



The bridge to possible

2024

Global Networking Trends Report

Netzwerkstrategien für modernes
Digital Business



Willkommen beim Global Networking Trends Report 2024



Jonathan Davidson
Executive Vice President
& General Manager,
Cisco Networking

Mehr als 25 Jahre bin ich nun bereits in der Netzwerkbranche tätig. Konstant blieb in all der Zeit vor allem eines: die stetig zunehmende Bedeutung des Netzwerks. So ist das Netzwerk auch alles andere als ein Allerweltsprodukt, sondern untrennbar mit den geschäftlichen Strategien der von uns Befragten verbunden. Unsere Untersuchungen zeigen zudem, dass fortschrittlichere Netzwerkumgebungen zu besseren geschäftlichen Ergebnissen führen.

Als IT-Verantwortliche wissen Sie, dass Faktoren wie künstliche Intelligenz (KI), Cloud, hybrides Arbeiten, containerisierte Apps und das Internet of Things (IoT) Innovationen vorantreiben – wenn sie nicht durch Komplexität ausgebremst wird. Die Qualität der User Experience (UX), die über das Netzwerk umgesetzt wird, hängt letztlich von Ihren Maßnahmen ab. Und häufig leidet diese infolge zunehmender Komplexität und unzeitgemäßer Ansätze rund um das Netzwerk sowie dadurch, dass es an den passenden Skill-Sets fehlt.

Dieser Report beleuchtet aktuelle Herausforderungen im Netzwerkkontext, IT- und Business-Prioritäten, Reifegrade von Architekturen und Investitionsstrategien anhand der Daten aus einer weltweiten Umfrage unter 2.052 IT-Führungskräften und -ExpertInnen in Unternehmen aus 10 unterschiedlichen Branchen. Das Ziel bestand dabei darin, Einblicke zu den Antriebsfaktoren für die Transformation von Netzwerken zu erhalten. Für mich stechen dabei drei Punkte besonders heraus, die auch in meinen Gesprächen mit Kunden ein häufiges Thema sind: die Plattform, Sicherheit und KI.

- **Die Plattform:** Eine Plattform für zentralisiertes Netzwerkmanagement ist ein entscheidender Transformationsfaktor, verhilft sie IT-Teams doch zu mehr Transparenz, Konnektivität und Sicherheit in einer Welt, die von Private- und Public-Cloud-Umgebungen ebenso geprägt ist wie von On-Premises-Workloads.
- **Sichere Netzwerke:** Cybersecurity-Fragen stehen bei den Befragten ganz oben auf der Liste. Unabhängig von der Branche erkennen sie das Potenzial, das IT-generierte Einblicke bieten, um mit der unablässigen Weiterentwicklung der Bedrohungslandschaft Schritt zu halten. Die Devise lautet: Was vernetzt ist, muss geschützt werden.
- **Für KI – und mit KI:** Unternehmen stoßen Modernisierungen ihrer Infrastrukturen zur Bewältigung von KI-Workloads und zur Verbesserung der Nachhaltigkeit ihrer Rechenzentren an. Zugleich nutzen sie KI zur Optimierung ihrer Netzwerke, zur Vorhersage von Ausfällen und zur Diagnose von Problemen.

Der Global Networking Trends Report 2024 liefert einen objektiven Blick darauf, welche Themen IT-Verantwortliche als kritisch einschätzen, um über das Netzwerk eine sichere Digital Experience für alle zu gewährleisten. Ich hoffe, Sie finden ihn so aufschlussreich und nützlich wie ich.



Jonathan Davidson



Inhalt

4 Überblick

5 Transformation von Architekturen

- Trend: Netzwerkplattformen im Aufwind
- Trend: Digital Experience Assurance für mehr Verlässlichkeit und Konsistenz
- Trend: Fokus auf Partner-Ecosystems und offene API-Integrationen

11 Security-Konvergenz

- Trend: Konvergenz von Netzwerk und Security als Mittel gegen Konsistenzprobleme
- Trend: Sicherheit von Multicloud-Netzwerken
- Trend: Cloud-basierte Sicherheit als wichtigster Bereich für Netzwerkinvestitionen

17 KI-Abläufe

- Trend: KI-Einsatz für mehr betriebliche Effizienz
- Trend: Daten-Governance und KI-gestützte Analytik für prädiktive Assurance
- Trend: KI-gestützte Sicherheit zur Risikominimierung

22 Skalierbares Rechenzentrum

- Trend: Priorität auf Modernisierung von Rechenzentren zur Skalierung von KI-Workloads
- Trend: KI und Plattformen hoch im Kurs bei Betreibern von Rechenzentren

26 Nachhaltigkeitsfortschritt

- Trend: Datengesteuerte Förderung von Nachhaltigkeit durch die IT
- Trend: Priorität auf Infrastruktur-Telemetrie und Transparenz
- Trend: Planung von Gebäudeinfrastruktur für mehr Effizienz und bessere Erlebnisse

32 Fazit

33 Methodik

Übersicht

Digitale Geschäftsprozesse erfordern einfachere, sicherere, besser skalierbare und nachhaltigere Netzwerke. Der diesjährige Global Networking Trends Report identifiziert fünf strategische Bereiche, deren Weiterentwicklung dabei entscheidend ist.



Architekturtransformation

Als Weg zur Vereinfachung von Betriebsabläufen und zur Stärkung digitaler Resilienz rückt neben einer Netzwerkplattform und einem integrierten Partner-Ecosystem auch die Absicherung der Digital Experience durch erweiterte Netzwerk-Telemetrie und End-to-End-Transparenz zunehmend in den Fokus.



Security-Konvergenz

Da Bedenken bezüglich der Sicherheit mit zunehmender Verbreitung der Cloud eine immer wichtigere Rolle spielen, gehört die Konvergenz von Netzwerk- und Security-Technologien wie auch der zugehörigen Workflows inzwischen zu den wichtigsten Prioritäten und Best Practices.



KI-Abläufe

KI-gestützte Automatisierung steht hoch im Kurs als Strategie zur Vereinfachung und Optimierung von Betriebsabläufen sowie dafür, die Digital Experience abzusichern und durch die Stärkung der Sicherheit Risiken zu minimieren.



Skalierbares Rechenzentrum

Aktuell findet eine Modernisierung der Rechenzentren statt, um die Anforderungen an KI-Workloads und neue Applikationen nach Maß zu erfüllen und im gleichen Zug die Komplexität anhand KI-nativer Plattformen in den Griff zu bekommen.



Nachhaltigkeitsfortschritt

Die IT will mit der Hilfe von Netzwerkplattformfunktionen die Telemetrie und Sichtbarkeit voranbringen und intelligente, nachhaltige Gebäude umsetzen, um Unternehmensziele im Bereich Klimaneutralität zu erreichen.



Architektur- transformation

IT-Verantwortliche und ihre Teams haben noch immer mit dem wenig effizienten und komplexen Infrastruktur-Framework zu kämpfen, das durch Punktlösungen entstand, die aufgrund zeitkritischer Anforderungen in der Pandemie benötigt wurden. Viele wollen daher auf einen Architekturansatz umstellen, der durch End-to-End-Transparenz und -Kontrolle über alle Netzwerkdomänen hinweg für mehr Effizienz sorgt.

42 % der IT-Verantwortlichen und -ExpertInnen sehen eine Netzwerkplattform als Lösung, die das Management domänenübergreifend vereinfachen und so zu mehr Performance und Innovation sowie Kosteneinsparungen beitragen kann.

Eine **Netzwerkplattform** führt Software, Richtlinien und offene APIs in einem integrierten System mit einer intuitiven Benutzeroberfläche, erweiterter Telemetrie und Automatisierung zusammen. Für Betriebspersonal wird so zentralisiertes End-to-End-Netzwerkmanagement möglich, wobei ein API-gesteuertes Ecosystem Abläufe etwa auch bei der Umsetzung von Digital Experiences über eine oder mehrere Netzwerkdomänen hinweg vereinfacht.

Durch die Weiterentwicklung in Richtung einer **KI-nativen Netzwerkplattform** profitieren IT-Teams durchgängig von Intelligence-Daten und automatisierten Steuerungen zur konsistenten Gewährleistung einer Digital Experience von hoher Qualität.

Trend

Netzwerkplattformen im Aufwind

Nach Ansicht der Befragten muss das Netzwerk eine tragendere Rolle bei der Umsetzung dynamischer IT- und Business-Initiativen einnehmen – von der Optimierung der End User Experience sowie der Netzwerk- und Security-Performance bis hin zur Kostenkontrolle im Betrieb. Für IT-Verantwortliche und ExpertInnen gilt eine Netzwerkplattform dabei als Lösung für eine Architektur, die sich durch mehr Effizienz und Konsistenz auszeichnet und diese und andere Initiativen so durch eine domänenübergreifend vereinfachte Integration und optimierte Performance unterstützen kann.

Heute

Rund ein Fünftel (21 %) der befragten Unternehmen hat derzeit mehrere separate Managementsysteme für seine Campus-, Zweigstellen, WAN-, Rechenzentrums- und Multicloud-Domänen im Einsatz. Zugleich stützen derzeit aber bereits 39 % zumindest einige ihrer Netzwerkdomänen auf eine Plattformarchitektur. Insgesamt erfährt ein plattformorientierter Netzwerkansatz unter den Befragten eine enorme Fürsprache angesichts der Vorteile, die er ihnen bei der Umsetzung ihrer IT- und Business-Ziele in Aussicht stellt. Dazu gehören schnellere IT- und Business-Innovation (43 %), eine Verbesserung der Netzwerk-Performance und des Sicherheitsstatus (40 %) und Kosteneinsparungen (37 %).

Neben den Vorteilen einer Netzwerkplattform erkennen die Befragten auch die Bedeutung von Cloud-basiertem Management: Derzeit setzen 33 % darauf für ihr LAN, WAN und SD-WAN. Als Vorteile von Cloud-basiertem Management nennen die Befragten erhöhte Netzwerksicherheit (45 %), eine schnellere Infrastrukturbereitstellung (41 %) sowie schnelleren Zugang zu neuen Management-Features (39 %).

„Unternehmen können durch einen plattformorientierten Ansatz von vereinfachtem Management und fortschrittlicher Funktionalität profitieren. Wer dies umsetzt, wird im Wettbewerbsumfeld des digitalen Zeitalters stärker aufgestellt sein.“¹

Brandon Butler, Research Manager Enterprise Networks, IDC



Ausblick auf die nächsten zwei Jahre

Netzwerkplattformen dürften künftig auf noch breiterer Basis Anwendung finden: Mit 72 % erwarten knapp zwei Drittel der Befragten, eine entsprechende Architektur über eine oder mehrere Domänen hinweg zu implementieren. 39 % von ihnen gehen dabei von einer Ausweitung der Plattformarchitektur auf sämtliche Netzwerkdomänen aus. Dies verspricht eine enorme Vereinfachung des Netzwerkmanagements und zahlreiche geschäftliche, betriebliche und technische Vorteile – von offenen API-Ecosystems über eine bessere Zusammenarbeit zwischen IT-Fachbereichen bis hin zu vereinfachten Integrationen und einem umfassenden Datenpool. Letzterer entsteht durch Aggregation von Telemetrie aus sämtlichen Netzwerkdomänen und ermöglicht unternehmensweite Einblicke anhand KI-gestützter Analytik, die bei der Optimierung von Performance und UX, Sicherheit und Kosteneffizienz sowie der Nachhaltigkeit helfen können.

72%

der IT-Verantwortlichen und -ExpertInnen sehen eine oder mehrere ihrer Netzwerkdomänen in den kommenden zwei Jahren unter dem Dach einer Plattformarchitektur.

➤ Lesen Sie das [IDC-Whitepaper](#) zum plattformorientierten Netzwerkansatz.



„Cloud-basierte Plattformen machen alles deutlich einfacher: Mein Team kann Usern Möglichkeiten aufzeigen, die weit über einfaches Netzwerk-Troubleshooting hinausgehen. Unsere Innovationskraft steigt dadurch bedeutend.“

Jack Satterfield,
Chief Technology Officer,
Pima Community College



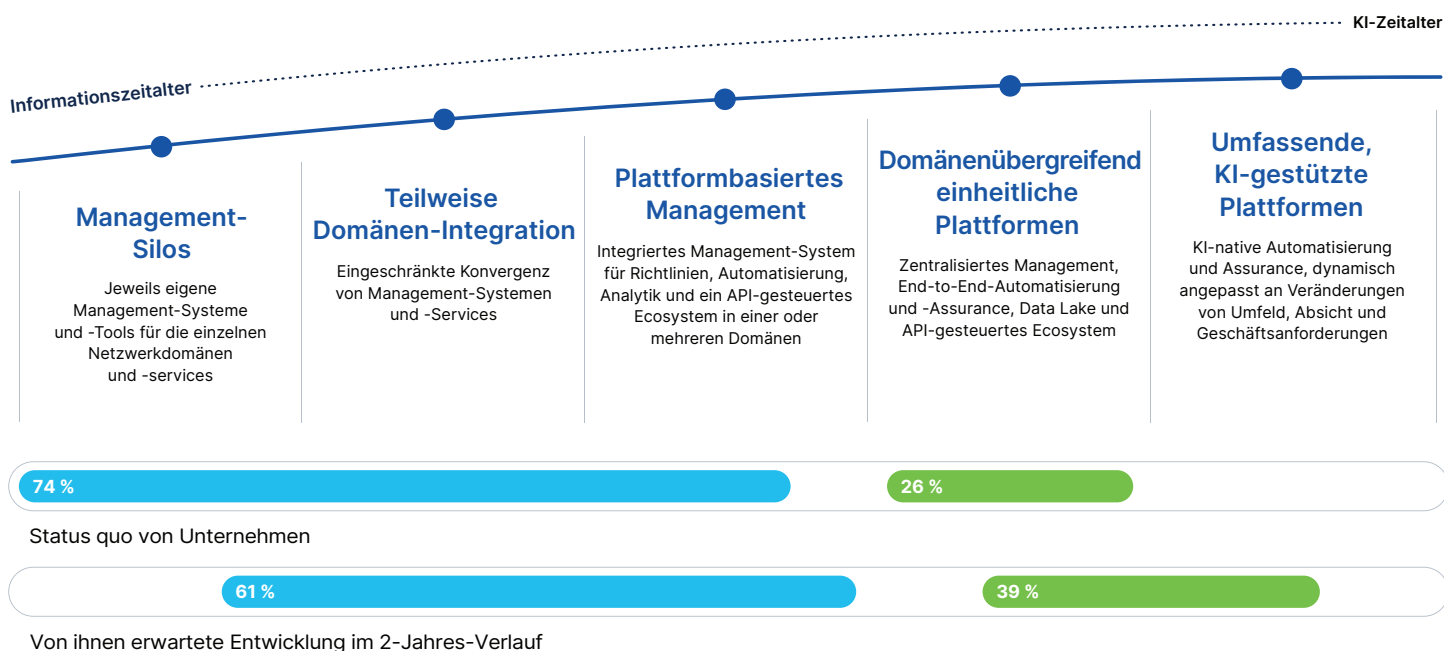


„Mit Daten aus dem Gesamtunternehmen, die in eine Plattform eingespeist und KI-gestützt in Einblicken und Empfehlungen aufbereitet werden, wird End-to-End-Transparenz zur Identifikation und Behebung potenzieller Performance- und Konnektivitätsprobleme möglich. Im Verbund mit einem offenen und erweiterbaren Entwickler-Ecosystem können IT-Teams eine solche Plattform tief in ihre Business-Workflows integrieren und schnelleren Mehrwert durch Automatisierung generieren.“

Lawrence Huang, Senior Vice President & General Manager, Cisco Networking – Meraki & Wireless

Reifegrad der Netzwerkarchitektur (aktuell vs. 2-Jahres-Ausblick)

Der Begriff „Netzwerkarchitektur“ beschreibt das Infrastrukturdesign des Unternehmensnetzwerks einschließlich Lifecycle-Management und Governance der verschiedenen Domänen wie Campus, Zweigstelle, WAN, Rechenzentrum, Multicloud, industrielle Netzwerke etc.





Ausblick auf die nächsten zwei Jahre

75 % aller Befragten planen den Einsatz von Tools, die End-to-End-Transparenz in einer zentralen Konsole ermöglichen. Davon erwarten 38 %, dass sie ihre Digital Experience Assurance auf KI stützen werden, sowie 37 %, dass sie End-to-End-Transparenz über eine zentrale Konsole umsetzen werden. Eine KI-native Netzwerkplattform, die Datenbestände aus verschiedenen Netzwerkdomänen zusammenführt und anhand von KI bzw. Machine Learning (ML) analysiert, trägt zu einer Entscheidungsfindung im Sinne proaktiver und vorausschauender statt reaktiver Betriebsabläufe bei.

75 %

der Unternehmen wollen sich in den kommenden zwei Jahren End-to-End-Transparenz durch eine zentrale Konsole verschaffen, um Digital Experiences von hoher Qualität zu gewährleisten.

Trend

Digital Experience Assurance für mehr Verlässlichkeit und Konsistenz

Digital Experience Assurance bezeichnet die Fähigkeit, über sämtliche unternehmenseigenen (Rechenzentrum, Campus und Zweigstelle, WAN- und industrielle Netzwerke) und externen Domänen (Internet, Cloud-Provider, Multicloud) hinweg ein verlässliches Benutzererlebnis unabhängig von Geräten, Apps oder Services zu gewährleisten. Daten werden dabei korreliert und kontextualisiert, um durchgängig Intelligence zu erhalten und Korrekturmaßnahmen an jedem Punkt des End-to-End-Netzwerks zu automatisieren. So können IT-Teams digitale Resilienz und im gleichen Zug stets verfügbare Digital Experiences von hoher Qualität für MitarbeiterInnen, Kunden und das Unternehmen insgesamt gewährleisten.

Heute

Ob für Kunden oder MitarbeiterInnen, IT-Verantwortliche betrachten die Netzwerk-UX ganz klar als Kernsäule für die Förderung von geschäftlichem Erfolg im Umfeld der Digitalisierung. Infolge der zunehmenden Verteilung von Belegschaften, Apps und Services gestaltet es sich jedoch schwieriger, die Hops zwischen Netzwerk-, Cloud- und Internet-Domänen klar nachzuvollziehen. Der Grund hierfür ist, dass der Anfangs- und Endpunkt vieler dieser Verbindungen außerhalb der klassischen Unternehmensinfrastruktur liegt. So beklagt mehr als ein Drittel (35 %) der Befragten, dass es ihnen im Hinblick auf komplette Netzwerkpfade bis ins Internet und Cloud-Netzwerk an Transparenz fehlt. Nach Aussage von 41 % der Befragten muss zudem die Verlässlichkeit ihrer Services deutlich verbessert werden, um Konsistenz in puncto UX und App-Bereitstellung vorhersehbar gewährleisten zu können. Andernfalls werden sie ihre IT- und Business-Ziele nicht umsetzen können.

Ein End-to-End-Ansatz an Digital Experience Assurance, der sämtliche unternehmenseigenen und externen Netzwerkpfade abdeckt, ist für die Gewährleistung digitaler Resilienz unabdingbar. Entgegen dem geben 39 % der Befragten an, ihr Digital-Experience-Monitoring über mehrere Konsolen umzusetzen und so entweder eingeschränkte oder vollständige Transparenz über User, Geräte, Apps und Services hinweg zu erhalten.

„In unserem Netzwerk kann schon eine kleine Störung große Auswirkungen haben. Deshalb müssen wir unsere Services von Anfang an absichern.“

Simon Challis, Senior Technology Manager, Platform Design, EasyJet

Trend

Fokus auf Partner-Ecosystems und offene API-Integrationen

Da es für die IT gilt, ihre Infrastruktur sowie unternehmenseigene Gebäude schnellstmöglich nachhaltiger zu gestalten, ist sie zunehmend auf ausgedehnte Partner-Ecosystems und Plattformen angewiesen, die sich anhand von offenen APIs integrieren lassen.

Heute

In den Netzwerken von rund einem Fünftel (21 %) der Befragten sind derzeit keinerlei API-gestützte Ecosystem-Integrationen im Einsatz. Bei weiteren 22 % bestehen in eingeschränktem Maße IT-Integrationen über fragmentierte Netzwerkdomeänen hinweg.

Im Hinblick auf Netzwerkinvestitionen liegt bei mehr als einem Viertel (26 %) in den kommenden 12 Monaten höchste Priorität auf Management-Plattformen für vereinfachte Betriebsabläufe und API-gestützte Integrationen. 33 % nennen dabei die Möglichkeit zur Integration in ihre bestehenden Netzwerke als wichtigstes Kriterium für die Evaluierung entsprechender Technologieinvestitionen. Nach Aussage von 29 % kann das Netzwerk durch ein erweiterbares Ecosystem mit Plattformen, die Technologie-Innovationen durch offene APIs und Partner-Integrationen ermöglichen, besser zum Erfolg von IT und Business beitragen.



Ausblick auf die nächsten zwei Jahre

Mit 64 % erwartet die Mehrheit der Befragten, anhand von APIs in den kommenden zwei Jahren einheitliche Integrationen zur Förderung von IT- und Business-Innovation zu implementieren. 20 % von ihnen gibt an, auf dem Weg dorthin ein API-gesteuertes Intent-Based-Netzwerk umzusetzen. Entsprechende Netzwerke abstrahieren die Komplexitäten der unteren Netzwerkebenen. Dies ermöglicht die Entwicklung nachhaltiger Anwendungen, die Netzwerkressourcen gemäß dem aktuellen Bedarf dynamisch anfordern. Ressourcen werden so effizienter genutzt und dadurch der ökologische Fußabdruck verkleinert. 40 % sehen erhebliche Potenziale, ihre Strategie rund um Nachhaltigkeit mit der Hilfe von Partnern voranbringen zu können, die spezielle Services hierfür anbieten.

64 %

der Befragten erwartet, in den kommenden zwei Jahren einheitliche Integrationen zur Förderung von IT- und Business-Innovation anhand von APIs zu implementieren.





Security-Konvergenz

„Flexibilität und Agilität sind zu einem gewissen Grad wichtig für uns. An erster Stelle steht jedoch die Sicherheit unseres Netzwerks. Dabei gilt es zu verstehen, wie wir die zugrunde liegende Architektur wirklich sicher gestalten, ausrollen und managen können.“

IT Director
eines multinationalen
Finanzinstituts aus Europa

Infolge hochgradig verteilter Belegschaften und Apps wird die Angriffsfläche und damit auch das Risiko für die Cybersicherheit immer größer. So rangiert das Thema auch weiterhin ganz oben auf der Prioritätenliste von Unternehmen: 40 % der Befragten nennen Cybersicherheit als wichtigsten Einflussfaktor für ihre Netzwerkstrategie. Neben Cloud-basiertem Security-Management gilt dabei die Konvergenz von Security und Netzwerken als Priorität, wenn es darum geht, mit der Wachstumsdynamik der Bedrohungslandschaft Schritt zu halten.

40 %

der IT-Verantwortlichen und ExpertInnen nennen Cybersicherheit als wichtigsten Einflussfaktor für ihre Netzwerkstrategie.



Trend

Konvergenz von Netzwerk und Security als Mittel gegen Konsistenzprobleme

Unternehmen betrachten die Integration von Netzwerk- und Security-Domänen und -Teams als Ziel von höchster Priorität für IT und Business gleichermaßen. Ihnen ist klar, dass es heute keine Option mehr ist, Tools, Daten, Plattformen und Prozesse rund um Netzwerke und Sicherheit voneinander zu trennen. Denn durch eine Brücke zwischen beiden Domänen, die durch die KI-gestützte Analyse kombinierter Netzwerk- und Security-Daten Einblicke liefert, werden verlässlichere, optimierte Verbindungen und stärkere Sicherheit über alle Umgebungen hinweg möglich – von Campus und Zweigstelle bis hin zum Rechenzentrum und zur Operational Technology (OT) bzw. Betriebstechnik.

Heute

42 % der in diesem Jahr Befragten nannten die Integration von Netzwerk und Security als den Bereich, bei dem mit Blick auf die Umsetzung von IT- und Business-Zielen der größte Verbesserungsbedarf besteht.

Eine schnellere Erkennung von und Reaktion auf Bedrohungen für die Cybersicherheit ist laut 44 % der Befragten der wichtigste Vorteil, den die Konvergenz von Netzwerk- und Security-Technologien, -Prozessen und -Tools in Aussicht stellt. Auf Platz 2 der wichtigsten Vorteile rangiert mit 29 % der Austausch von Daten und Telemetrie, gefolgt von standortunabhängig konsistentem und sicherem Zugriff auf Multicloud-Apps laut 27 % der Befragten.

„Konvergenz ist weit mehr als nur eine technische Anpassung. Vielmehr ist sie eine strategische Priorität, für die es der Umsetzung eines IT-Frameworks bedarf, das aus Daten, Prozessen und menschlicher Expertise eine starke Einheit formt, um Bedrohungen abzuwehren und konsistente Erlebnisse zu gestalten.“

Omri Guelfand, Vice President, Product Management, SASE, Cisco



Ausblick auf die nächsten zwei Jahre

Um die Konvergenz ihrer Netzwerke und Sicherheit voranzutreiben, planen Unternehmen diverse Investitionen auf Architektur- und Technologieebene. Ihre Top-Prioritäten bei Security-Fragen für die kommenden zwei Jahre machen dies deutlich: 52 % nannten hierauf die Integration von Netzwerksicherheit in breiter gefasste Funktionsbereiche der IT-Sicherheit. Ein wichtiges Beispiel hierfür ist das Vorhaben von 76 % dieser Unternehmen, im gleichen Zeitraum eine SASE-Architektur (Secure Access Service Edge) zu implementieren, die SD-WAN und Cloud-Security auf Basis eines Security Service Edge integriert.

76%

planen in den kommenden zwei Jahren die Implementierung einer SASE-Architektur, die SD-WAN und Cloud-Security auf Basis eines Security Service Edge integriert.



Entdecken Sie [Secure Networking](#) zur Absicherung von Usern, Apps und Daten.



Fokusbereiche für Investitionen in Netzwerksicherheit in den kommenden Jahren

52 % Integration von Netzwerksicherheit
in breiter gefasste IT-Sicherheit

49 % Umstellung von mehr Security-Tools
auf Cloud-basierte Varianten

33 % Management-Optimierung durch
Anbieterkonsolidierung

26 % Implementierung eines
Zero-Trust-Netzwerks

23 % Umsetzung einer umfassenden SASE-Architektur durch
Integration von SD-WAN und Cloud-basierter Security



Ausblick auf die nächsten zwei Jahre

60 % der Unternehmen rechnen damit, in den kommenden zwei Jahre eine auf gemeinsame APIs gestützte, integrierte Plattform für Netzwerk- und -Sicherheitsmanagement in Multiclouds für sichere Workload-Mobilität, Netzwerk- und Anwendungstransparenz sowie Richtlinienmanagement einzusetzen.

In Sachen IT-Innovation führende Unternehmen wollen zudem Automatisierung im AIOps-Stil umsetzen, um Workload-Mobilität durch End-to-End-Transparenz über Multicloud-, Private-Cloud- und Edge-Netzwerke hinweg zu optimieren.

60%

der Unternehmen gehen davon aus, das Management von Multicloud-Netzwerk und -Sicherheit innerhalb der nächsten zwei Jahre auf eine integrierte Plattform zu stützen.

Trend

Sicherheit von Multicloud-Netzwerken

Aufgrund der starken Tendenz unter Unternehmen, ihre Workloads auf Public und Private Clouds zu verteilen, prägt die Multicloud das Bild ihrer Umgebungen. So geht aus dem [Global Networking Trends Report 2023](#) hervor, dass 92 % aller Unternehmen die Services von mindestens zwei Public-Cloud-Providern nutzen, 34 % auch die von mehr als vier. Je nach Provider gestaltet sich jedoch das Betriebsmodell für Netzwerk und Security unterschiedlich. Gleiches gilt für private Rechenzentren und Hybrid-Cloud-Umgebungen. Daraus resultieren komplexe Management-Prozesse, für die es einer Strategie bedarf, die in puncto Konnektivität und Sicherheit über verschiedene Private- und Public-Cloud-Umgebungen für mehr Transparenz und konsistente Kontrollen sorgt.

Heute

Bei 20 % der Befragten erfolgt die Daten- und Workload-Integration zwischen Rechenzentrums-, Edge- und Public-Cloud-Netzwerken anhand separater Tools für das Cloud-Netzwerkmanagement, die je nach Provider spezifisch sind. 17 % setzen dagegen auf die Verbindung via SD-WAN On-Ramp, um Konnektivität und Management über verschiedene Clouds hinweg konsistenter zu gestalten. Ferner haben 28 % eine grundlegende Multicloud-Netzwerkplattform im Einsatz, anhand derer sie die übergreifende Vernetzung zweier oder mehrerer Cloud-Umgebungen managen.

„Multicloud ist eine Realität, mit der wir zurechtkommen müssen. Hätte ich eine Wahl, würde ich mich allerdings dagegen entscheiden. Denn das Management von Multicloud-Umgebungen gestaltet sich enorm komplex – von der Konfiguration und Wartung bis hin zur Cybersicherheit.“

IT Director eines globalen Akteurs aus der Automobilindustrie

Trend

Cloud-basierte Sicherheit als wichtigster Bereich für Netzwerkinvestitionen

38 % der Befragten nennen Cloud-basierte Sicherheit als den Bereich, in den sie in diesem Jahr am umfangreichsten investieren. Eines der zentralen Elemente künftiger IT-Strategien ist die sichere Vernetzung verteilter Belegschaften und ihrer Geräte. In einem Umfeld, das von Multiclouds und standortunabhängiger Arbeit geprägt ist, braucht es einen engeren Austausch zwischen Netzwerk und Sicherheit. Umsetzbar ist dies mit einer Cloud-nativen Security-Lösung wie SSE, die Zugriffskontrolle und den Schutz vor Bedrohungen, Datensicherheit, Security-Monitoring und Kontrollmechanismen zur akzeptablen Nutzung zentralisiert.

Heute

Angesichts der zunehmenden Verteilung moderner Belegschaften überrascht es wenig, dass 39 % der Befragten die größte Herausforderung in ihrem Netzwerk darin verorten, verlässliche Sicherheit für Remote- und Hybrid-Teams zu gewährleisten. Ihre Entscheidung für Cloud-basierte Sicherheit begründen 40 % insbesondere mit ihrem Einsatz von Cloud-Apps sowie damit, von kontinuierlichen Updates für gehostete Security-Engines zur Schwachstellenerkennung sowie von Engines für umfangreiche Datenanalysen profitieren zu können. Neben IP-VPN, das mit 53 % auf Platz 1 der Liste der populärsten Cloud-basierten Security-Features rangiert, stehen sichere Web-Gateways (47 %) und Cloud Access Security Broker (40 %) bei den Befragten hoch im Kurs.



Ausblick auf die nächsten zwei Jahre

In den kommenden zwei Jahren wollen 49 % der Befragten in erheblichem Maße in Cloud-basierte Security-Tools investieren. Dabei rechnen 39 % damit, dass noch in dieser Zeitspanne bereits mehr als die Hälfte ihrer Security-Tools Cloud-basiert sein werden. Mit Blick auf Prognosen, denen zufolge der Markt für Cloud-Security-Lösungen weltweit von 33 Milliarden US-Dollar im Jahr 2022 bis 2029 um das Dreifache anwachsen und damit ein Volumen von 106 Milliarden US-Dollar erreichen wird, dürfte sich dieser Trend zudem noch weiter fortsetzen.² Ein weiterer Fokusbereich für IT-Investitionen liegt in richtlinienbasierter Mikrosegmentierung: 29 % der Befragten wollen hier investieren, um eine Zero-Trust-Netzwerkinfrastruktur für IoT-Geräte umzusetzen.

49 %

der Befragten wollen in den kommenden zwei Jahre in erheblichem Maße in Cloud-basierte Security-Tools investieren.



Top-Bereiche für Netzwerkinvestitionen in den nächsten 12 Monaten

38 % Cloud-basierte Security-Durchsetzung

34 % KI-gestützte Netzwerktechnologie für prädiktive Assurance

33 % Upgrades des Rechenzentrumsnetzwerks zur besseren Unterstützung neuartiger App- und Workload-Typen (z. B. generative KI)

31 % Einstellung von neuem oder Weiterbildung von bestehendem Netzwerkpersonal

30 % Netzwerkautomatisierung

29 % Initiativen rund um Nachhaltigkeitsziele





KI- Abläufe

„Die Stärke von KI bei der Bild- und Textgenerierung liegt auf der Hand. Ich sehe sie aber insbesondere darin, Korrelationsanalysen zu beschleunigen. KI wird in der Lage sein, Engstellen extrem schnell zu erkennen und uns darüber sowie über die potenzielle Ursache wie etwa einen Konfigurationsfehler zu benachrichtigen – und sie dann auch direkt automatisch zu beheben.“

Group CIO
einer Private-Equity
Gesellschaft
mit Sitz in Europa

Aus den Daten der diesjährigen Umfrage lässt sich schließen, dass IT-Verantwortliche und -ExpertInnen eindeutig vom enormen Potenzial überzeugt sind, das der Einsatz von KI in Bereichen wie der Automatisierung von Betriebsabläufen, der Durchsetzung von Richtlinien, der Stärkung der Sicherheit oder auch der Gewährleistung digitaler Resilienz bietet.

Trend

KI-Einsatz für mehr betriebliche Effizienz

KI-gestützte Betriebsabläufe stellen gewaltige Effizienzgewinne in Aussicht. Ihre weitläufige Implementierung wird vertrauenswürdige Systeme möglich machen, die sich laufend verbessern und so dazu beitragen, dass manuelle Arbeitsschritte in erheblichem Maße reduziert werden.

Heute

Noch nicht einmal 5 % der Befragten attestieren ihren IT-Teams die Fähigkeit zur Umsetzung der Innovationen, die nötig sind, um geschäftliche Strategien zu steuern, die Kundenzufriedenheit zu fördern und Abläufe zu optimieren. Bezeichnend sind auch ihre Aussagen dazu, wie sich ihr Tagesgeschäft rund um Netzwerkdesign, -bereitstellung und -management gestaltet: 37 % beklagen Schwierigkeiten, mit ihren vorhandenen Personalressourcen Konsistenz in Design und Bereitstellung zu gewährleisten. Für mehr als ein Drittel stellt fehlende Automatisierung betrieblicher Aufgaben ein erhebliches Problem dar. Priorität hat es daher, die IT vom administrativen Aufwand zu entlasten, der mit der zunehmenden Komplexität von immer weiter verteilten Netzwerken und Intelligence aus unterschiedlichen Domänen und Produkten einhergeht.

So haben die IT-Teams einer Mehrheit der Befragten (67 %) bereits Initiativen für den Einsatz von KI auf den Weg gebracht, um Abläufe zu vereinfachen, komplexe Aufgaben zu automatisieren und Performance-Probleme schneller zu beheben. Eine passende Lösung für die Umsetzung eines KI-gestützten Netzwerkbetriebs sehen 32 % in einer Netzwerkplattform. Grund hierfür ist ihre Eignung zur Aggregation von Netzwerk-Telemetriedaten für Analytik- und spezialisierte KI-Anwendungen.

„Künftig werden wir noch umfangreicher automatisieren. Mit Fokus auf die Effizienz unserer Abläufe gilt es dabei stets, mit IT-Investitionen aktiv zu umsatzgenerierenden Projekten beizutragen.“

Nicolas Gachet, Global Head of Network Special Projects, The Adecco Group



Ausblick auf die nächsten zwei Jahre

Für die kommenden zwei Jahre rechnen 60 % der Befragten damit, in sämtlichen Domänen KI für prädiktive Automatisierung einzusetzen, um Betriebsabläufe im Netzwerk zu managen und zu vereinfachen. Zudem werden 17 % im gleichen Zeitraum voraussichtlich einen KI-gestützten Netzwerkbetrieb mit AIOps integrieren und so die prädiktive Optimierung zwischen Usern, Geräten und Apps über alle Netzwerkdomänen hinweg ermöglichen.

60 %

der Befragten rechnen damit, im Verlauf der kommenden zwei Jahre in sämtlichen Domänen KI für prädiktive Automatisierung zu implementieren, um Betriebsabläufe im Netzwerk zu managen und zu vereinfachen.

Entdecken Sie Automatisierung und Assurance für Ihre Services mit [NetOps gestützt auf KI](#).

Für die kommenden zwei Jahre erwartete Umsetzung KI-gestützter Innovationen zur Optimierung von Netzwerkbetrieb, Sicherheit, digitaler Resilienz und Nachhaltigkeit:

KI-Einsatz für prädiktive Netzwerkautomatisierung über alle Domänen hinweg, um NetOps zu vereinfachen

60 %

KI-gesteuerte SASE-Architektur (Secure Access Service Edge) für die Cloud

54 %

Endpoint-Erkennung und Richtlinienmanagement gestützt auf KI

51 %

KI-Einsatz zur prädiktiven Digital Experience Assurance

38 %

KI-gestützte Netzwerklösungen zur Förderung der Nachhaltigkeit

25 %





Ausblick auf die nächsten zwei Jahre

Zwei Drittel bzw. 66 % der Befragten gehen davon aus, im Verlauf der kommenden zwei Jahren Governance-Richtlinien und -Verfahren zu implementieren, die den Zugriff auf Daten sowie deren Nutzung in spezifischen Anwendungsfällen unterstützen. Dabei erwartet ein Drittel, dass diese Anwendungsfälle ihren Unternehmen Wettbewerbsvorteile verschaffen werden. Bei 38 % der Befragten gehören hierzu proaktive und prädiktive Betriebsabläufe mit KI-gestützter Assurance für das Netzwerk und Digital Experiences. Nach Einschätzung der Befragten werden ihnen entsprechende Investitionen zu den nötigen Ergebnissen in Sachen Performance und UX verhelfen, um ihr digitales Geschäft voranzutreiben.

66 %

der Befragten gehen davon aus, im Verlauf der kommenden zwei Jahre Governance-Richtlinien und -Verfahren zur Nutzung spezifischer Anwendungsfälle umzusetzen. Mehr als die Hälfte von ihnen erwartet sich davon einen Wettbewerbsvorteil.

Trend

Daten-Governance und KI-gestützte Analytik für prädiktive Assurance

IT-Verantwortliche und -ExpertInnen wissen um die entscheidende Bedeutung von Einblicken in Performance-Daten aus diversen Netzwerkdomänen, wenn es um die Gewährleistung konsistenter Digital Experiences von hoher Qualität geht. So suchen sie nach Wegen zum Zugriff sowohl auf aggregierte, proprietäre Telemetriedaten als auch auf Performance-Telemetrie aus unternehmenseigenen und externen Domänen. Durch Aggregation dieser Datenbestände wird es möglich, KI darauf anzuwenden. Mit ihrer Hilfe können Fachbereiche aus IT und Business den Traffic analysieren und Erkenntnisse zur Performance gewinnen, die sie bei der Entscheidungsfindung zugunsten optimierter Abläufe und dem Erzielen von Wettbewerbsvorteilen unterstützen.

Heute

Weniger als 7 % der Befragten schätzen ihre aktuellen Verfahren zur Daten-Governance als geeignet dafür ein, ihnen Wettbewerbsvorteile zu verschaffen. Als Priorität nennen zwei Drittel der UmfrageteilnehmerInnen die Aggregation datengestützter Analytik über eine Netzwerkplattform. Weitere 41 % sind der Ansicht, dass sich mit einer solchen Plattform die App-Performance verbessern lässt.

Erkannt wird dabei aber auch, dass die Erfassung von Performance-Daten nur der erste Schritt ist. Dies zeigt sich daran, dass KI-gestützte Netzwerktechnologie für prädiktive Assurance bei über einem Drittel der Befragten (34 %) als zweitwichtigster Bereich gilt, in dem sie in den kommenden 12 Monaten in ihr Netzwerk investieren möchten. Indem KI-Modelle anhand von Netzwerkdaten auf die prädiktive und proaktive Behebung von Problemen trainiert werden, können Netzwerkperformance und hochperformante Digital Experiences verlässlicher gewährleistet werden. AIOps-gestützte Service Assurance, anhand derer diese Faktoren zwischen Usern, Geräten, Apps und Services gemanagt werden, haben derzeit jedoch weniger als 4 % der Befragten implementiert. Demnach erfolgt die Gewährleistung der Netzwerkperformance aktuell also weitgehend reaktiv und nicht nach proaktiver und vorausschauender Methodik.

„Jedes Unternehmen benötigt ein Netzwerk, um BenutzerInnen zu verbinden. Um sicherzustellen, dass unser Unternehmen richtig funktioniert, ist eine äußerst konsistente Netzwerkerfahrung erforderlich. Ohne ein zuverlässiges Netzwerk würde ein Unternehmen weder existieren noch seine BenutzerInnen verbinden können.“

Michael Kutka, Network Architect, Insight Global

Trend

KI-gestützte Sicherheit zur Risikominimierung

Auch weiterhin verorten Unternehmen die größten Sorgen um ihr Netzwerk in den Risiken für die Cybersicherheit. Um diese vor dem Hintergrund ebenso komplexer wie allgegenwärtiger Verbindungen, weit verteilten Usern und chronischem Ressourcenmangel bestmöglich zu minimieren, richten sie ihren Blick auf datengestützte Konzepte und den Einsatz von KI. Neben der Stärkung ihres Sicherheitsstatus sollen dadurch auch Kompetenzlücken im Cybersecurity-Kontext ausgeglichen werden.

Heute

Sicherheit bereitet den Befragten nicht nur die größten Sorgen, sondern wird von 30 % auch als wichtigste Erfolgskennzahl für Netzwerkinitiativen und -investitionen zugrunde gelegt. Was den Einsatz von KI zur Gestaltung eines stärkeren und konsistenteren Sicherheitsstatus angeht, so befinden sich die Befragten bis dato allerdings noch im Anfangsstadium.

Etwas mehr als ein Viertel automatisiert derzeit die Erkennung von Endpunkten und das Management von Richtlinien mithilfe von KI. Der Einsatz von KI zur End-to-End-Segmentierung, wodurch ein Zero-Trust-Modell für die Absicherung von User- und Geräteverbindungen umsetzbar wird, ist dagegen aktuell nur bei 4 % festzustellen.

„Aktuelle Sicherheitsmodelle und Telemetriedaten aus Milliarden von Security-Ereignissen bilden die Grundlage für die Entwicklung und das Training von Identity Intelligence. Ihre Anwendung auf Sicherheitskontrollen der nächsten Generation wie Secure Service Edge oder SASE verhilft IT-Teams zu intelligenteren Zero-Trust-Zugriffsentscheidungen und dazu, identitätsbasierte Angriffe effektiver abzuwehren.“

D. J. Sampath, Vice President, Product Management, AI Security, Cisco



Ausblick auf die nächsten zwei Jahre

Im Verlauf der kommenden zwei Jahre ist von einem ausgedehnteren Einsatz von KI zur Cybersecurity-Stärkung auszugehen: 51 % der Befragten planen, sie für Endpoint-Erkennung und Richtlinienmanagement einzusetzen. Dies wird es ihnen erleichtern, Performance- und Sicherheitsprobleme auszumachen und proaktiv anzugehen. Ferner ist bei 54 % der Befragten geplant, in den kommenden zwei Jahren eine KI-gesteuerte SASE-Architektur für die Cloud zu implementieren.

51 %

der IT-Verantwortlichen und -ExpertInnen planen, ihre Cybersicherheit in den kommenden zwei Jahren durch den Einsatz von KI zur Endpoint-Erkennung sowie zum Richtlinienmanagement zu stärken.



Skalierbares Rechenzentrum

Die Anforderungen an die Rechenzentrumsinfrastruktur von KI-Workloads hängen von ihrem Typ ab. Daher müssen Unternehmen ihre Rechenzentren entsprechend dem Typ der KI-Workload modernisieren, den sie priorisieren möchten. Zu unterscheiden sind dabei die folgenden drei Workload-Typen:

1. Umfangreiches Training zum grundlegenden Aufbau des Modells
2. Optimierung des Modells zur Feinjustierung eines bereits trainierten Modells anhand spezifischer Datensätze
3. Anwendung des Modells zur Inferenz von Erkenntnissen aus neuen Daten

Wie ein Tsunami brechen KI-Workloads auf die Rechenzentren von Unternehmen herein, hinzu kommt der Einsatz eher konventioneller Workloads. So nimmt die Modernisierung von Rechenzentren erneut eine hohe Priorität ein: Gefragt ist eine Infrastruktur, die diese anspruchsvollen neuen Workloads effektiv hosten kann, ebenso wie die Vereinfachung damit verbundener Betriebsabläufe.

Trend

Priorität auf Modernisierung von Rechenzentren zur Skalierung von KI-Workloads

Zur Unterstützung der zunehmend datenintensiven Workloads neuartiger Anwendungen wie KI und ML konzentrieren IT-Verantwortliche und -ExpertInnen ihre Budgets darauf, Modernisierungen im Rechenzentrum durch Ethernet und erweitertes Ethernet voranzutreiben.

Heute

Neben Public und Private Clouds kommt On-Premises-Rechenzentren und Edge-Umgebungen eine zunehmend wichtige Bedeutung bei der IT-Hosting-Planung zu. Deutlich wird dies dadurch, dass die Befragten 25 % ihrer Workloads in Rechenzentren, gehosteten Clouds oder Umgebungen in Co-Location-Rechenzentren ausführen. Weitere 17 % werden in Edge-Umgebungen mit kleineren Formfaktoren gehostet.

Was Prioritäten für Investitionen in den kommenden 12 Monaten angeht, so nennt ein Drittel der Befragten Upgrades seiner Rechenzentrums-Netzwerke. Im Fokus steht dabei die Bewältigung der zunehmenden Anforderungen neuartiger Anwendungen und Workloads wie generative KI. Nach Ansicht von 32 % ist dabei InfiniBand die derzeit am besten geeignete Technologie für höchste Anforderungen an Performance und Throughput, wie sie die Vernetzung datenintensiver Workloads stellt.

„Der Einsatz von KI ist mit Detailfragen verbunden, die sich unablässig weiterentwickeln. Daher hängt zukünftiger Erfolg davon ab, in Sachen Infrastruktur jetzt die richtigen Weichen zu stellen. Ethernet ist dafür ideal – seit jeher bewährt und zugleich zukunftssicher dank neuen standardbasierten Innovationen.“

Kevin Wollenweber, Senior Vice President & General Manager, Engineering, Data Center & Provider Connectivity, Cisco



Ausblick auf die nächsten zwei Jahre

47 % der Befragten gehen davon aus, dass das Workload-Hosting in Rechenzentren, Cloud-Umgebungen oder Co-Location-Rechenzentren in den kommenden 2 Jahren entweder in moderatem oder erheblichem Maße zunehmen wird.

Im Hinblick auf KI-Workloads bedeutet dies eine enorme Herausforderung bei der Skalierung des Netzwerks, da sie effizienter erfolgen muss als dies mit klassischen Netzwerkprotokollen möglich ist, wie sie für HPC-Umgebungen (High-Performance-Computing) zum Einsatz kommen. Umso größer ist daher das Interesse an Ethernet- und erweiterter Ethernet-Konnektivität. Ausdruck findet dies in der Absicht von 89 % der Befragten, innerhalb von zwei Jahren die eine oder andere Form von KI-fähigen Rechenzentrums-Cluster einzusetzen, sowie darin, dass 56 % die Implementierung eines erweiterten Ethernet-Netzwerks der nächsten Generation planen, um KI-Workloads durch standardisierte Technologie zur verlustfreien Paketübertragung zu unterstützen.

56 %

der Befragten planen, zur Erfüllung der zunehmenden Anforderungen von KI-Workloads in den kommenden zwei Jahren erweiterte Ethernet-Netzwerke der nächsten Generation zu implementieren.



Entdecken Sie, wie Sie Ihr [Rechenzentrum für KI-Anwendungen skalieren können](#).



Ausblick auf die nächsten zwei Jahre

61 % der Befragten planen, den Betrieb ihres Rechenzentrumsnetzwerks in den kommenden zwei Jahren durch einen KI-nativen Plattformansatz zu vereinfachen, der ihnen prädiktive Einblicke in ihre Abläufe vermittelt. Diese sollen wiederum dazu beitragen, das Management von Workloads und Services über NetOps, DevOps und CloudOps hinweg effizienter und zugleich sicherer zu gestalten.

61 %

der Befragten wollen den Betrieb ihres Rechenzentrumsnetzwerks in den kommenden zwei Jahren durch einen KI-nativen Plattformansatz vereinfachen, der ihnen prädiktive Einblicke in ihre Abläufe vermittelt.

Trend

KI und Plattformen hoch im Kurs bei Betreibern von Rechenzentren

Angesichts zunehmend komplexer Betriebsprozesse ihrer Rechenzentrumsnetzwerke setzen die verantwortlichen Teams auf den Einsatz von Netzwerkplattformen und KI.

Heute

Gegenwärtig attestieren 38 % der Unternehmen einer Netzwerkplattform klare Vorteile dabei, Management-Prozesse im Rechenzentrumsnetzwerk zu vereinfachen. Bei 32 % schlägt sich dies ganz unmittelbar nieder: Durch den Zugriff auf aggregierte Netzwerk-Telemetriedaten, die sich in Analytik- und KI-native Features einspeisen lassen, erzielen sie bessere Ergebnisse für User und IT gleichermaßen.

Als wichtigsten Vorteil eines Plattformansatzes nennen 43 % der Befragten die schnellere Umsetzung von Innovation in IT und Business. Für 42 % liegt er darin, das Netzwerk-Management durch funktionsübergreifende Integrationen von IT-Workflows über SecOps, CloudOps und ITOps durchgängig zu vereinfachen. Ein ebenfalls bedeutender Vorteil besteht nach Ansicht von 41 % darin, dass ein Plattformansatz zu einer schnelleren Bereitstellung von Anwendungen und Netzwerken beiträgt.

Modernisierung von Rechenzentren im 2-Jahres-Ausblick: Diese Initiativen planen Unternehmen zur Bewältigung zunehmender Anforderungen an Workloads und Betrieb.



47 % der Befragten erwarten eine moderate oder erhebliche Zunahme der Workloads, die in privaten Rechenzentren, Cloud-Umgebungen oder Co-Location-Rechenzentren gehostet werden.

89 %

Bereitstellung von Rechenzentrums-Clustern zur Ausführung von KI-Workloads

61 %

KI-nativer Plattformansatz für prädiktive Einblicke in Betriebsabläufe

56 %

Erweiterte Ethernet-Netzwerk-Fabrics für die Ausführung von KI-Workloads

43 %

Plattformarchitektur über alle Domänen und das Rechenzentrum hinweg

40 %

Einsatz moderner Hardware für mehr Energieeffizienz und bessere Ergebnisse in Sachen Nachhaltigkeit



Nachhaltigkeitsfortschritt

Business-Stakeholder bleiben bei Fragen um die Nachhaltigkeit anspruchsvoll, häufig auch aufgrund von Vorgaben zur ESG-Compliance (Umwelt, Soziales und Unternehmensführung), die es zu erfüllen gilt. Die IT steht dabei an vorderster Front, wenn es darum geht, einen Beitrag zur Reduzierung des Energieverbrauchs und der Minimierung von Emissionen zu leisten. Ausgebremst wird sie dabei durch mangelnde Transparenz und unzureichende Qualität von Daten zur Nachhaltigkeit. So liegt ihr Fokus darauf, sich netzwerkübergreifend Einblicke in hierfür relevante Daten zu verschaffen und Gebäudeumgebungen intelligenter und nachhaltiger zu gestalten.

„Für den CIO ist Nachhaltigkeit in der heutigen Zeit strategisches Mandat. Erstens muss die IT gewährleisten, dass ihre Lösungen aktiv zur Umsetzung der ökologischen Ziele des Unternehmens beitragen. Ebenso wichtig ist aber, dass auch ihre Lösungen selbst auf nachhaltiger Technologie basieren.“

CIO
einer privaten Holding-
Gesellschaft
in Lateinamerika



Trend

Datengesteuerte Förderung von Nachhaltigkeit durch die IT

Unternehmen sehen die IT in einer Schlüsselrolle, wenn es um die Umsetzung ihrer Strategien zur Nachhaltigkeit geht. Die Erfassung der Daten, die nötig sind, um Einblicke in Potenziale zur Reduzierung von Stromverbrauch und CO₂-Emissionen zu erhalten, ist derzeit noch im Gange. Viele Unternehmen rechnen hier jedoch noch innerhalb der nächsten zwei Jahre mit deutlichen Fortschritten.

Heute

IT-Verantwortlichen und -ExpertInnen zufolge haben Netzwerkinvestitionen in den vergangenen 12 Monaten dazu beigetragen, gemäß ihren Nachhaltigkeitszielen Verbesserungen um 19 % zu erzielen. Weiter sehen 42 % der Unternehmen in der Nachhaltigkeit den wichtigsten Bereich, in dem das Netzwerk digitalen Geschäftserfolg vorantreiben kann. Der IT schreiben sie dabei eine zentrale Rolle zu, wenn es um die Ausgestaltung von Nachhaltigkeitsstrategien geht.

„Auf dem Weg in eine zunehmend digitale Zukunft wird die IT eine entscheidende Rolle bei der Umsetzung [von Netto-Null-Emissionen in sämtlichen Campus-Umgebungen bis 2025] spielen.“

Rachel Higham, Global Chief Information Officer, WPP



Ausblick auf die nächsten zwei Jahre

Innerhalb der kommenden zwei Jahre wird die IT nach Einschätzung von 56 % der Befragten unternehmensweit in Nachhaltigkeitsstrategien eingebunden werden. 55 % der IT-Verantwortlichen und -ExpertInnen gehen zudem davon aus, dass Netzwerkprotokoll-gesteuerte Nachhaltigkeitsinitiativen wie selektive Stromversorgung und die Nutzung von Energiesparmodi die Nachhaltigkeitsziele positiv beeinflussen werden. Die AnalystInnen von IDC verweisen zudem auf die zunehmende Bedeutung von Kennzahlen zur Nachhaltigkeit: Bis 2026 rechnen sie damit, dass Kennzahlen zur ESG-Performance zu den wichtigsten Entscheidungsfaktoren bei Investitionen in IT-Ausrüstung gehören werden und darüber hinaus mehr als 50 % der Ausschreibungen eine detaillierte Aufstellung zu CO₂-Emissionen, Rohstoffeinsatz und Arbeitsbedingungen beinhalten werden.³

56 %

der IT-Verantwortlichen und -ExpertInnen gehen davon aus, dass ihre IT im Verlauf der kommenden zwei Jahre unternehmensweit in Nachhaltigkeitsstrategien eingebunden wird.



Ausblick auf die nächsten zwei Jahre

Netzwerkgesteuertes Energiemanagement (z. B. Echtzeit-Telemetrie und Plattform-Dashboards) wird sich nach Einschätzung von 60 % der Befragten in erheblichem Maße positiv auf Nachhaltigkeitsstrategien auswirken. Weitere 25 % rechnen damit, Netzwerk- und KI-Lösungen einzusetzen, die auf die Förderung von Nachhaltigkeit entsprechend den Anforderungen spezifischer Branchen oder Baupläne zugeschnitten sind. Ein Beispiel hierfür wäre ein ausgedehnter Bürokomplex, in dem pro Sekunde Tausende Datenpunkte zur Feinjustierung der Energieeffizienz im Hinblick auf Heizung, Klimaanlage und Beleuchtung generiert werden.

60%

der Befragten erwarten, dass sich Lösungen für netzwerkgesteuertes Energiemanagement (z. B. Echtzeit-Telemetrie und Plattform-Dashboards) in den kommenden zwei Jahren in erheblichem Maße positiv auf Nachhaltigkeitsstrategien auswirken werden.

Trend

Priorität auf Infrastruktur-Telemetrie und -Transparenz

Teams, denen es an Einblicken in relevante Kennzahlen zur Nachhaltigkeit fehlt, sehen eine Lösung in Plattform-Dashboards. Von diesen erwarten sie sich, eine Echtzeit-Ansicht auf sämtliche Telemetrie zur Nachhaltigkeit zu erhalten.

Heute

Auf ihrem Weg, ein nachhaltigeres Unternehmen zu werden, besteht 40 % der Befragten zufolge die größte Hürde in der unzureichenden Transparenz, die ihnen bestehende IT-Produkte zu Nachhaltigkeitsdaten liefern. Insbesondere fehlt es dabei an Einblicken in IT-bezogene Daten zu Energieverbrauch und Emissionen, wie 32 % knapp ein Drittel der Befragten zu Protokoll gibt. 39 % sind sich zudem unsicher darüber, ob die von ihnen erfassten Daten die Qualitätsstandards zur Ermittlung der Nachhaltigkeits-Performance erfüllen, die für eine entsprechende Berichterstattung an externe Stellen erforderlich sind.

„Durch größere Transparenz ihrer Infrastruktur können Unternehmen künftige Updates optimieren, indem sie nur genau so viel Kapazitäten beziehen wie nötig. Dadurch vermeiden sie unnötigen Energieverbrauch.“

Frank Osberg, Network Architect, Solar Denmark



Für die kommenden 2 Jahre geplante Initiativen mit positivem Einfluss auf die Nachhaltigkeitsstrategie:

60 % Durch das IT-Netzwerk gesteuertes Energiemanagement (z. B. Echtzeit-Telemetrie und Plattform-Dashboards)

55 % Durch Netzwerkprotokolle gesteuerte Nachhaltigkeitsinitiativen (z. B. selektive Stromversorgung und Energiesparmodi sowie Bedarfsprognosen)

44 % Transformation von Beschaffungsvorgaben (z. B. hinsichtlich Partner-/Anbieterwahl, Verpackung, Recycling)

40 % Auswahlverfahren für Partner/Anbieter (z. B. nach Reifegrad von Services und Programmen für Nachhaltigkeit)

39 % Hardware-Modernisierung (z. B. Produkt-Modularität und -Effizienz)

Trend

Planung von Gebäudeinfrastruktur für mehr Effizienz und bessere Erlebnisse

Mehr als die Hälfte der Belegschaft arbeitet den Umfrageergebnissen nach derzeit in erster Linie an Unternehmensstandorten – Gebäude, auf die ein erheblicher Anteil der CO₂-Emissionen entfällt. Hier können IT-Teams Modernisierungen durch die Erfassung und Analyse von Gebäudedaten ansetzen, um Ziele zur Nachhaltigkeit ebenso zu erfüllen wie solche zur Mitarbeiterproduktivität.

Heute

Arbeitsmodelle verteilen sich in Unternehmen ausgeglichen auf zwei Lager: 54 % der Befragten gaben an, sich an einem Büro- oder Unternehmensstandort mit dem Netzwerk zu verbinden, bei 46 % erfolgte die Verbindung entweder von zu Hause aus, im Außendienst oder abhängig von hybriden Arbeitsplänen. In diesem Kontext ist zu erwähnen, dass branchenspezifischen Daten zufolge 37 % der weltweiten CO₂-Emissionen auf Gebäude zurückgehen.⁴ Bezeichnend dabei: Laut Daten aus den USA werden Schätzungsweise 30 % der Energie, die ein Gebäude verbraucht, überhaupt nicht genutzt.⁵ So befinden auch 36 % der TeilnehmerInnen unserer Studie, dass Vernetzung, Infrastruktur und Anlagenmanagement allesamt in erheblichem Maße optimiert werden müssen, um nachhaltiger zu werden.

Umso wichtiger also, dass IT-Teams gemeinsam mit ExpertInnen für Prozesse im Anlagenmanagement Modernisierungen von Arbeitsumgebungen anstoßen. Neben der Zufriedenheit und Produktivität von MitarbeiterInnen können sie dabei durch Monitoring, Datenanalysen und effizientere Infrastruktur auch die Energieeffizienz verbessern und dadurch ihren CO₂-Ausstoß verringern.

„Uns war es gerade auch nach der einschneidenden Zeit der Corona-Pandemie ein besonderes Anliegen, eine ansprechende Umgebung zu gestalten, in der alle ihre Kreativität entfalten können. [...] Wir müssen dazu beitragen, dass die Leute wieder gern ins Büro kommen. Vermisst haben sie es allemal.“

Colin Bannon, Chief Technology Officer, BT



Ausblick auf die nächsten zwei Jahre

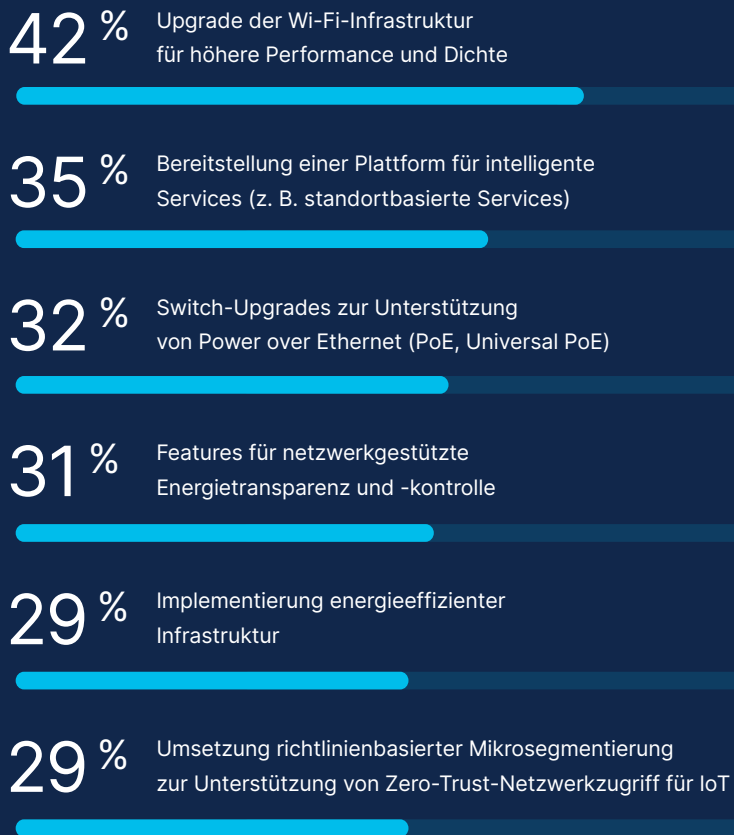
30 % der Befragten gehen davon aus, dass Nachhaltigkeitsthemen in den kommenden zwei Jahren erheblichen Einfluss auf die Netzwerkstrategie ihres Unternehmens nehmen werden. Den wichtigsten Investitionsschwerpunkt im Hinblick auf intelligente Gebäude wird nach Einschätzung von 31 % der Befragten in den kommenden zwei Jahren die Implementierung von Features für netzwerkgestützte Energietransparenz und -kontrolle bilden.

Daneben priorisieren sie für diesen Zeitraum auch Upgrade-Vorhaben der Wi-Fi-Infrastruktur für höhere Performance und Dichte (42 %), die Bereitstellung einer Plattform für intelligente Services (35 %) und Switch-Upgrades zur Unterstützung von Power over Ethernet (PoE) (34 %).

42 %

der Unternehmen werden Investitionen in intelligente Gebäude in den kommenden zwei Jahre insbesondere auf Upgrade-Vorhaben der Wi-Fi-Infrastruktur zur Optimierung von Performance und Dichte konzentrieren.

Wichtigste Investitionsschwerpunkte für intelligente Gebäude in den kommenden zwei Jahren:



Fazit

In einer Zeit des wirtschaftlichen und gesellschaftspolitischen Wandels ist der Weg von Unternehmen klar gesteckt: Es gilt, für betriebliche Effizienz zu sorgen, sichere Vernetzung zu gewährleisten und die Weiterentwicklung digitaler Geschäftsprozesse durch schnelle IT-Innovation voranzutreiben.

Auf diesem Weg stellen IT-Verantwortliche verschiedene Weichen für ihr Netzwerk:

- ✓ Proaktive Gewährleistung verlässlicher, sicherer und vernetzter Umgebungen für mehr digitale Resilienz
- ✓ Gestaltung unkomplizierter, einheitlicher Betriebsabläufe über alle Domänen und Teams hinweg durch KI-native Netzwerkplattformen
- ✓ Gewährleistung der nötigen Skalierbarkeit und Flexibilität zur Erfüllung der Anforderungen heutiger wie zukünftiger Anwendungsfälle, Anwendungen und Workloads
- ✓ Implementierung umfangreicher datengesteuerter Features, um domänenübergreifende Umgebungen zu vereinfachen, Problemstellen proaktiv zu beheben und über User und Geräte hinweg für stärkere Sicherheit zu sorgen
- ✓ Vereinfachung des Zugangs zu einem umfangreichen Ecosystem aus Partnerlösungen anhand offener APIs

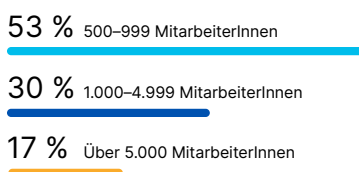
In den kommenden zwei Jahren werden noch deutlich mehr Unternehmen ihre Umgebungen um Netzwerkarchitekturen und -funktionen ergänzen. So werden sie trotz des zunehmenden Mangels an Personalressourcen deutlich mehr erreichen und völlig neue Möglichkeiten dafür erschließen, mit ihrem Netzwerk zu geschäftlichem Erfolg beizutragen.

Methodik

Dem Global Networking Trends Report liegt eine Umfrage sowie Untersuchungen und Analysen zugrunde, mit denen Cisco die AnalystInnen von IDC im November 2023 beauftragt hat. Befragt wurden dabei 2.052 IT-Führungskräfte und -ExpertInnen in Unternehmen aus 13 Ländern, die in 10 unterschiedlichen Branchen tätig sind, um die wichtigsten Herausforderungen im Netzwerkkontext, Zielprioritäten für IT und Business sowie Strategien für zukünftige Investitionen zu ermitteln. Grundlage hierfür bildete ein Dutzend Kriterien mit Relevanz für die Weiterentwicklung von Unternehmensnetzwerken, diesen zugrunde liegende Architekturen, domänenübergreifende Security-Strategien und die zentrale Rolle von KI in sämtlichen Bereichen des Netzwerks.



Unternehmensgröße



Demografie

- 13 Länder
- 10 Branchen
- 2.052 UmfrageteilnehmerInnen
 - 68 % IT-Verantwortliche (Manager, Director)
 - 32 % IT-Führungskräfte (VP, EVP, C-Level)

Ziele

- Beurteilung der wichtigsten Herausforderungen im Netzwerkkontext
- Ermittlung von Zielprioritäten für IT und Business
- Einordnung des Entwicklungsgrads eingesetzter Architekturen
- Bestimmung aktueller Strategien für zukünftige Investitionen



- ¹ IDC Analyst Connection: „How A Network Platform Approach Is Becoming Imperative for IT and Business Agility“ im Auftrag von Cisco, #US51420323, Dezember 2023
- ² „Cloud Security Market Size, Share, Trends“, Fortune Business Insights, 2021
- ³ IDC Blog, IDC FutureScape: WW Sustainability/ESG 2023 Predictions, 5. Dezember 2022
- ⁴ „Building Materials and the Climate: Constructing a New Future“, United Nations Environmental Program, 2023
- ⁵ „How Much Energy is Consumed in U.S. Buildings?“, FAQ, U.S. Energy Information Administration, 2023