Netzwerk, Security und Cloud lassen sich unter diesen Bedingungen nicht mehr getrennt betrachten. Entscheidend ist, die Architektur so aufzubauen, dass sie als Gesamtsystem steuerbar bleibt. Konsolidierung bedeutet dabei nicht primär Reduktion, sondern Integration – also das Zusammenführen von Funktionen, Plattformen und Steuerungslogik.

Unternehmen, die hier Fortschritte erzielen, gehen schrittweise vor. Sie orientieren sich an wenigen klaren Prinzipien und entwickeln ihre Infrastruktur im laufenden Betrieb weiter, statt sie in isolierten Projekten neu zu denken.

Dieses Whitepaper zeigt auf Basis von Praxiserfahrungen, wie sich Komplexität reduzieren und Steuerungsfähigkeit zurückgewinnen lässt.

Das Ergebnis ist ein steuerbares Netzwerk:

Weniger Ausnahmen, klarere Verantwortlichkeiten und eine Architektur, die Kosten, Performance und Sicherheit im Zusammenspiel abbildet.



Einleitung

Wenn Anwendungen langsamer werden oder Cloud-Kosten unerwartet steigen, liegt die Ursache oft nicht im Detail, sondern im System. In vielen Unternehmen ist es nicht ein einzelnes Tool, sondern eine gewachsene Netzwerkinfrastruktur, die mit ihrer eigenen Komplexität an Grenzen stößt. Der Engpass ist dabei nicht Technologie, sondern Steuerbarkeit.

Diese Situation ist das Ergebnis eines grundlegenden Wandels. Unternehmensnetzwerke haben sich von klar abgegrenzten Strukturen zu verteilten Architekturen entwickelt. Cloud-Services, mobile Nutzung und hybride Arbeitsmodelle haben feste Grenzen aufgelöst und die IT räumlich wie organisatorisch fragmentiert.

Damit hat sich auch die Logik von Datenverkehr und Sicherheit verändert. Verbindungen verlaufen heute dynamisch zwischen Clouds, Standorten und Nutzern, statt entlang klar definierter Wege. Sicherheit lässt sich nicht mehr an wenigen Punkten bündeln, sondern muss innerhalb der gesamten Architektur wirksam sein.

Das Netzwerk übernimmt dadurch eine neue Rolle. Es ist nicht länger nur Transport-, sondern zentrale Steuerungs- und Durchsetzungsschicht für Performance, Kosten und Sicherheitsrichtlinien. Architekturentscheidungen wirken sich direkt auf Governance und Betrieb aus.

Für CIOs, CISOs und CTOs stellt sich damit die entscheidende Frage:

Wie lässt sich eine verteilte, dynamische Umgebung so gestalten, dass sie als Gesamtsystem transparent und steuerbar bleibt?



Die Realität 2026
Drei Herausforderungen, die es zu meistern gilt

IT-Verantwortliche stehen aktuell vor mehreren Herausforderungen gleichzeitig, die direkte Auswirkungen auf die Gestaltung von Netzwerken und Security haben:

Kosten

Budgets stagnieren oder schrumpfen, während IT-Systeme komplexer werden. Abteilungen konkurrieren um knappe Mittel, und Investitionen fließen vorrangig in unmittelbare Geschäftsthemen (z. B. KI-Projekte) statt in „unsichtbare“ Basistechnologie. Gleichzeitig explodieren die Cloud-Kosten, insbesondere durch datenintensive KI- und Multi-Cloud-Szenarien: Cloud-Anbieter stellen den ausgehenden Datenverkehr (Egress) teuer in Rechnung, was zu schwer kalkulierbaren Belastungen führt.



Personal

Kleine bis mittelgroße IT-Teams müssen immer komplexere, historisch gewachsene Landschaften betreiben. Qualifizierte Fachkräfte sind rar, gleichzeitig verteilt sich vorhandenes Know-how auf eine Vielzahl von Tools und Insellösungen. Ein erheblicher Teil der verfügbaren Zeit fließt in den laufenden Betrieb und in wiederkehrende Routineaufgaben im Netzwerk- und Security-Umfeld. Diese operative Bindung von Ressourcen lässt kaum Spielraum, um Automatisierungspotenziale konsequent zu heben oder IT-Projekte mit höherer Wertschöpfung und direkter Geschäftsrelevanz voranzutreiben. Die Weiterentwicklung der Architektur bleibt damit häufig hinter den strategischen Anforderungen zurück.

Regulierung & Nachweispflichten

Vorgaben wie die EU-NIS2-Richtlinie oder die DORA-Verordnung machen Cybersecurity zur Chefsache. Unternehmen müssen umfangreiche Risikoanalysen, Dokumentationen und Compliance-Nachweise erbringen. Eine fragmentierte Architektur mit vielen Einzellösungen vervielfacht hierbei den Aufwand: Unterschiedliche Reporting-Tools, verteilte Logs und unklare Zuständigkeiten erschweren den geforderten Überblick und das Nachweisen klarer Verantwortlichkeiten. NIS2 verankert Risikomanagement und Verantwortung explizit auf Leitungsebene – ohne Integration ist das kaum erfüllbar.

Alle drei Herausforderungen haben einen gemeinsamen blinden Fleck: das Netzwerk. Bisher rückt das Unternehmensnetz wegen seiner scheinbaren Stabilität im Tagesgeschäft oft in den Hintergrund. Doch gerade das Netzwerk ist der Ort, an dem alle Daten – und damit Kosten, Sicherheit und Performance – zusammenlaufen. Ohne ganzheitliche Netzstrategie entstehen ineffiziente Parallelstrukturen, unkontrollierte Kosten (z. B. durch Cloud-Traffic) und Lücken in der Resilienz. Im nächsten Schritt betrachten wir daher ein zentrales Muster, mit dem erfolgreiche Unternehmen diesen Herausforderungen begegnen.

Konsolidieren statt Addieren
LAN, WAN und Security zusammendenken

Ein Schlüssel zu mehr Effizienz und Kontrolle liegt in der Konsolidierung der Netzwerk- und Sicherheitslandschaft. Erfolgreiche Unternehmen verabschieden sich vom Silodenken und betrachten LAN, WAN und Security nicht als getrennte Objekte, sondern als ganzheitlichen Architekturverbund.

Zum Vergleich: In anderen Unternehmensbereichen sind Konsolidierungen längst Standard – etwa bei integrierten ERP- oder CRM-Systemen, die früher aus Dutzenden Einzellösungen bestanden. Dem gegenüber sind Netzwerke und Security-Infrastrukturen in vielen Firmen historisch fragmentiert. Ein konsolidierter Ansatz bringt jedoch handfeste Vorteile:

Kostenreduktion

Weniger unterschiedliche Hersteller und Einzelprodukte bedeuten weniger Lizenz- und Wartungskosten. Doppelausgaben lassen sich vermeiden, aktuelle Preiserhöhungen werden abgefedert.

Entlastung der IT-Teams

Sinkt die Zahl der Tools, verringert das die operative Komplexität. Automatisierung greift besser über einheitliche Plattformen hinweg, und das Team kann sich gezielt auf eine konsolidierte Umgebung fokussieren, statt sich in unzähligen Spezialtools zu verlieren.

Mehr Transparenz

In einer integrierten Network-Security-Plattform liegen alle Datenflüsse und Policies konsistent vor. Blinde Flecken verschwinden, da nicht mehrere Systeme separat überwacht werden müssen. Dokumentations- und Audit-Aufwände (z. B. für NIS2) sinken, weil Richtlinien einheitlich nachverfolgbar sind.



Wer Netzwerk, Security und Cloud Connectivity als Einheit betrachtet, hebt Potenziale, die in isolierten Einzelprojekten verborgen bleiben. Anstelle punktueller Optimierungen bewirkt konsistentes Architekturdenken spürbar positive Effekte in den Bereichen Kosten, Betrieb und Sicherheit. Entscheidend ist dabei weniger das Prinzip der Integration selbst, sondern die Frage, ob die verfügbaren Plattformen diesem Anspruch heute auch in der Praxis gerecht werden.

Der unterschätzte Kostenhebel
Cloud Connectivity

Die Cloud-Rechnung explodiert und niemand weiß, warum. Workloads laufen stabil, Nutzung bleibt konstant und dennoch steigen die Kosten plötzlich deutlich. Die Ursachen werden oft bei Instanzen oder Storage gesucht, während der eigentliche Treiber unsichtbar bleibt: der Datenverkehr zwischen Clouds und Standorten.

Lange galt die Anbindung über das Internet auch aus Kostensicht als „gut genug“. Netzwerkkosten spielten kaum eine Rolle, doch diese Annahme greift zunehmend nicht mehr. Die Spielregeln ändern sich fundamental.

Explodierende Egress-Gebühren

Mit KI-Workloads, Multi-Cloud-Architekturen und riesigen Data Lakes steigt der ausgehende Datenverkehr zwischen Clouds und Standorten sprunghaft an. Analysten beobachten, dass Egress- und Datentransferkosten einen relevanten und häufig unterschätzten Anteil der Cloud Gesamtkosten ausmachen, insbesondere, sobald Datenhaltung, Verarbeitung und Nutzung räumlich entkoppelt sind. Viele Unternehmen erleben dadurch eine Kostenexplosion auf der Cloud-Rechnung, ausgelöst durch Datentransfers.

Die Cloud-Auffahrt beeinflusst Kosten und Performance

Die Mehrkosten tauchen häufig in der Cloud-Rechnung auf – insbesondere durch steigende Egress-Gebühren für ausgehenden Datenverkehr. Mit wachsenden Datenmengen, Multi-Cloud-Strategien und KI-Anwendungen gewinnt daher die Wahl der Cloud-Anbindung zunehmend an Bedeutung. Neben dem Zugang über das öffentliche Internet bieten Cloud-Provider auch dedizierte Zugangswege an, die sowohl Performance als auch die Wirtschaftlichkeit beeinflussen können.

Cloud-Auffahrten – viele Wege führen nach Rom

Cloud-Provider wie die Deutsche Telekom, Microsoft oder AWS bieten neben dem Zugang über das öffentliche Internet auch dedizierte Zugänge an. Bei der Deutschen Telekom und AWS heißt dieser Dienst beispielsweise *Direct Connect*. Für die Umsetzung arbeiten die Cloud-Provider mit zertifizierten Connectivity-Providern zusammen, die die Verbindung zwischen Unternehmensnetzwerk und Cloud bereitstellen.

Planbare Ausgaben, bessere Performance

Private Cloud-Anbindungen bieten einen dedizierten Zugang zur Cloud, der nicht mit anderen Nutzern geteilt wird. Das sorgt für stabile Latenzen, garantierte Bandbreiten und eine höhere Verfügbarkeit – besonders bei datenintensiven Anwendungen und KI-Workloads. Der Zugang verursacht zusätzliche Kosten bei Cloud- und Connectivity-Providern. Bei hohen Datenvolumina oder hohen Anforderungen an Performance und Verfügbarkeit können sich diese Investitionen jedoch technisch und wirtschaftlich auszahlen.

Gerade für datenintensive Organisationen (etwa mit KI, Big Data oder verteilten Anwendungen) wird das Netzwerk so zum aktiven Kosten- und Performance-Hebel. Wer hier investiert, kann mittelfristig Kosten senken und besser planen – ein klarer Vorteil in Zeiten knapper Budgets.



Warum integrierte Plattformen (SASE) heute empfehlenswert sind

Mehr Security-Tools bedeuten heute nicht automatisch mehr Sicherheit. Im Gegenteil: In vielen Unternehmen zeigt sich heute das Gegenteil von mehr Sicherheit: Jede zusätzliche Speziallösung erhöht Integrationsaufwand, Betriebsrisiken und Reaktionszeiten. Richtlinien greifen nicht konsistent und Transparenz verteilt sich auf mehrere Konsolen.

Genau deshalb verschiebt sich der Markt. Integrierte Plattformen bündeln Netzwerk- und Sicherheitsfunktionen in einem gemeinsamen Betriebsmodell mit zentraler Steuerung. SASE (Secure Access Service Edge) steht exemplarisch für diesen Ansatz: keine neue Technologie, sondern die konsistente Zusammenführung des Bewährten, nämlich SD-WAN mit netznaher Sicherheit. Drei Marktentwicklungen unterstreichen diesen Trend zur Konsolidierung:



Portfolio-Erweiterungen der Hersteller

Klassische Netzwerk-Anbieter investieren massiv in Security-Funktionen, während ehemals reine Security-Anbieter Technologien wie SD-WAN, Routing oder WLAN in ihr Angebot integrieren. Dadurch entstehen Plattformen mit einem breiten Fächer an Funktionen.

„Suite“-Angebote mit großer Abdeckung

Viele integrierte Lösungen decken heute einen sehr breiten Funktionsumfang ab – von Connectivity bis Zugriffssteuerung. Zahlreiche Spezialtools können entfallen, ohne dass eine kritische Lücke entsteht.

Pragmatische 90-Prozent-Lösungen

Integrierte Plattformen liefern für die meisten Anwendungsfälle ausreichend Schutz und Performance. Nicht jede Organisation benötigt die theoretisch beste Einzellösung, wenn eine vereinfachte Gesamtplattform die Sicherheitsanforderungen zu etwa 90 % erfüllt und dabei betriebsfähig bleibt. Die restlichen 10 % Spezialbedarf lassen sich oft gezielt ergänzen, ohne dadurch die Komplexität der Architektur wesentlich zu erhöhen.

Nicht „mehr Tools“ bringen eine Organisation voran, sondern ein stimmiges Zusammenspiel der richtigen Tools. Integrierte Plattformen reduzieren Brüche zwischen Netzwerk und Security, denn genau diese Brüche verursachen in der Praxis die meisten Lücken und Probleme.

Netznahe Sicherheit
Kontrolle die dort greift, wo Traffic entsteht

Sicherheit entsteht heute nicht mehr an einzelnen Punkten, sondern entlang des gesamten Datenflusses. In modernen Netzwerkarchitekturen müssen Kontrollen dort greifen, wo Daten entstehen und verarbeitet werden – vom Endgerät über LAN/WAN bis zur Cloud-Anbindung.

Im Unterschied zum klassischen Perimeter-Modell wird Sicherheit nicht mehr an wenigen Übergabepunkten gebündelt, sondern in der verteilten Architektur verankert. Dadurch lassen sich Richtlinien unabhängig vom Standort eines Workloads durchsetzen. Mit dieser Verschiebung verändert sich auch die Steuerungslogik. Nicht einzelne Komponenten stehen im Vordergrund, sondern das Zusammenspiel von Verbindungen, Identitäten und Richtlinien über eine verteilte Umgebung hinweg.

Übergreifend lassen sich dafür einige zentrale Prinzipien beobachten:

- **Zero Trust-Zugriff (ZTNA):**
  Zugriffe werden kontextabhängig entschieden, nicht pauschal gewährt.
- **Segmentierung und Mikrosegmentierung:**
  Netzwerke werden so strukturiert, dass Abhängigkeiten begrenzt und Auswirkungen kontrollierbar bleiben.
- **Sichere Cloud-Anbindung:**
  Sicherheitsrichtlinien greifen unabhängig vom Ort der Verarbeitung – auch bei Cloud Services.
- **Verschlüsselung mit gezielter Sichtbarkeit:**
  Verschlüsselung wird mit bewusst definierten Sichtbarkeitsmechanismen kombiniert.
- **Zentral ausgewertete Security-Telemetrie:**
  Betriebsrelevante Daten werden zusammengeführt und auswertbar gemacht, um ein konsistentes Lagebild zu schaffen.

Diese Prinzipien zeigen, wie Sicherheit und Steuerbarkeit architektonisch zusammengeführt werden können. Entscheidend ist jedoch weniger ihre Definition, als ihre konsequente Umsetzung in bestehenden Umgebungen.



Von der Beobachtung zur Umsetzung
Architektur gezielt weiterentwickeln

Erfolgreiche Unternehmen betrachten Netzwerk- und Sicherheitsarchitektur heute nicht mehr als reines IT-Detail, sondern als Teil der Führungsaufgabe. Wer das Netzwerk als strategische Ebene für Kosten, Performance *und* Sicherheit versteht, reduziert Komplexität und erhöht die Resilienz – ohne die Organisation mit Großprojekten zu überfordern.

Auffällig ist ein gemeinsamer Ansatz: Statt immer neue Tools aufzusetzen, arbeiten diese Unternehmen an der Architektur – schrittweise, pragmatisch und konsequent auf Steuerbarkeit ausgerichtet.

Klarheit schaffen – nicht Perfektion

Der Einstieg ist kein aufwendiges Voll-Audit, sondern ein fokussierter Perspektivwechsel. Typische Leitfragen sind:

- Welche Datenflüsse sind geschäfts- bzw. produktionskritisch?
- Wo entstehen Ausnahmen – und warum?
- Welche Abhängigkeiten akzeptieren wir bewusst?

Entscheidend ist Relevanz statt Vollständigkeit: Transparenz dort, wo Kosten, Risiken und Ausfälle wirkungsvoll beeinflusst werden können. So entsteht eine Grundlage für eine Architektur, die nicht nur schützt, sondern steuert.

Jetzt Praxisbeispiele entdecken

Erfahren Sie, wie Unternehmen ihre Netzwerk- und Sicherheitsarchitektur erfolgreich modernisieren.

Wenige Prinzipien, konsequent umgesetzt

Unabhängig von Branche oder Ausgangslage orientieren sich erfolgreiche Unternehmen an wenigen, klaren Prinzipien:

- **Policy vor Tool:**
  Regeln sind eindeutig definiert und steuerbar – unabhängig von der eingesetzten Technologie.
- **Segmentierung zur Vereinfachung:**
  Segmente begrenzen Komplexität und machen Netzwerke kontrollierbarer.
- **Identitäten statt Netzgrenzen:**
  Zugriffe werden kontext- und identitätsbasiert gesteuert, nicht pauschal über Netzzugehörigkeit.
- **Resilienz als Standard:**
  Ausfallszenarien sind eingeplant, nicht nachträglich ergänzt.
- **Souveränität messbar machen:**
  Abhängigkeiten und Ausnahmen sind transparent und steuerbar.
- **Applikationsorientierung:**
  Datenverkehr wird gezielt nach Anwendungen priorisiert.

Diese Prinzipien schaffen klare Leitplanken für Architektur und Betrieb – insbesondere unter begrenzten Ressourcen.

Architektur in Etappen entwickeln

Statt mit einem „Big Bang“ setzen erfolgreiche Unternehmen auf ein gestaffeltes Vorgehen. Hierfür hat sich ein vierstufiger Prozess etabliert:

Phase 1: Transparenz schaffen

Datenflüsse, Ausnahmen und Verantwortlichkeiten sichtbar machen

Ziel: *Klarheit über Ist-Zustand und Steuerungslücken*

Phase 2: Steuerung etablieren

Erste Segmentierung umsetzen, Policies netznah durchsetzen, Logging-Basics einführen

Ziel: *Einheitliche Richtlinien dort wirksam machen, wo der Verkehr entsteht*

Phase 3: Resilienz verankern

Fallback-Mechanismen und Redundanzen einbauen, Notfallbetrieb üben

Ziel: *Handlungsfähigkeit auch unter Stress sicherstellen*

Phase 4: Standardisieren & automatisieren

Architektur vereinheitlichen, Routineprozesse automatisieren, Betriebsmodell optimieren

Ziel: *Weniger Ausnahmen, mehr Skalierbarkeit und Wiederholbarkeit*

Durch dieses iterative Vorgehen zeigen sich frühe Erfolge, ohne den Betrieb zu überlasten. Jede Etappe verbessert die Steuerbarkeit spürbar und schafft die Grundlage für die nächste.

Fortschritt messbar machen

Was gesteuert werden soll, muss gemessen werden. Erfolgreiche Teams setzen auf wenige, aussagekräftige Kennzahlen, die sowohl IT- als auch Management-Ebene nachvollziehen können. Beispiele dafür sind:

- **Ausnahmequote:**
  Anzahl aktiver Policy-Ausnahmen (und deren durchschnittliche Dauer).
- **Segment-Abdeckung:**
  Anteil kritischer Datenflüsse, der durch definierte Segmentgrenzen geführt wird.
- **Policy-Konsistenz:**
  Anteil der Standorte/Cloud-Anbindungen mit identischer Basis-Policy.
- **Time-to-Isolate:**
  Zeit bis zur Isolation eines kompromittierten Segments (im Störfall).
- **Compliance-Scope:**
  Anzahl der Systeme, die im Prüfungsumfang (Scope) für Audits liegen (und dessen Trend über die Zeit).
- **Abhängigkeitsindex:**
  Anzahl identifizierter Single Points of Failure entlang der zentralen Kommunikationspfade (Provider, Identity, DNS etc.).

Solche KPIs verbinden technische Realität mit Management-Transparenz. Sie machen Fortschritte (oder Lücken) greifbar und schaffen bereichsübergreifend ein einheitliches Verständnis von Erfolg.

Souveränität richtig einordnen
Kontrolle vor Ideologie



Diskussionen über *digitale Souveränität* sind oft ideologisch aufgeladen. Praktisch lässt sich das Thema auf **einige einfache Leitfragen** reduzieren:

Wer betreibt das Netzwerk – und wo?

Ist sichergestellt, dass kritische Netzkomponenten durch vertrauenswürdige Teams oder vertraglich gebundene Dienstleister betrieben werden? Erfolgt der Betrieb in klar definierter Jurisdiktion und nach festgelegten Vorgaben, etwa zu Standortanforderungen oder Hintergrundprüfungen? Souveränität bedeutet hier: Betrieb und Verantwortlichkeiten sind nachvollziehbar geregelt – unabhängig davon, ob intern oder extern betrieben wird.

Wer hat Zugriff auf Schlüssel und Policies?

Wird die Hoheit über Kryptoschlüssel, Zertifikate und Policy Stores behalten oder an Dritte abgegeben? Ein souveränes Netzwerk behält die Kontrolle über sicherheitskritische Steuerungsinstanzen, insbesondere über Schlüsselmaterial und Richtlinien.

Sind Pfade, Abhängigkeiten und Ausnahmen transparent?

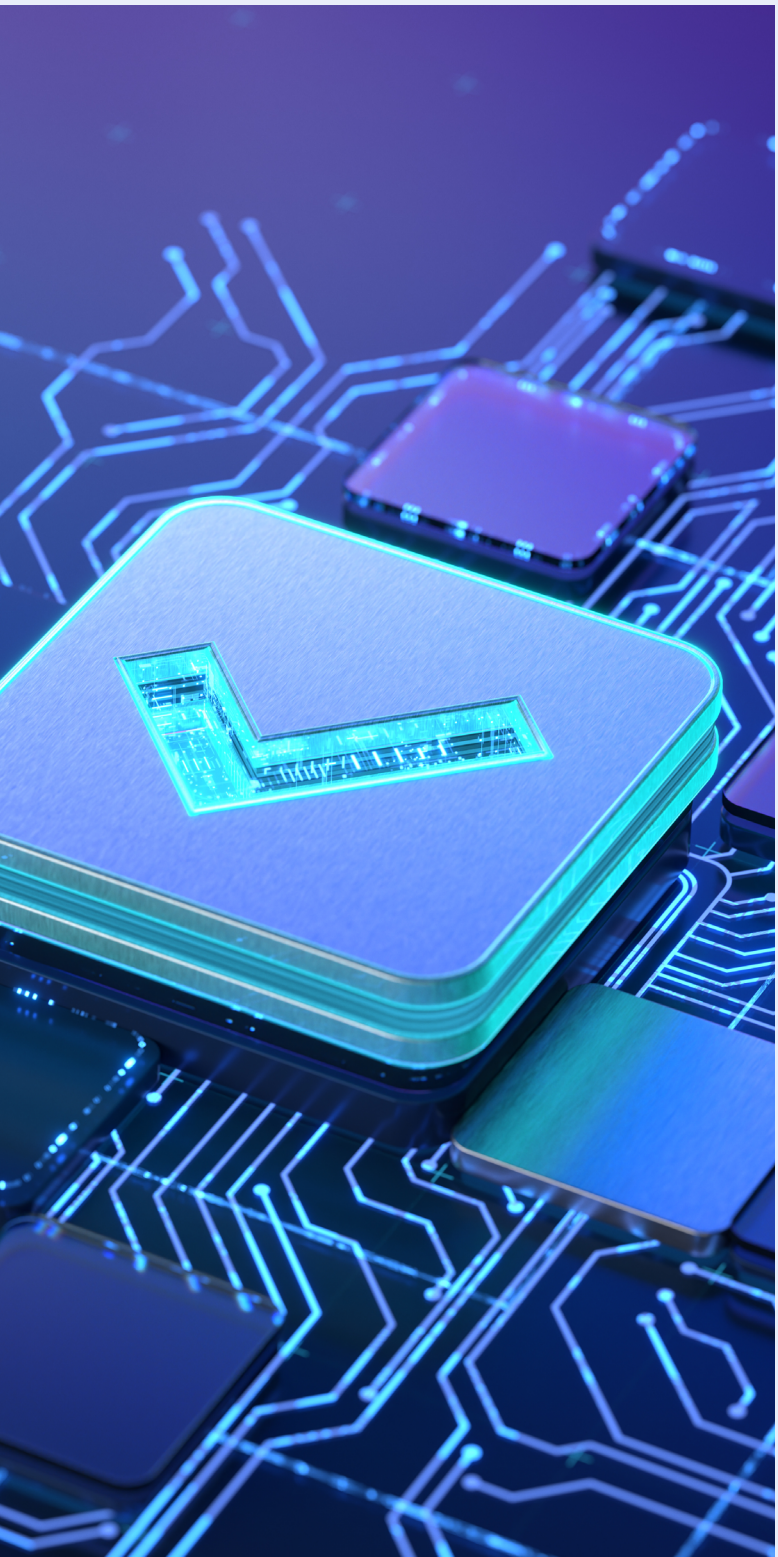
Ist für jede Verbindung nachvollziehbar, über welche Provider, Länder und Systeme sie führt? Lassen sich Single Points of Failure minimieren? Sind Abweichungen von definierten Sicherheitsrichtlinien vollständig dokumentiert, genehmigt und zeitlich befristet? Ohne Transparenz über Abhängigkeiten gibt es keine echte Steuerungsfähigkeit – und damit keine Souveränität.

Dies sind pragmatische Kernaspekte von Souveränität.
Es geht nicht um totale Autarkie, sondern um Kontrolle und Wahlmöglichkeiten. Eine souveräne Netzwerk-Architektur gibt dem Unternehmen die Zügel in die Hand.

Regulierung als Chance
NIS2 pragmatisch nutzen

Regulatorische Vorgaben werden oft als Bürde gesehen – dabei können sie gezielt als Treiber für Verbesserungen eingesetzt werden. Die EU-Richtlinie NIS2 etwa verpflichtet Unternehmen, ihre Cybersecurity-Strategie grundlegend zu prüfen.

Anstatt NIS2 als Drohkulisse zu behandeln, lässt sich das Momentum nutzen, um interne Veränderungen voranzubringen. Ein konsolidierter Secure-Networking-Ansatz zahlt direkt auf mehrere NIS2-Pflichten ein:



Einfachere Dokumentation

Weniger heterogene Systeme bedeuten weniger Aufwand für Nachweise. Netzwerk- und Security-Policies, Änderungen und Incidents lassen sich in einer konsolidierten Plattform viel leichter dokumentieren und Prüfern gegenüber belegen.

Klare Verantwortlichkeiten

NIS2 fordert eindeutige Zuständigkeiten und Meldewege. In einer integrierten Architektur verschwimmen Netzwerk und Security nicht – Verantwortliche für Datenflüsse und Richtlinien sind klar benennbar, und ihre Einhaltung lässt sich nachhalten.

Nachvollziehbarkeit & Kontrolle

Durch zentrale Telemetrie sowie zentrales Monitoring erhalten Unternehmen eine lückenlose Sicht auf alle Kommunikationspfade und Sicherheitskontrollen. Kennzahlen wie Policy-Compliance an allen Standorten oder Time-to-Detect bei Incidents sind auf Knopfdruck verfügbar. So wird aus Compliance ein Management-Werkzeug: Man gewinnt Kontrolle, statt nur Haken zu setzen.

Eine ganzheitliche Secure-Networking-Strategie kehrt den Spieß um. Höhere Anforderungen lassen sich mit weniger Gesamtkomplexität erfüllen, weil Integration die Effizienz steigert. Regulierung wird zum Motor sinnvoller Architekturentscheidungen – nicht zum Hemmschuh.

Secure Networking mit der Telekom
Netzwerk und Sicherheit aus einer Hand

Die größten operativen Risiken entstehen heute nicht innerhalb einzelner Technologien, sondern an ihren Schnittstellen. Brüche zwischen Netzwerk und Security sowie zwischen Cloud und Betrieb erschweren Governance und erhöhen Risiken. Genau hier setzt ein integrierter Secure-Networking-Ansatz an.

Die Deutsche Telekom verbindet Netzbetrieb und Security Services in einem einheitlichen Betriebsmodell. Während viele Anbieter Konnektivität und Security getrennt liefern, werden Sicherheitsfunktionen hier direkt in das Netzwerk integriert – nicht als Zusatz, sondern als fester Bestandteil der Netzdienste.

Das Portfolio umfasst Access-Netze, WAN und Cloud-Anbindungen sowie zentrale Security- und Compliance-Funktionen. Verbindungen und Richtlinien greifen dabei gemeinsam und folgen klaren Verantwortlichkeiten, statt über mehrere Systeme hinweg koordiniert werden zu müssen.

Dieser integrierte Ansatz wird auch extern bestätigt: Der IDC MarketScape „Worldwide Managed SD WAN Services 2025“ positioniert die Deutsche Telekom als führenden Anbieter und hebt insbesondere die Kombination aus globaler Konnektivität, SD-WAN-Management und integrierter Security hervor.

Netzwerk und Sicherheit gemeinsam zu denken, bewährt sich sowohl operativ als auch am Markt.



Noch mehr Tools ist nicht die Lösung
Erfolgreiche Transformationsstrategien

Zum Abschluss lohnt ein Blick auf typische Ansätze von Vorreiter-Unternehmen. Deren Transformationsprojekte folgen bemerkenswert ähnlichen Mustern und unterscheiden sich deutlich von klassischen „Mehr investieren, mehr Tools“-Strategien:

Ende-zu-Ende statt Silos

Erfolgreiche IT-Teams betrachten Datenflüsse ganzheitlich über alle Domains. Entscheidungen zu Cloud, WAN, LAN und Security werden vernetzt getroffen. So entstehen Architekturen mit deutlich weniger Übergabepunkten und Medienbrüchen – das erhöht Sicherheit *und* Steuerbarkeit.

Weniger Tools, mehr Integration

Statt immer neue Produkte obenauf zu setzen, reduzieren diese Unternehmen gezielt die Zahl der Komponenten. Sie konsolidieren Funktionen auf integrativen Plattformen. Jede Schnittstelle weniger bedeutet weniger Fehlerpotenzial und weniger Betriebsaufwand. Selbst kleine Teams behalten so den Überblick.

Architektur in Etappen entwickeln

Keine erfolgreiche Organisation hat ihre Zielarchitektur in einem Big Bang erreicht. Allen gemein ist ein iteratives Vorgehen in überschaubaren Etappen. Zuerst wird Transparenz über den Status quo geschaffen, dann folgen grundlegende Architekturentscheidungen (Segmentierung, Enforcement-Punkte, Identity-Steuerung). Anschließend werden nach und nach Resilienz-Mechanismen ergänzt und schließlich durch Standardisierung und Automatisierung die Skalierbarkeit erhöht. Dieses *lernende Vorgehen* sorgt dafür, dass das Unternehmen agil bleibt und früh greifbare Verbesserungen spürt, anstatt in jahrelangen Umbauprojekten festzustecken.

Beobachten statt belehren

Die genannten Methoden sind aus der Praxis geboren, nicht theoretisch erdacht. Die implizite Botschaft lautet: Was in erfolgreichen Architekturen funktioniert, liefert die Blaupause – ohne jedem kurzfristigen Hype hinterherlaufen zu müssen. Auch die Deutsche Telekom berät nach diesem Prinzip: aus *Best Practices* werden Empfehlungen.



Fazit
Weniger Aufwand – mehr Steuerbarkeit



Die technologischen Möglichkeiten werden weiterwachsen, während Budgets, Personal und Zeit begrenzt bleiben. Unter diesen Bedingungen entscheidet nicht die Anzahl eingesetzter Lösungen über den Erfolg, sondern deren Steuerbarkeit. Der entscheidende Hebel liegt nicht im Hinzufügen weiterer Komponenten, sondern darin, Komplexität gezielt zu reduzieren und Zusammenhänge beherrschbar zu machen.

Secure Networking beschreibt dafür einen architektonischen Ansatz: Netzwerk, Security und Cloud werden als zusammenhängendes System gestaltet. Ziel ist nicht maximale Funktionalität, sondern Transparenz, klare Verantwortung und operative Kontrolle. Konsolidierung bedeutet in diesem Kontext vor allem eines – weniger Fragmentierung und mehr Klarheit darüber, wie Datenflüsse, Zugriffe und Kosten tatsächlich zusammenhängen.

Kernpunkte zum Mitnehmen

- **Konsolidierung erhöht Steuerbarkeit – mit direktem Kosteneffekt:** Weniger Plattformen und Sonderlösungen reduzieren nicht nur Ausgaben, sondern vor allem Abstimmungsaufwand und Komplexität im Betrieb.
- **Integration schafft stabile Betriebsmodelle:** Einheitliche Prozesse und klare Zuständigkeiten entlasten Teams und bilden die Grundlage für konsistente Governance.
- **Das Netzwerk wird von einer Transport- zur Steuerungsebene:** Durch Transparenz und gezielte Anbindung lässt sich das Netzwerk aktiv für Performance-, Kosten- und Resilienzsteuerung nutzen.
- **Security folgt der Architektur:** Werden Netzwerk und Sicherheit gemeinsam gedacht, entsteht Kontrolle über Datenflüsse und Zugriffe – nicht nachgelagert, sondern strukturell verankert.

Damit verschiebt sich der Fokus grundlegend: weg von der Optimierung einzelner Maßnahmen, hin zu mehr Steuerbarkeit durch klare Architekturprinzipien. Netzwerke weiterdenken heißt, es als integralen Bestandteil von Governance und Sicherheitsstrategie zu verstehen.

Quellen:
Cloud-Kosten & Wirtschaftlichkeit
- Wasabi
- Gartner Magic Quadrant for Cloud Financial Management Tools

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

Transformation & Zielarchitektur
- Gartner Strategic Roadmap for SASE Convergence 2025

Das Ergebnis ist keine komplexere, sondern eine klarere IT-Architektur

Weniger Ausnahmen, eindeutigere Verantwortlichkeiten und ein System, das Kosten und Risiken aktiv steuert – statt auf sie zu reagieren.

Melden Sie sich für eine persönliche Beratung!

Kontakt
Zum Kontaktformular
www.geschaeftskunden.telekom.de

Herausgeber
Deutsche Telekom
Geschäftskunden GmbH
Landgrabenweg 149
53227 Bonn

Connecting your world.

Deutsche Telekom GmbH | 06/2026