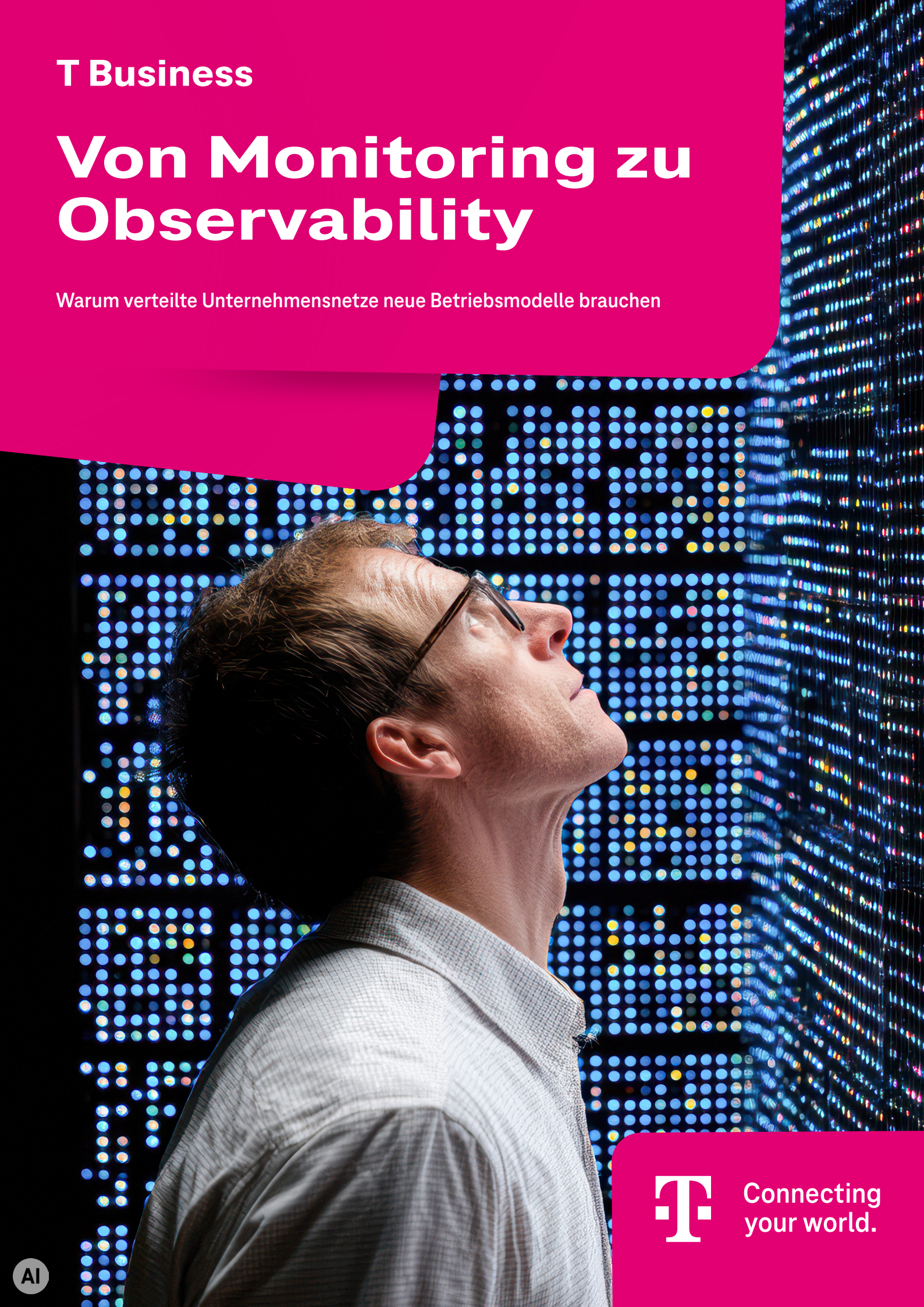
T Business

Von Monitoring zu Observability

Warum verteilte Unternehmensnetze neue Betriebsmodelle brauchen



Connecting your world.

AI

Einführung

Während Unternehmensnetze früher vor allem zentrale Rechenzentren und klar abgegrenzte Standorte miteinander verbunden haben, sind sie inzwischen zu einem bedeutenden Produktionsfaktor geworden. Egal ob Fertigungs- und Logistikstandorte, Niederlassungen, Homeoffice oder mobile Mitarbeiter: Netzwerke sind das essenzielle Bindeglied für den Zugriff auf Cloud-Plattformen, SaaS-Anwendungen sowie zentrale IT-Dienste.

Kommt es zu Störungen – insbesondere bei der Anwendungsnutzung – werden diese selten allein durch eine einzelne Netzwerkkomponente verursacht. Auch WLAN, Weitverkehrspfade, Routingtabellen, DNS, Security-Policies, Endgerätekonfiguationen, Provider oder externe Plattformen können die Nutzererfahrung bzw. Performanz beeinflussen.

Klassisches Monitoring zeigt hierbei, ob Systeme erreichbar sind, Grenzwerte überschritten werden oder Kennzahlen wie Latenz, Paketverlust und Auslastung auffällig sind. Für die Frage, warum ein Service beeinträchtigt ist und welche Abhängigkeiten dabei eine Rolle spielen, braucht es jedoch zusätzlichen Kontext. Observability verknüpft dafür relevante technische Signale mit Informationen zu Standorten, Services, Nutzern, Providern und Änderungen. So lassen sich Ursachen und Auswirkungen besser einordnen.

Das ist besonders für Unternehmen mit vielen verteilten Standorten wichtig. Unterschiedliche Anschlussarten, Provider, Sicherheitsvorgaben und lokale Betriebsbedingungen erschweren eine einheitliche Steuerung. Gleichzeitig müssen IT-Teams Servicequalität bewerten, Störungen gezielt eingrenzen und ihre Auswirkungen für Fachbereiche und Management verständlich darstellen.

Dieses Whitepaper erläutert, wie sich Monitoring und Observability unterscheiden, welche Herausforderungen in verteilten Unternehmensnetzen entstehen und welches Zielbild daraus folgt. Im Mittelpunkt steht dabei nicht die möglichst umfassende Sammlung von Daten. Entscheidend ist, relevante Informationen so in Betrieb und Prozesse einzubinden, dass sie bessere Analysen und fundierte Entscheidungen unterstützen.

Die Deutsche Telekom unterstützt Unternehmen bei diesem Zielbild, indem sie relevante Leistungsbereiche zusammenführt: von der Standort- und Cloud-Anbindung, über softwaredefinierte Netzsteuerung, LAN-/WLAN-Betrieb und integrierte Security-Lösungen bis hin zu Managed Services. Was davon im Einzelfall relevant ist, hängt von Standortstruktur, Cloud-Nutzung, Sicherheitsanforderungen, Datenqualität und Betriebsmodell des jeweiligen Unternehmens ab.



Warum verteilte Netze mehr als Monitoring brauchen

In Unternehmen mit vielen Standorten treffen unterschiedliche Generationen von Anschlüssen, LAN- und WLAN-Infrastrukturen, Sicherheitslösungen und Providerleistungen aufeinander. Hinzu kommen Cloud- und SaaS-Dienste, mobile Zugriffe und neue Netzwerkarchitekturen. Dadurch kann eine Beeinträchtigung an einer Stelle entstehen und sich an anderer Stelle bemerkbar machen. Eine langsame Anwendung in einer Filiale kann beispielsweise mit dem lokalen WLAN, dem WAN-Pfad, einer DNS-Konfiguration, einer Security-Prüfung oder einem externen Cloud-Service zusammenhängen.

Monitoring liefert dafür wichtige Statusinformationen. Es erkennt etwa, wenn Geräte oder Verbindungen nicht erreichbar sind, Latenz oder Paketverlust zunehmen oder definierte Grenzwerte überschritten werden. Damit beantwortet es vor allem die Frage: **Was passiert?** Seine Grenzen zeigen sich, wenn mehrere Ursachen infrage kommen. Ein einzelner Alarm erklärt selten, welche Abhängigkeiten beteiligt sind oder welche Nutzer und Services betroffen sind.

Observability ergänzt Monitoring um Kontext und Korrelation und beantwortet somit die Frage: **Warum passiert es?** Sie verknüpft relevante Metriken, Logs und Ereignisse mit Topologie- und Serviceinformationen. So lässt sich beispielsweise prüfen, ob eine Auffälligkeit mit einer Änderung, einer Security-Policy, einem Provider oder einem anderen Abschnitt des Servicepfads zusammenfällt. Das unterstützt Teams dabei, Ursachenhypothesen zu bilden, Auswirkungen einzuordnen und gezielter über nächste Schritte zu entscheiden.

Eine besondere Herausforderung entsteht, wenn die beteiligten Teams mit unterschiedlichen Systemen arbeiten. Der Netzwerkbetrieb sieht möglicherweise Latenz oder Paketverlust, Security Operations Policy- oder Inspection-Ereignisse, der Cloud-Betrieb Plattformmetriken und der Service Desk Tickets. Provider liefern zusätzlich eigene Statusinformationen. Ohne gemeinsamen Kontext bleibt unklar, wie diese einzelnen Beobachtungen zusammenhängen. Bei einer Störung, die nur manche Standorte betrifft, müssen Teams etwa untersuchen, ob ein bestimmter Provider, eine Region, ein Standorttyp, eine Security-Policy oder eine Änderung im Routing beteiligt ist. Fehlt dieser Zusammenhang, werden Tickets häufig weitergereicht, statt die Ursache gezielt einzugrenzen.

Bei internationalen Standortnetzen erschweren zudem unterschiedliche Provider, Anschlussarten, Service-Level, Betriebsfenster und Eskalationswege die einheitliche Steuerung. Die zentrale IT muss Servicequalität bewerten und vergleichbar berichten, obwohl die operative Datenlage je nach Land oder Standort verschieden sein kann. Dafür braucht sie neben technischen Signalen auch Standort-, Provider- und Servicekontext.

Auch Netzwerkleistung und Security lassen sich nicht immer getrennt beurteilen. Sicherheitsprüfungen, die näher an Nutzer, Standorte und Cloud-Zugriffe rücken, können die Nutzererfahrung beeinflussen, ohne dass ein klassischer Netzwerkausfall vorliegt. Bei Architekturen wie SASE, die Netzwerk- und Security-Funktionen verbinden, wird es deshalb wichtiger, Performance- und Security-Ereignisse gemeinsam einzuordnen.



Abbildung 1: Erst die Verknüpfung von technischen Signalen, Standorten, Providern und Betriebsprozessen schafft den Kontext für schnelle, fundierte Entscheidungen

Ähnliches gilt für Änderungen. Eine neue SD-WAN-Policy, eine Anpassung im Firewall-Regelwerk, ein anderer Cloud-Pfad, eine neue DNS-Konfiguration oder ein Providerwechsel kann an verschiedenen Standorten unterschiedliche Auswirkungen haben. Werden die relevanten Daten nicht zusammengeführt, bleibt schwer erkennbar, ob eine Störung auf die Änderung, lokale Bedingungen oder eine externe Abhängigkeit zurückgeht. Observability kann dazu beitragen, diese Wirkung nachvollziehbarer zu machen.

Denn: Fachbereiche und Management brauchen eine Einordnung, die über technische Einzelwerte hinausgeht. Sie fragen nach der Stabilität geschäftlicher Prozesse – nicht allein nach Paketverlust oder Routingpfaden. Observability kann technische Signale mit Services, Standorten und Betriebsprozessen verknüpfen und eine fundiertere Bewertung unterstützen. Sie ersetzt weder Monitoring noch Security-Architektur oder Operations. Entscheidend ist, die relevanten Signale im passenden Kontext verfügbar zu machen.

Welches Zielbild Observability im Enterprise-Kontext braucht

Ein tragfähiges Zielbild für Observability beginnt nicht bei einer Plattform, sondern bei der Frage, welche Betriebsfähigkeit das Unternehmen erreichen will. Für grosse Standortorganisationen geht es selten darum, jede technische Einzelheit permanent sichtbar zu machen. Entscheidend ist vielmehr, für geschäftskritische Services die relevanten Signale so zusammenzuführen, dass Ursachen, Auswirkungen und Verantwortlichkeiten nachvollziehbarer werden.

Im Zentrum steht ein gemeinsamer Daten- und Kontextlayer. Er verbindet Informationen aus WAN, LAN, WLAN, SD-WAN, SASE, Cloud-Anbindung, Security-Komponenten, Endgeräten, Applikationen und ITSM-Systemen. ITSM steht für IT Service Management und beschreibt Prozesse wie Incident, Problem, Change und Service Reporting. Diese Prozesse sind wichtig, weil Observability-Daten erst dann betrieblichen Wert entfalten, wenn sie in Entscheidungen, Tickets, Eskalationen und Management-Reports einfliessen.

Das Zielbild muss dabei zwischen Signal, Kontext und Entscheidung unterscheiden. Ein Signal ist zum Beispiel eine auffällige Latenz, ein Paketverlust, ein Log-Ereignis, ein Policy-Hit oder ein fehlgeschlagener Zugriff. Kontext entsteht erst, wenn dieses Signal mit Standort, Provider, Applikation, Nutzergruppe, Topologie, Change-Historie oder Security-Regel verknüpft wird. Eine Entscheidung entsteht wiederum erst, wenn dieser Kontext in eine betriebliche Handlung übersetzt wird: Eskalation an einen Provider, Rücknahme eines Changes, Anpassung einer Policy, Erweiterung eines Anschlusses, Analyse eines Endgeräts oder Priorisierung einer Modernisierungsmassnahme.

Für viele Unternehmen ist dieser Übergang die eigentliche Herausforderung. Dashboards sind schnell aufgebaut, aber sie schaffen nicht automatisch ein gemeinsames Verständnis. Ein Standort kann auf einer Netzwerkseite grün erscheinen, während Nutzer trotzdem eine schlechte Applikationserfahrung haben. Eine Security-

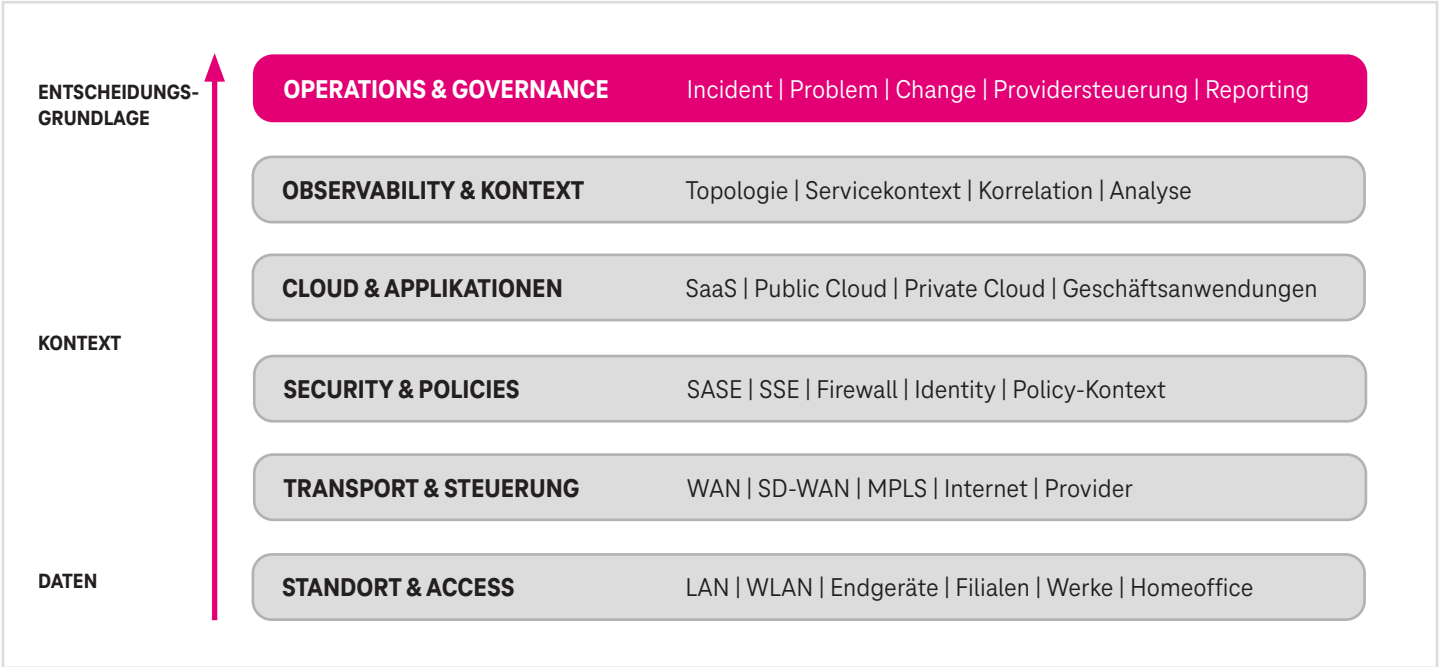


Abbildung 2: Fundierte Betriebsentscheidungen im Rahmen von Observability erfordern eine durchgängige Wirkungskette

Konsole kann eine Richtlinie korrekt ausführen, während der Fachbereich eine spürbare Verzögerung erlebt. Ein Provider kann seine Serviceparameter erfüllen, während die Ende-zu-Ende-Erfahrung nicht den Erwartungen entspricht. Observability muss diese Perspektiven zusammenführen, ohne die Verantwortung zwischen Teams zu verwischen.

Ein belastbares Zielbild enthält deshalb klare Designprinzipien. Die Datenquellen müssen relevant und verlässlich sein. Die Korrelation muss auf einem verständlichen Modell beruhen. Die wichtigsten Services und Standorte müssen priorisiert werden. Zugriffsrechte, Datenschutz und Datenresidenz müssen geklärt sein. Rollen und Verantwortlichkeiten müssen so definiert werden, dass Observability nicht zu einem weiteren Tool-Silo wird. Und die technische Architektur muss offen genug bleiben, um unterschiedliche Hersteller, Provider, Cloud-Plattformen und Betriebsmodelle einzubinden. Für Unternehmen mit vielen Standorten gilt zusätzlich: Standardisierung darf lokale Realität nicht ignorieren. Standorte unterscheiden sich in Kritikalität, Bandbreite, Anwendungen und Sicherheitsanforderungen. Eine große Produktionsstätte mit OT-nahen Systemen wie beispielsweise SPS-Programmiergeräten oder Manufacturing Execution Systems stellt andere Anforderungen als eine kleine Vertriebsniederlassung; eine Filiale mit Kassensystemen und Kundenzugängen andere als ein Bürostandort mit Collaboration-Fokus. Das Zielbild sollte daher nicht starr, sondern abgestuft sein: Kritische Standorte und Services erhalten tiefere Observability, weniger kritische Bereiche werden angemessen, aber nicht überdimensioniert eingebunden.

Security und Compliance gehören ebenfalls ins Zielbild, aber mit realistischen Erwartungen. Observability verbessert Nachvollziehbarkeit, liefert Daten für Untersuchungen und macht Zusammenhänge zwischen Netzwerkereignissen und Sicherheitskontext sichtbar. Sie macht ein Unternehmen jedoch nicht automatisch compliant und verhindert keine Angriffe. Aussagen zu regulatorischer Erfüllung, Risikoreduktion oder Security-Wirkung müssen belegt und fachlich freigegeben werden.

Ein gutes Zielbild beantwortet damit drei Fragen: Welche Services und Standorte sind wirklich relevant? Welche Daten und Kontexte werden benötigt, um deren Verhalten zu verstehen? Und welche Betriebsprozesse nutzen diese Erkenntnisse? Erst wenn diese Fragen geklärt sind, wird Observability von einer technischen Datensammlung zu einem steuerbaren Betriebsmodell.



Wie Observability technisch funktioniert

Die technische Architektur von Observability lässt sich als Datenfluss vom Standort bis zur Entscheidung beschreiben. Am Anfang stehen Signale aus der Infrastruktur: Metriken aus Routern, Switches und Access Points, Flow-Daten aus Netzwerkpfaden, Logs aus Security-Komponenten, Statusinformationen aus SD-WAN-Controllern, Daten aus Cloud-Verbindungen, DNS-Informationen, Endgeräteinformationen und synthetische Tests aus der Perspektive von Nutzerinnen und Nutzern. Diese Signale sind für sich genommen wertvoll, aber sie erklären selten allein die Ursache eines Problems.

Der nächste Schritt ist die Verknüpfung mit Topologie und Servicekontext. Ein Latenzwert wird aussagekräftiger, wenn er einem Standort, einem Provider, einer Anwendung, einer Nutzergruppe und einem konkreten Pfad zugeordnet werden kann. Ein Log-Eintrag wird hilfreicher, wenn sichtbar ist, welche Policy, welcher Service und welche Änderung damit verbunden sind. Ein Ticket wird verwertbarer, wenn es nicht nur eine Beschwerde beschreibt, sondern mit technischen Ereignissen und betroffenen Services verbunden ist. Observability lebt von dieser Übersetzung: aus Rohdaten wird ein Betriebszusammenhang.

In modernen Standortnetzen spielen SD-WAN- und SASE-Daten eine wichtige Rolle. SD-WAN steht für softwaredefinierte Steuerung von Weitverkehrsnetzen. Für Observability ist daran relevant, dass Applikationspfade, Policies und Verkehrsentscheidungen nicht verborgen bleiben sollten, sondern Teil der Ursachenanalyse werden. Wenn ein Standortproblem auftritt, reicht es nicht zu wissen, dass der Standort online ist. Entscheidend ist, welcher Pfad genutzt wurde, welche Anwendung betroffen war und welche Policy gegriffen hat.

SASE ergänzt diese Perspektive um Sicherheitskontext. Wenn Netzwerkzugriffe und Sicherheitsprüfungen stärker zusammengeführt werden, beeinflussen Security-Entscheidungen auch Pfade, Latenzen und Nutzererfahrung. Observability sollte daher nicht nur Netzwerkmetriken erfassen, sondern auch sichtbar machen, welche Security-Komponenten und Policies an einem Zugriff beteiligt sind. Das ist besonders wichtig, wenn Standorte, mobile Nutzer, IoT-Geräte und Cloud-Anwendungen über ein gemeinsames Sicherheits- und Zugriffsmodell gesteuert werden.

Neben WAN und Security bleibt die lokale Standortebene entscheidend. Viele Probleme entstehen nicht im Weitverkehrsnetz, sondern im LAN, WLAN, in der lokalen Strom- oder Geräteumgebung, in falsch dimensionierten Access Points oder in lokalen Konfigurationsunterschieden. Wenn diese Ebene nicht sichtbar ist, kann ein zentrales Observability-Modell falsche Schlüsse ziehen.

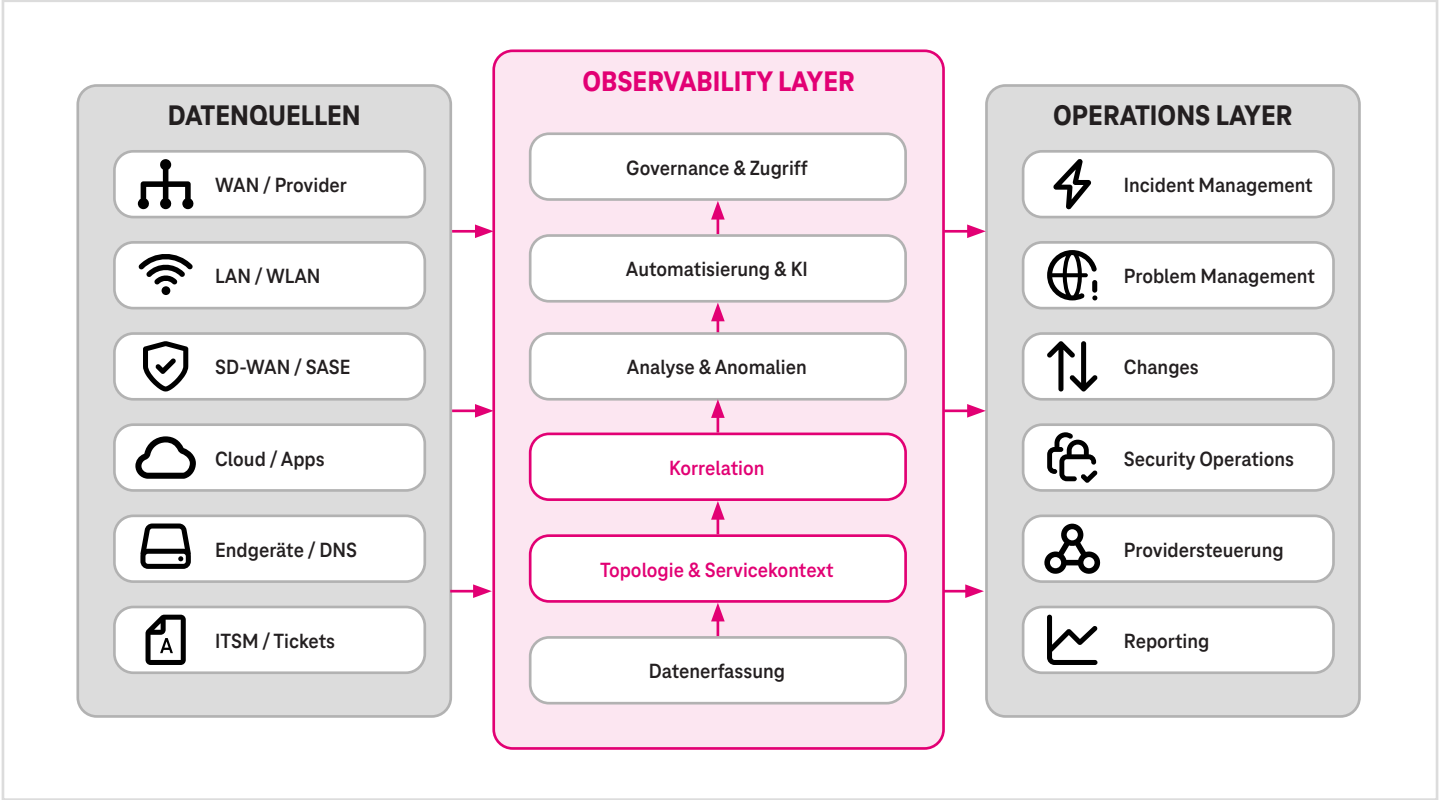


Abbildung 3: Architekturmodell für Observability

Ein langsamer Cloud-Zugriff kann dann als WAN-Problem erscheinen, obwohl die Ursache im lokalen WLAN-Funknetz liegt. Für Unternehmen mit vielen Standorten wird deshalb wichtig, lokale Signale in denselben Analysekontext einzubinden wie WAN-, Cloud- und Security-Daten.

Die Architektur braucht ausserdem eine Integrationsschicht. Observability-Plattformen, Netzwerkmanagementsysteme, Security-Tools, Cloud-Monitoring, ITSM-Systeme und Providerportale müssen nicht zwingend in einem einzigen System aufgehen. Entscheidend ist, dass relevante Informationen so verbunden werden, dass Teams gemeinsam arbeiten können. In der Praxis kann das über APIs, Event-Streams, Datenmodelle, Dashboards, Automatisierungen oder ITSM-Integrationen geschehen. Technisch geht es dabei weniger um Vollständigkeit als um Relevanz: Welche Daten helfen tatsächlich, die wichtigsten Use Cases zu erklären?

Auch künstliche Intelligenz und Automatisierung können hier unterstützen. Muster- und Anomalieerkennung sowie automatisierte Korrelation erleichtern die Analyse, wenn Datenqualität, Kontextmodell und Prozessintegration stimmen. Ohne saubere Daten und klare Verantwortlichkeiten beschleunigt Automatisierung jedoch nur Fehlinterpretationen.

Technisch betrachtet besteht Observability aus mehreren Schichten: Datenerfassung, Kontextualisierung, Korrelation, Analyse, Prozessintegration und Governance. Der Wert entsteht nicht in einer einzelnen Schicht, sondern im Zusammenspiel. Eine Plattform kann Daten sammeln, aber sie schafft keine Verantwortung. Ein Dashboard kann Muster zeigen, aber es ersetzt keine Eskalationslogik. Ein Telemetriestandard kann Daten strukturieren, aber er löst keine organisatorischen Zielkonflikte. Deshalb muss die technische Architektur mit dem Betriebsmodell verbunden werden.

Wie Betrieb, Governance, Security und Compliance zusammenspielen

Observability entfaltet ihren Wert nicht allein durch technische Datenerfassung. Sie wird erst wirksam, wenn Unternehmen klären, wer Daten interpretiert, wer Massnahmen auslöst, wer Provider steuert und wer Entscheidungen gegenüber Fachbereichen oder Management erklärt. In großen Standortorganisationen ist diese Frage anspruchsvoll, weil Netzwerkbetrieb, Security, Cloud, Service Desk, Applikationsbetrieb und externe Dienstleister unterschiedliche Sichtweisen auf dieselbe Störung haben.

Eine langsame Anwendung in mehreren Filialen zeigt, warum ein gemeinsamer Servicekontext nötig ist: Netzwerk-, Security- und Cloud-Daten sowie Tickets und Providerinformationen müssen demselben Service, Standort und Zeitraum zugeordnet werden. Erst dann lässt sich aus den einzelnen Beobachtungen eine gemeinsame Ursachenhypothese bilden. Observability muss diese Zusammenhänge deshalb in Betriebsabläufe und Verantwortlichkeiten einbetten – nicht nur in Dashboards.

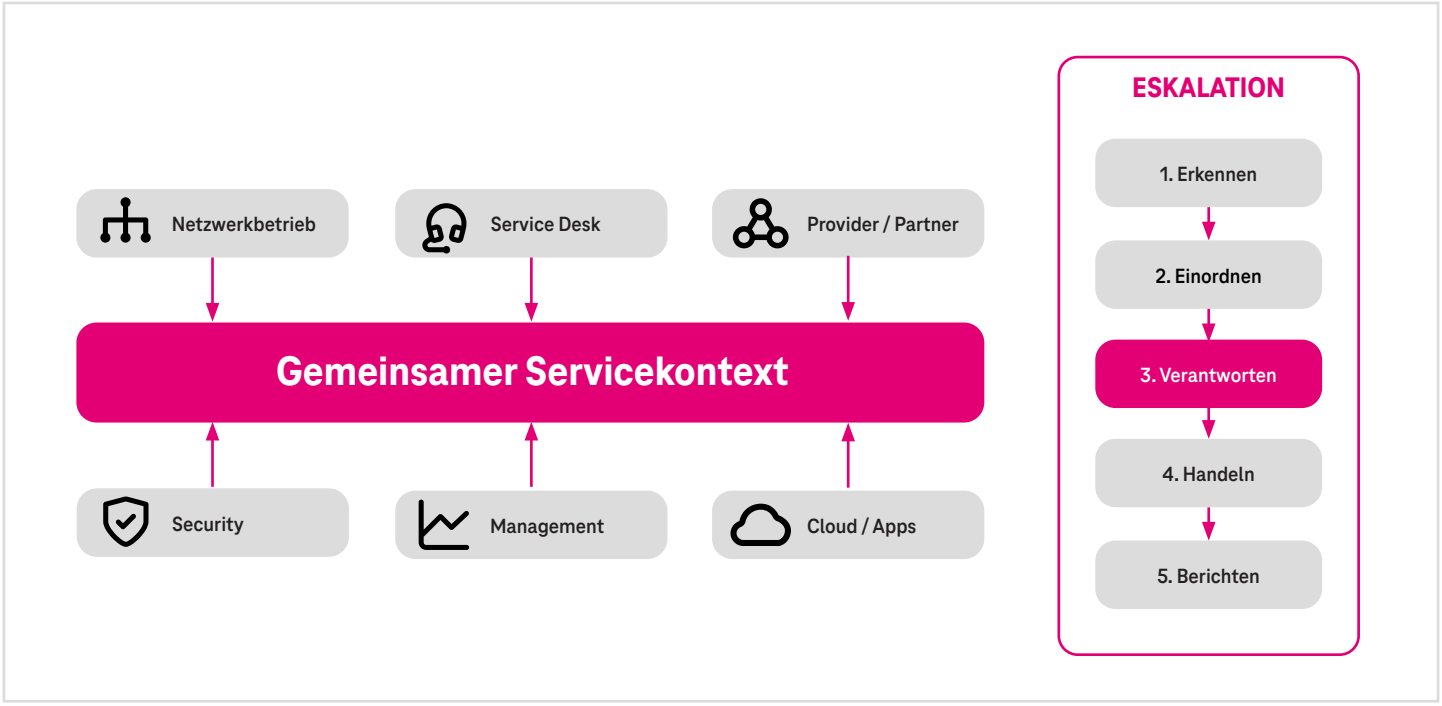


Abbildung 4: Observability erfordert zur Wertentfaltung einen gemeinsamen Servicekontext

Für den Betrieb bedeutet das: Observability-Daten müssen in Incident Management, Problem Management, Change Management und Service Reporting eingebunden werden. Incident Management adressiert aktuelle Störungen, Problem Management sucht wiederkehrende Ursachen, Change Management bewertet die Wirkung von Änderungen. Wenn Observability-Signale nicht mit diesen Prozessen verbunden sind, bleiben sie Analysehilfen einzelner Teams. Werden sie dagegen in Tickets, Eskalationspfade und Serviceberichte integriert, entsteht eine gemeinsame Entscheidungsgrundlage.

Governance spielt dabei eine zentrale Rolle. Unternehmen sollten festlegen, welche Datenquellen verbindlich sind, welche Dashboards für welche Rollen gelten, wie Datenqualität geprüft wird und welche Eskalationsregeln bei Providergrenzen greifen. Für Unternehmen mit Standorten in mehreren Ländern kommt hinzu, dass lokale Provider, unterschiedliche Service-Level, Zeitfenster und regulatorische Rahmenbedingungen berücksichtigt werden müssen. Observability kann diese Komplexität nicht beseitigen, aber sie kann helfen, technische und organisatorische Abhängigkeiten strukturierter sichtbar zu machen.

Bei integrierten Netzwerk- und Security-Architekturen wie SASE müssen Netzwerk- und Sicherheitsdaten gemeinsam ausgewertet werden. Dafür ist festzulegen, welche Teams die Daten interpretieren und wer daraus Massnahmen ableitet.

Compliance berührt Observability vor allem dort, wo Daten erfasst, gespeichert, korreliert und ausgewertet werden. Logs, Flow-Daten, Nutzerkontext, Standortinformationen und Security-Ereignisse können datenschutz- oder regulierungsrelevant sein. Deshalb sollten Datenresidenz, Zugriffskontrollen, Aufbewahrungsfristen, Rollenrechte und Nachvollziehbarkeit früh geprüft werden. Aussagen wie „erfüllt NIS2“ oder „macht compliant“ wären ohne rechtliche und fachliche Prüfung riskant. Ein strukturiertes Observability-Modell kann Unternehmen dabei unterstützen, technische und organisatorische Anforderungen nachvollziehbarer zu bewerten und Nachweise besser vorzubereiten. Ob konkrete regulatorische Anforderungen erfüllt werden, hängt von Architektur, Branche, Land, Verantwortlichkeiten und weiteren Massnahmen ab.

Die zentrale Betriebsfrage lautet damit nicht, ob ein Unternehmen genügend Daten hat. Sie lautet, ob Daten, Rollen und Prozesse so verbunden sind, dass Teams konsistent handeln können. Observability wird so zu einem Bestandteil der Governance: Sie verbindet technische Transparenz mit klaren Zuständigkeiten, abgestimmten Eskalationswegen und nachvollziehbaren Entscheidungen.

Observability einführen: wichtige Schritte und typische Stolpersteine

Stolpersteine im Überblick

- **Tool zuerst:** Auswahl einer Plattform, bevor Use Cases und Ziele geklärt sind
- **Zu viele Daten ohne Kontext:** Datenflut durch mehr Telemetrie statt besserer Ursachenanalyse
- **Unklare Rollen:** Teams interpretieren Daten unterschiedlich, Verantwortlichkeiten bleiben offen
- **Zu grosser Pilot:** Ein überladener Pilot überfordert die beteiligten Teams
- **Datenschutz und Compliance:** zu späte Einbindung und fehlende Prüfungen können spätere Anpassungen erzwingen
- **Zu hohes Nutzenversprechen:** Aussagen verlieren an Glaubwürdigkeit, wenn die organisatorischen Voraussetzungen fehlen

Die Einführung von Network Observability sollte nicht mit der Auswahl einer Plattform beginnen. Ein Tool kann Daten sammeln, visualisieren und korrelieren. Es entscheidet aber nicht, welche geschäftskritischen Services priorisiert werden, welche Daten verlässlich sind, welche Teams Verantwortung übernehmen und wie Eskalationen ablaufen. Unternehmen sollten deshalb mit einem konkreten Betriebsproblem starten, nicht mit einer vollständigen Zielarchitektur.

Ein sinnvoller Einstieg ist die Priorisierung weniger, aber relevanter Use Cases. Für Unternehmen mit vielen verteilten Standorten können das wiederkehrende Performance-Probleme in Filialen sein, schwer erklärbare SaaS-Verzögerungen, unklare Cloud-Latenzen, WLAN-Probleme an einzelnen Standorttypen, Auswirkungen von Security-Inspection oder eskalationsintensive Providerfälle. Der Use Case bestimmt, welche Datenquellen benötigt werden. Er verhindert, dass Observability zu einem breit angelegten Datensammelprojekt wird, dessen Nutzen schwer zu erklären ist.

Im nächsten Schritt sollten Unternehmen die vorhandenen Datenquellen und deren Qualität bewerten. Relevante Signale können aus WAN, LAN, WLAN, SD-WAN, SASE, Firewalls, DNS, Cloud-Anbindungen, Endgeräten, Applikationsmonitoring, synthetischen Tests und ITSM-Systemen kommen. Dabei geht es nicht um Voll-

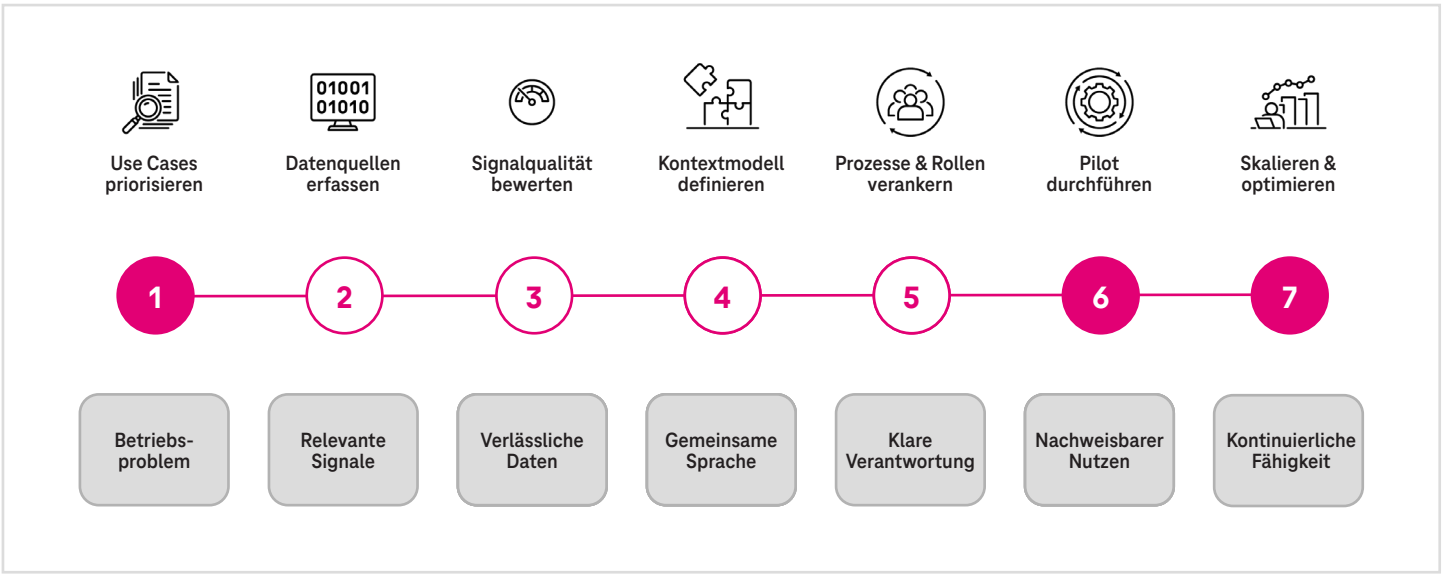


Abbildung 5: Die erfolgreiche Einführung von Observability beginnt mit der Definition eines Betriebsproblems, nicht mit der Auswahl einer Plattform

ständigkeit um jeden Preis. Wichtiger ist die Frage, welche Daten helfen, konkrete Ursachenhypothesen zu bilden. Ein hoher Datenumfang ohne Standort-, Service- und Providerkontext erzeugt häufig mehr Analyseaufwand statt mehr Klarheit.

Danach braucht es ein gemeinsames Kontextmodell. Unternehmen sollten definieren, welche Standorte, Anwendungen, Nutzergruppen, Provider, Policies, Serviceklassen und Betriebsprozesse miteinander verknüpft werden. Für einen Handelskonzern kann die Filialkritikalität entscheidend sein. Für ein Produktionsunternehmen können Werke, OT-nahe Netze und Campus-Infrastrukturen im Vordergrund stehen. Für ein Finanzunternehmen kann der Nachweis von Zugriffen, Rollen und Servicequalität wichtiger sein. Observability muss diese Unterschiede abbilden, ohne das Modell zu überfrachten.

Erst auf dieser Basis sollten Plattform, Integrationen und Automatisierung betrachtet werden. Eine Observability-Plattform sollte Daten aufnehmen, korrelieren und für unterschiedliche Rollen nutzbar machen. Aber sie muss auch in die bestehenden Prozesse passen: Service Desk, Incident Management, Change Management, Security Operations, Providersteuerung und Management-Reporting. Eine technische Integration ohne Prozessintegration führt häufig zu neuen Dashboards, aber nicht zu besseren Entscheidungen.

Ein Pilot ist der richtige Weg, um die Tragfähigkeit des Modells zu prüfen. Er sollte nicht zu gross sein, aber relevant genug, um echte Betriebsfragen zu beantworten. Geeignete Erfolgskriterien sind zum Beispiel eine klarere Ursachenklassifikation, weniger manuelle Datensuche, bessere Providereskalation, höhere Aussagekraft von Reports oder bessere Nachvollziehbarkeit von Changes. Somit kann ein Pilot zeigen, ob Ursachen schneller eingegrenzt und Verantwortlichkeiten klarer zugeordnet werden können.

Die Skalierung folgt erst danach. Unternehmen können weitere Standorte, Anwendungen, Provider und Datenquellen einbinden, wenn Datenmodell, Rollen, Dashboards und Prozesse funktionieren. Dabei sollte Observability als kontinuierliche Betriebsfähigkeit verstanden werden. Standortnetze verändern sich, Cloud-Zugriffe wachsen, Security-Policies werden angepasst, Provider wechseln, neue Anwendungen kommen hinzu. Observability muss deshalb gepflegt, überprüft und weiterentwickelt werden.

Typische Stolpersteine entstehen dort, wo Unternehmen diese Reihenfolge umdrehen. Ein Tool-first-Ansatz führt oft zu schneller Datensammlung, aber langsamer Nutzenklärung. Mehr Telemetrie ohne Kontext erzeugt Datenflut. Unklare Rollen führen zu widersprüchlichen Interpretationen. Zu grosse Pilotumfänge überfordern Teams. Fehlende Datenschutz- und Compliance-Prüfung kann spätere Anpassungen erzwingen. Und überzogene Nutzenversprechen schwächen die Glaubwürdigkeit eines Programms, wenn die organisatorischen Voraussetzungen fehlen.

Die Einführung gelingt deshalb am besten als schrittweiser Betriebsaufbau. Use Case, Datenquelle, Kontextmodell, Prozessintegration, Pilot und Skalierung bilden eine Kette. Wenn eines dieser Elemente fehlt, bleibt Network Observability technisch interessant, aber betrieblich unvollständig.

Welche organisatorische und wirtschaftliche Wirkung realistisch ist

Der wirtschaftliche Wert von Observability liegt nicht in der blossen Sichtbarkeit von Daten. Sichtbarkeit allein spart keine Kosten, verhindert keine Störungen und verbessert keine Servicequalität. Wirkung entsteht dort, wo Daten in bessere Entscheidungen übersetzt werden: schnellere Eingrenzung von Ursachen, klarere Eskalationen, bessere Priorisierung von Modernisierungsmassnahmen, nachvollziehbarere Providersteuerung und belastbarere Kommunikation gegenüber Fachbereichen.

Für IT-Entscheider ist dabei wichtig, Nutzen realistisch zu formulieren. Observability kann dazu beitragen, manuelle Suchaufwände transparenter zu machen, wenn Datenquellen konsistent verbunden sind. Sie kann die Providersteuerung erleichtern, wenn technische Signale, Service-Level und Eskalationspfade nachvollziehbar zusammengeführt werden. Sie kann Change-Prozesse unterstützen, wenn Veränderungen an Netzwerk, Security oder Cloud-Anbindung besser mit späteren Effekten verknüpft werden. Diese Wirkungen sind plausibel, aber sie hängen stark von Ausgangslage, Datenqualität, Architektur und Betriebsmodell ab.

Observability kann Silos zwischen Teams verringern, wenn alle auf denselben Kontext zugreifen. Ursachen lassen sich so gemeinsam bewerten, ohne Zuständigkeiten zu verwischen. Ein gutes Modell macht transparent, wer Daten interpretiert, Massnahmen auslöst und Eskalationen verantwortet. Das strukturiert die Zusammenarbeit.

Auch für Managementkommunikation kann Observability wertvoll sein. Führungskräfte benötigen keine Rohdaten zu Paketverlust oder Flow-Statistiken. Sie brauchen eine belastbare Einschätzung, welche Standorte betroffen sind, welche Geschäftsprozesse beeinflusst werden, ob ein Providerproblem vorliegt, ob ein Change ursächlich sein könnte und welche Massnahmen priorisiert werden sollten. Observability kann helfen, technische Analysen in eine serviceorientierte Sprache zu übersetzen.

In Unternehmen mit vielen Standorten kann zudem die Modernisierungsplanung profitieren. Wenn wiederkehrende Störungen, Standorttypen, Providerabhängigkeiten oder Applikationspfade transparent werden, lassen sich Investitionen besser priorisieren. Ein Unternehmen erkennt dann eher, ob ein Problem durch lokale WLAN-Modernisierung, WAN-Anpassung, SD-WAN-Policy, Cloud-Anbindung, Security-Architektur oder Prozessänderung adressiert werden sollte. Das kann die Grundlage für bessere Budgetentscheidungen schaffen, ersetzt aber keine Wirtschaftlichkeitsrechnung.

Die realistische Wirkung liegt damit in drei Bereichen: bessere Transparenz über verteilte Infrastrukturen, bessere Steuerbarkeit von Betriebs- und Providerprozessen sowie bessere Entscheidungsgrundlagen für Modernisierung und Governance. Das ist weniger spektakulär als ein pauschales Einsparversprechen, aber für grosse Unternehmensnetze deutlich belastbarer.



Abbildung 6: Observability liefert keine pauschalen Einsparversprechungen, jedoch bessere Transparenz, Steuerbarkeit und Entscheidungen

Observability Checkliste für IT-Entscheider

Vor einer Entscheidung für Observability sollten Unternehmen nicht nur Plattformfunktionen vergleichen. Entscheidend ist, ob das Zielbild zur eigenen Standortlandschaft, Betriebsorganisation und Providerstruktur passt.

Strategische Relevanz und Scope

- Welche Standorte, Anwendungen und Geschäftsprozesse sind besonders kritisch?
- Welche wiederkehrenden Störungen verursachen heute den höchsten Analyse- oder Eskalationsaufwand?
- Geht es primär um Netzwerkbetrieb, Nutzererfahrung, Providersteuerung, Security-Kontext oder Cloud-Zugriffe?
- Welche Standorte liegen in anderen Ländern, und welche zusätzlichen Provider-, Service- oder Governance-Fragen entstehen dadurch?

Datenquellen und Architektur

- Welche Datenquellen sind heute verfügbar: WAN, LAN, WLAN, SD-WAN, SASE, Cloud, DNS, Endgeräte, Applikationen, ITSM?
- Welche Daten fehlen, um Ursachen über Standort-, Provider- und Servicegrenzen hinweg zu verstehen?
- Können technische Signale mit Standort, Anwendung, Nutzergruppe, Provider, Policy und Change-Historie verknüpft werden?
- Welche Integrationen in bestehende Netzwerk-, Security-, Cloud- und ITSM-Systeme sind erforderlich?

Security, Datenschutz und Compliance

- Welche Logging-, Datenresidenz-, Zugriffskontroll- und Aufbewahrungsanforderungen gelten?
- Welche Security-Daten dürfen in welchem Kontext verarbeitet und korreliert werden?
- Welche regulatorischen Aussagen müssen durch Legal, Compliance oder Fachbereiche geprüft werden?

Betrieb und Governance

- Wer besitzt Datenqualität, Dashboards, Alert-Regeln und Korrelationslogik?
- Welche Teams interpretieren Observability-Daten, und wer entscheidet über Massnahmen?
- Wie werden Providereskalationen dokumentiert, gesteuert und nachverfolgt?
- Wie werden Observability-Erkenntnisse in Incident, Problem, Change und Reporting überführt?

Pilot und Skalierung

- Welcher Use Case eignet sich für einen überschaubaren, aber relevanten Pilot?
- Welche Erfolgskriterien sind realistisch messbar, ohne unbelegte Effizienzclaims zu erzeugen?
- Wie wird das Modell nach dem Pilot auf weitere Standorte, Provider, Anwendungen und Sicherheitsdomänen erweitert?
- Welche Rolle soll ein Managed-Service-Partner übernehmen: Beratung, Integration, Betrieb, Eskalation oder kontinuierliche Optimierung?



Welche nächsten Schritte Unternehmen jetzt prüfen sollten

Observability ist keine Abkürzung, die komplexe Unternehmensnetze automatisch einfacher macht. Sie ist ein strukturierter Weg, um Komplexität besser zu verstehen und betriebliche Entscheidungen nachvollziehbarer zu treffen. Für Unternehmen mit vielen verteilten Standorten wird diese Fähigkeit wichtiger, weil Netzwerk, Cloud, Security, Provider und Nutzererfahrung enger zusammenwirken.

Der nächste sinnvolle Schritt ist eine Standort- und Use-Case-Analyse. Unternehmen sollten identifizieren, welche Services, Standorte und Störungsbilder besonders relevant sind. Danach folgt eine Bewertung der vorhandenen Datenquellen: Welche Signale sind verfügbar, welche fehlen, welche sind verlässlich und welche lassen sich miteinander verknüpfen? Erst daraus ergibt sich, welche Plattform, welche Integrationen und welches Betriebsmodell sinnvoll sind.

Parallel sollten Verantwortlichkeiten geklärt werden. Observability betrifft Netzwerkbetrieb, Security, Cloud, Service Desk, Applikationsbetrieb, Providersteuerung und Management-Reporting. Wenn diese Rollen nicht früh eingebunden werden, entsteht ein technisches Projekt ohne ausreichende betriebliche Verankerung. Ein Pilot sollte daher nicht nur technische Daten erfassen, sondern auch Eskalation, Reporting und Entscheidungslogik testen.

Die Deutsche Telekom kann in dieser Phase als Architektur-, Integrations- und Betriebspartnerin zur Seite stehen. Sie bringt ein umfangreiches Lösungsspektrum sowie jahrelange Erfahrung aus den Bereichen Konnektivität, SD-WAN, SASE, LAN/WLAN, Cloud-Anbindung, Security und Managed Services zusammen. Welche Kombination daraus geeignet ist, sollte aus den priorisierten Use Cases und dem Zielbild abgeleitet werden. So bleibt Observability ein kundenseitiges Betriebsmodell und wird nicht auf eine einzelne Produktentscheidung reduziert.

Die Schlussfolgerung lautet: Unternehmen sollten Observability nicht als weiteres Monitoring-Projekt starten. Sie sollten es als Modernisierung des Netzwerkbetriebs verstehen. Entscheidend ist der Weg von Daten zu Kontext, von Kontext zu Verantwortung und von Verantwortung zu besseren Entscheidungen.

Bildquellen / Grafiken:

- Adobe Stock (Seiten 1, 2, 5, 11)
- Deutsche Telekom (Seiten 3, 4, 6, 7, 9, 10)

Deutsche Telekom Geschäftskunden GmbH | 10/2026 | Text mit Unterstützung von KI erstellt | CF

Melden Sie sich für eine persönliche Beratung!

Kontakt
telekom.de/business

Herausgeber
Deutsche Telekom
Geschäftskunden GmbH
Landgrabenweg 149
53227 Bonn

Connecting your world.