The bridge to possible

Global Networking Trends Report **2021**

Sonderausgabe zur Business Resiliency: Erkennen Sie die fünf Trends, die in Zeiten der Disruption Agilität und Widerstandsfähigkeit steigern.

Inhalt

Einführung: Widerstandsfähigkeit

Von Business Continuity zu Business Resiliency

Weder als Einzelpersonen noch als Unternehmen haben wir eine globale, langfristige Disruption wie COVID-19 vorhergesehen – und wir waren darauf nicht vorbereitet. Praktisch über Nacht begannen ganze Belegschaften remote zu arbeiten, während einige Unternehmen ihre Waren und Dienstleistungen online anbieten wollten und andere strategische Lieferketten auf neue Lieferanten und Standorte verlagerten.

Verständlicherweise war die Pandemie ein Weckruf für jedes Land, jede Gemeinde und jedes Unternehmen. Doch was genau hat sich verändert? Schließlich ist es nicht die erste missliche Lage, in der sich Unternehmen befinden: 7 von 10 Unternehmen haben in den letzten 5 Jahren mindestens eine schwere Krise erlebt und 95 % sind überzeugt, dass es nicht ihre letzte sein wird.[1]

Unternehmen haben in den letzten 5 Jahren mindestens eine schwere Krise erlebt.

Quelle: PwC: Global Crisis Survey 2019.

Durch Menschen verursachte Disruptionen – darunter fallen soziale Unruhen, Cyberangriffe, aber auch behördliche Auflagen – haben in den letzten Jahren stetig zugenommen. Ebenso erleben wir die immensen **natürlichen Auswirkungen** wie Hurrikane, Waldbrände oder Überschwemmungen immer stärker und häufiger.

Die erfolgreiche Bewältigung künftiger Disruptionen erfordert von IT-Führungskräften eine neue Denkweise. Eine, die den Schwerpunkt stärker auf die erforderliche IT-Flexibilität legt, um Business Resiliency zu erreichen, und nicht auf den eher präskriptiven und reaktiven Ansatz, der die Grundlage der traditionellen Planungen zur Business Continuity war. Anders als die heutigen Bemühungen um Business Continuity versetzt Business Resiliency Unternehmen in die Lage, sich auch auf Unerwartetes vorzubereiten.

[1] PwC, "PwC's Global Crisis Survey 2019."

Business Continuity im Vergleich zu Business Resiliency

Business Continuity: Die Fähigkeit eines Unternehmens, nach einer Unterbrechung die Lieferung von Produkten oder Dienstleistungen auf einem akzeptablen vordefinierten Niveau fortzusetzen. *

Business Resiliency: Die Fähigkeit eines Unternehmens, in einem sich verändernden Umfeld widerstandsfähig zu sein und sich anzupassen, damit es seine Ziele erreichen, überleben und gedeihen kann. **

* Internationale Organisation für Normung, „Security and Resilience – Vocabulary“, ISO 22300:2018

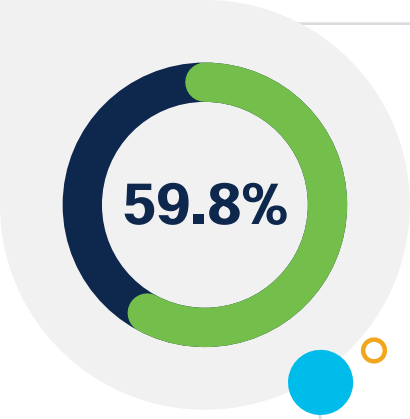
** Internationale Organisation für Normung, „Security and Resilience – Organizational Resilience – Principles and Attributes“, ISO 22316:2017

Abbildung 1: Von Business Continuity zu Business Resiliency

Fünf Netzwerk-Trends

Das Netzwerk: 5 Trends zur Stärkung der Business Resiliency

Zentrale Geschäftsprozesse hängen von einem immer komplexeren Netz digitaler Technologien ab, die die Grundlage für das Erreichen organisatorischer Widerstandsfähigkeit bilden.



Die Mehrheit der Fachleute im Bereich Business Continuity (59,8 %) bewertet die Widerstandsfähigkeit der IT als den wichtigsten Faktor bei der Reaktion auf die aktuelle Pandemie.

Quelle: BCI, „The Future of Business Continuity and Resilience“

Als einzige Plattform, die einen zunehmend dynamischen und verteilten Stamm von Benutzern und Geräten sowie zunehmend disaggregierte und verteilte Anwendungen und Workloads in Verbindung hält, schützt und befähigt, spielt das Netzwerk eine zentrale Rolle bei der Unterstützung von Unternehmen beim Aufbau ihrer Widerstandsfähigkeit.

Mit anderen Worten: Die Widerstandsfähigkeit des Netzwerks, also die Aufrechterhaltung von Netzwerkverbindungen und -verfügbarkeit, reicht nicht mehr aus. Unternehmen benötigen die Art von Widerstandsfähigkeit, die durch eine fortschrittliche Netzwerkplattform ermöglicht wird, die schnell auf alle Umstände reagieren, neue Betriebsmodelle und Services ermöglichen, sich in IT-Prozesse integrieren und ihre Mitarbeiter, Kernaktivitäten, Kunden und die Marke schützen kann. In der Tat handelt es sich dabei um dasselbe moderne Netzwerk, das zur Unterstützung von Digitalisierungsinitiativen erforderlich ist.

Widerstandsfähigkeit des Netzwerks vs. Business Resiliency-Networking

Widerstandsfähigkeit des Netzwerks: Die Fähigkeit, angesichts von Störungen und Herausforderungen des normalen Betriebs eines bestimmten Kommunikationsnetzwerks auf Grundlage vorbereiteter Einrichtungen ein akzeptables Serviceniveau bereitzustellen und aufrechtzuerhalten.*

Business Resiliency-Networking: Ein Netzwerk, das Unternehmen in die Lage versetzen soll, schnell, sicher und effektiv auf erwartete oder unerwartete Störungen zu reagieren.

* Internationale Fernmeldeunion, „Requirements for Network Resilience and Recovery“

Aufbau von Agilität und Widerstandsfähigkeit für Belegschaft, Arbeitsumgebung, Workloads und Betrieb

Wir möchten fünf Trends hervorheben, die Führungskräfte im Netzwerkbereich als Teil ihrer Bemühungen zur Unterstützung der Widerstandsfähigkeitspläne ihres Unternehmens in Betracht ziehen sollten. Sie beziehen sich auf die Verbesserung der Widerstandsfähigkeit von vier Schlüsselbereichen: **Belegschaft, Arbeitsumgebung, Workloads** und **IT-Betrieb**.

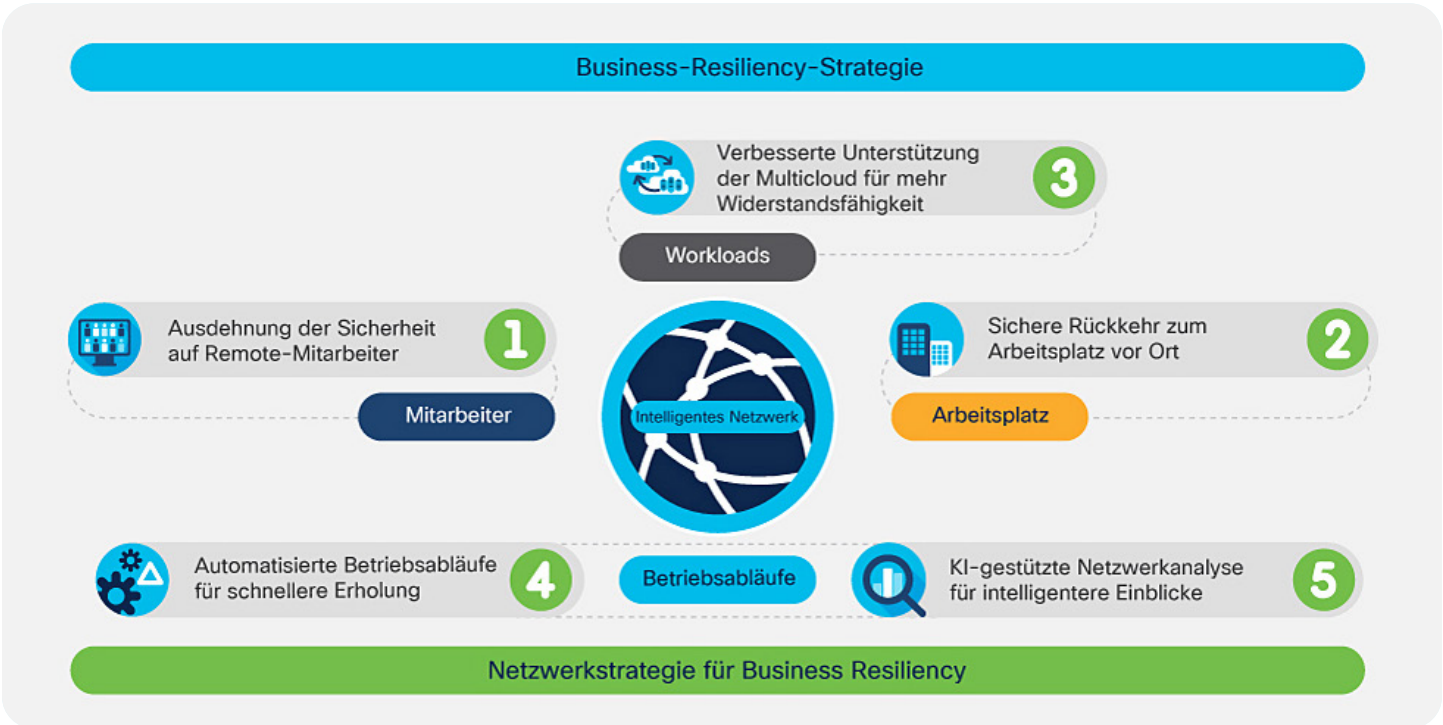


Abbildung 2: Das Netzwerk als Grundlage der Widerstandsfähigkeit von Belegschaft, Arbeitsumgebung, Workloads und Betrieb

Belegschaft: remote und sicher

Trend Nr. 1: Belegschaft – Ausdehnung der Sicherheit auf Remote-Mitarbeiter

Die meisten Unternehmen kommen zu der Erkenntnis, dass neue, flexiblere Arbeitsansätze für ihre Mitarbeiter zu einer dauerhaften Realität werden.

Im Vergleich zur Zeit vor der Pandemie arbeiten heute im Schnitt 4,7 Mal mehr Beschäftigte im Homeoffice. Viele IT-Teams kämpften mit der Skalierung, um die plötzliche Nachfrage zu bewältigen.

Quelle: Freeform Dynamics, „A New Perspective on the Modern Workplace“, von Cisco gesponserter Bericht, Juli 2020

Infolgedessen sieht sich die IT mit einer Reihe neuer Geschäftsanforderungen konfrontiert:

- Befähigung der Arbeitnehmer, von jedem Standort aus produktiv zu sein und zusammenzuarbeiten
- Optimierung von IT-Leistung, Kosten und Sicherheit für jeden Mitarbeiter
- Ausweitung von IT-Betrieb und -Governance der Enterprise-Klasse auf den privaten Bereich

Doch die Erfüllung dieser Anforderungen bietet einige Fallstricke. Insbesondere die Sicherheit der Remote-Mitarbeiter und das Endbenutzerverhalten sind für die Mehrheit der IT-Organisationen nach wie vor ein ständiges Anliegen und eine Herausforderung.

Die 4 größten IT-Herausforderungen für die Befähigung von Remote-Mitarbeitern:

Sicherheit (65 %)

Endbenutzerverhalten (52 %)

Anwendungsleistung (43 %)

IT-Betrieb (35 %)[2]

[2] Cisco Business Resiliency Networking-Umfrage 2020

Wenn private Geräte und Verbindungen für den Zugriff auf Unternehmensanwendungen und -daten verwendet werden, sind Remote-Mitarbeiter besonders anfällig für Cybersicherheitsangriffe. Viele umgehen das VPN und stellen eine direkte Verbindung zu Diensten und Anwendungen in der Public Cloud her, die nach wie vor die am schwierigsten zu verteidigende Umgebung ist.[3]

Überlegungen zum Netzwerk: Wenn es darum geht, sichere Modelle für die Arbeit von zu Hause aus in großem Maßstab zu ermöglichen, sollten IT-Teams einige oder alle der folgenden Ansätze übernehmen:

- **Skalierung von VPNs zum Schutz von Remote-Mitarbeitern:** Enterprise-VPNs bieten weiterhin eine der effektivsten und schnellsten Möglichkeiten, Kontrolle und Schutz auf Unternehmensebene auf Remote-Mitarbeiter auszudehnen.
- **Verwendung der mehrstufigen Authentifizierung (MFA) zum Schutz von Anwendungen:** MFA überprüft die Identität jedes Benutzers, bevor Zugriff auf das Netzwerk oder sensible Anwendungen und Daten gewährt wird, und ist damit für den Schutz des Unternehmens von entscheidender Bedeutung.
- **Einsatz eines Secure Access Services Edge (SASE) zum Schutz des Multicloud-Zugriffs:** Cloud-basierte Sicherheit und SASE helfen bei der Abwehr internetbasierter Bedrohungen, unabhängig von der Verbindung, dem Benutzergerät oder der Cloud-Umgebung.

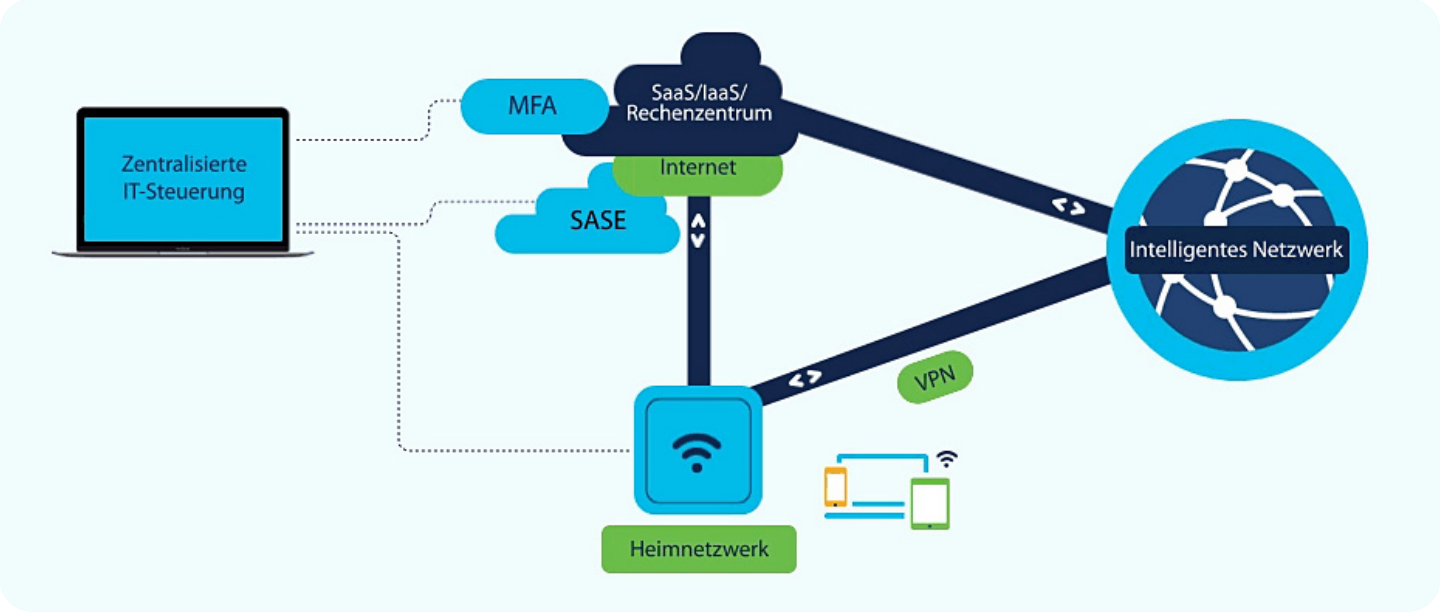


Abbildung 3: Sichere Remote-Mitarbeiter mit VPN, MFA und SASE

Erfahren Sie mehr über Vernetzung und Schutz Ihrer Mitarbeiter an Remote-Standorten

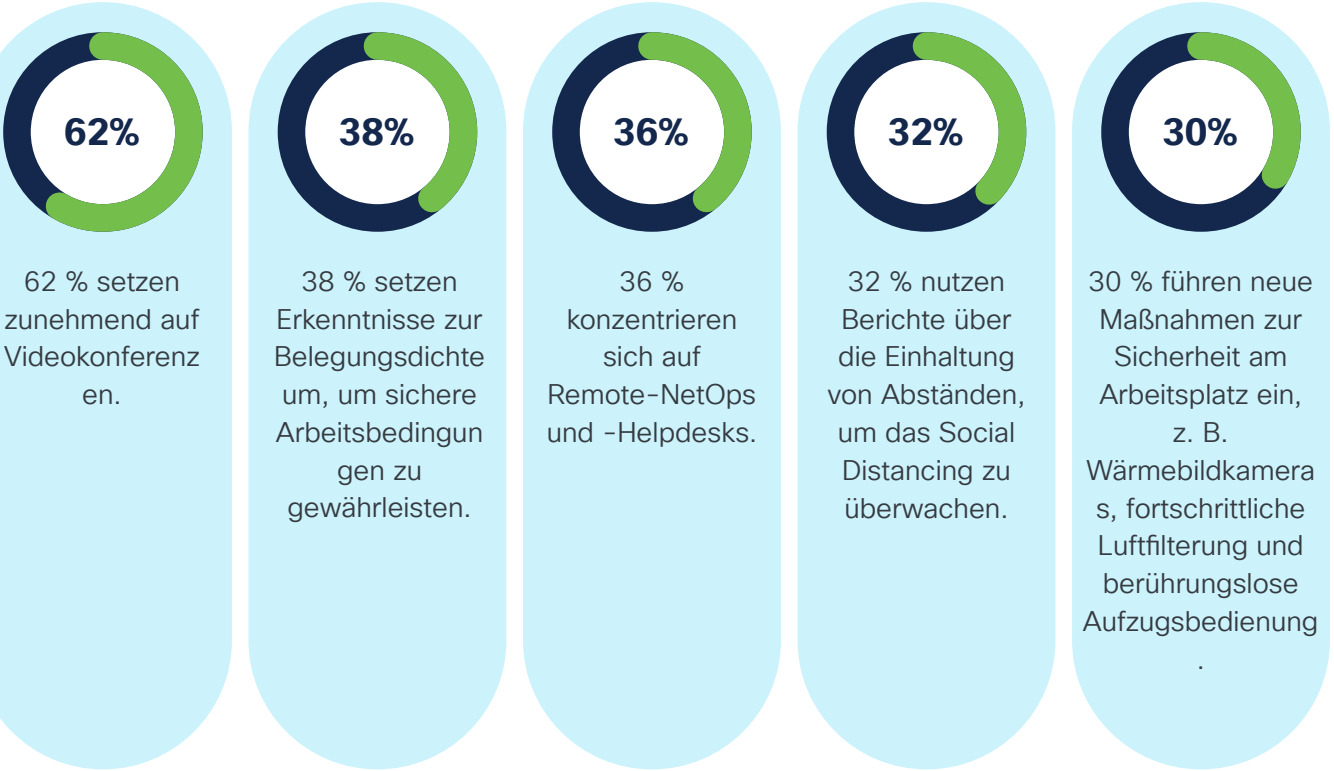
[3] Cisco Umbrella, „2019 Cybersecurity Trends“

Arbeitsumgebung: geschützt und vertrauenswürdig

Trend Nr. 2: Arbeitsplatz - Sichere Rückkehr zu lokalen Arbeitsbereichen

Es ist zwar noch nicht alles klar, aber es zeichnet sich deutlich ab, dass sich Arbeitsplätze und -umgebungen im Zuge der derzeitigen Pandemie weiterentwickeln werden. Unzählige Unternehmen sind dabei, bestehende Services wie Videokonferenzen und standortbasiertes Wi-Fi auszubauen. Andere stellen neue Services und Schutzvorkehrungen bereit, z. B. Überwachung des physischen Abstands und der Belegungsdichte, verstärkte Automatisierung am Arbeitsplatz und sogar Roboter, die die menschliche Produktivität und Kommunikation unterstützen.

Wie bereiten sich Netzwerkteams auf eine sichere Rückkehr an den Arbeitsplatz vor?



Quelle: Cisco Business Resiliency Networking-Umfrage 2020

Überlegungen zum Netzwerk: Ein modernes, agiles Netzwerk ist ein entscheidender Faktor, der die sichere und nahtlose Rückkehr an den Arbeitsplatz erleichtert.

- **Führen Sie einen Stresstest Ihres Netzwerks durch:** In vielen Fällen ist das Netzwerk seit mehreren Wochen außer Betrieb. Gehen Sie nicht selbstverständlich davon aus, dass es noch immer die notwendigen verkabelten und Wireless-Services bereitstellen kann.
- **Automatisieren Sie den identitätsbasierten sicheren Zugriff:** Unternehmen müssen in der Lage sein, das Onboarding und den Zugriff auf Services für Benutzer und Geräte einheitlich zu verwalten, zu sichern und zu segmentieren, unabhängig davon, ob diese sich von lokalen, privaten oder öffentlichen Netzwerken aus verbinden.
- **Erhöhen Sie die Sicherheit von Mitarbeitern und Kunden durch standortbasierte Analysen:** Ermöglichen Sie Arbeitsplatzüberwachung, Warnungen und Einblicke, um die Gesundheit und Sicherheit von Mitarbeitern, Partnern, Gästen und Kunden durch die Nutzung bestehender Wi-Fi-Netzwerke zu schützen.

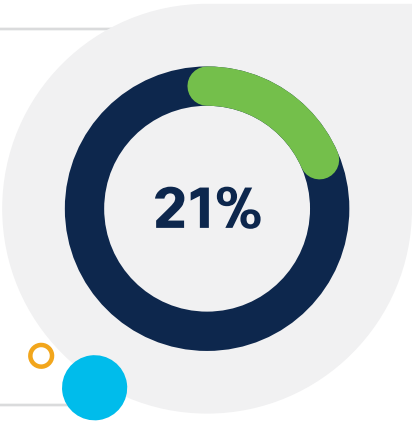
Erfahren Sie mehr über die Schaffung einer sicheren Arbeitsumgebung

Workload – Multicloud

Trend Nr. 3: Workload – Verbesserte Unterstützung der Multicloud für mehr Widerstandsfähigkeit

IT-Führungskräfte nutzen Cloud-Services zur Verbesserung der Business Resiliency angesichts der Pandemie. Dazu gehört auch die verstärkte Anwendung eines Multicloud-Modells – die Verteilung von Anwendungen, Workloads und Daten auf Vor-Ort-Rechenzentren und Public-Cloud-Anbieter –, um Kosten zu senken, die Flexibilität zu erhöhen und das Risiko katastrophaler Ausfälle zu verhindern und zu verteilen.

> „21 % der Unternehmen verlagern zusätzliche Workloads in die Public Cloud, um angesichts der Pandemie Kapitalausgaben einzusparen.“
>
> IDC, „COVID-19 Impact Survey, Wave 5“, 2020



Netzwerküberlegungen: Um eine konsistente Erfahrung für Benutzer und DevOps-Teams zu gewährleisten, benötigen Unternehmen eine proaktive Multicloud-Netzwerkstrategie, die das Netzwerk mit der Cloud, den Sicherheitsanforderungen und den Prioritäten des IT-Betriebs in Einklang bringt.

Erfolgreiche Multicloud Networking-Strategien basieren auf drei Hauptpfeilern:

- **Workload:** Einführung eines Cloud-Betriebsmodells zur Vereinfachung von Richtlinien, Sicherheit sowie der Verwaltung von Workloads und Services in Rechenzentren vor Ort, mehreren verschiedenen Clouds und anderen Computing-Umgebungen.
- **Zugriff:** Umsetzung von SD-WAN- und SASE-Ansätzen zur Gewährleistung eines dauerhaft sicheren Multicloud-Zugriffs (einschließlich SaaS) für Benutzer und Geräte in Unternehmens- und öffentlichen Netzwerken vom Campus, von Zweigstellen, von zu Hause oder von unterwegs.
- **Sicherheit:** Verringerung des Risikos, das mit Benutzern, Geräten und Anwendungen verbunden ist, die über mehrere Clouds und andere Computerumgebungen verteilt sind.

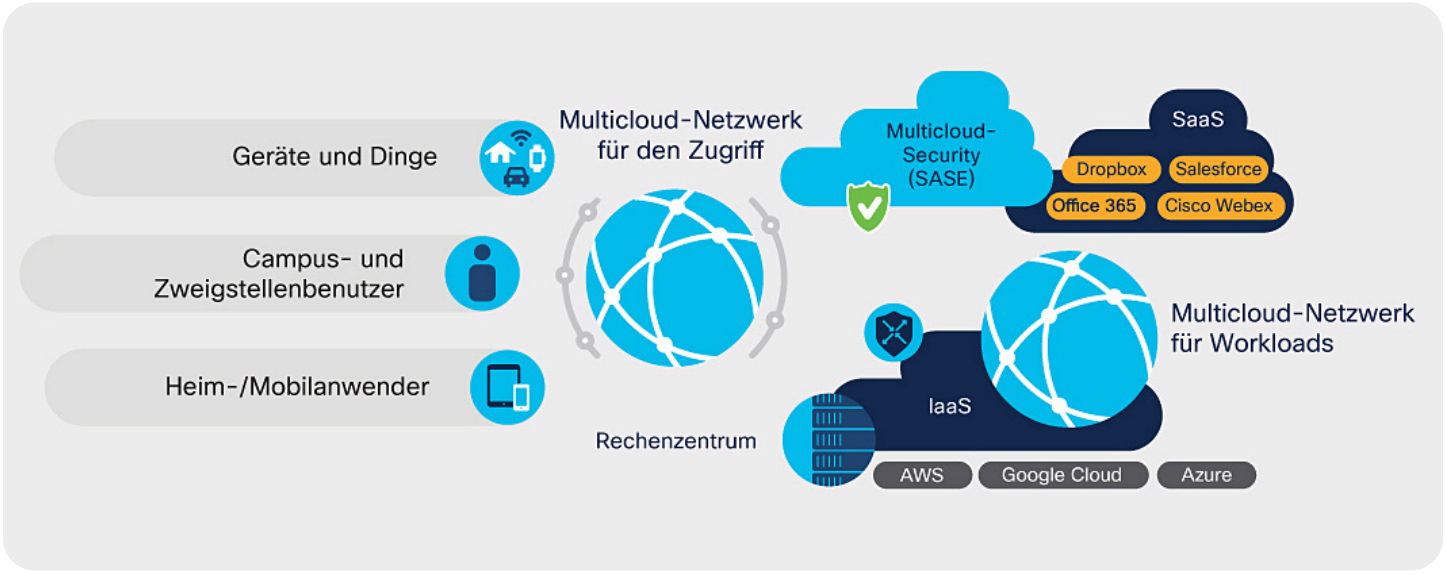


Abbildung 4: Multicloud-Netzwerk: Workload, Zugriff und Sicherheit

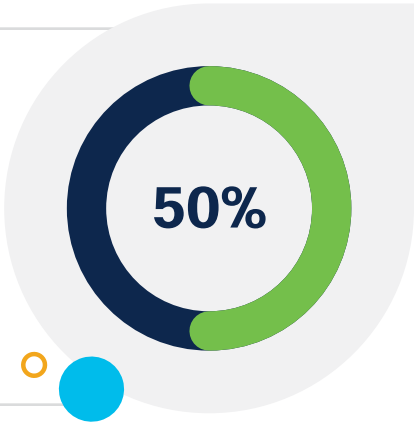
Erfahren Sie mehr über die Entwicklung einer sicheren und effektiven Multicloud-Netzwerkstrategie

Betrieb – automatisiert

Trend Nr. 4: Betrieb – Automatisierung des Betriebs zur schnelleren Erholung

Die explodierende Zahl der verstreut tätigen Remote-Mitarbeiter ist nicht das Einzige, was NetOps-Teams von heute außerordentlich belastet. Die Pandemie hat auch zu nie dagewesenen starken Schwankungen bei der Kundenanzahl, unbekannten Mustern im Anwendungsdatenverkehr und neuen Anwendungsfällen wie E-Learning, Videokonferenzen, virtuellen Veranstaltungen, Remote-Pflege, Prozessautomatisierung und anderen netzwerkabhängigen Services geführt.

> „50% priorisieren beim Umgang mit Disruptionen heutzutage die Netzwerkautomatisierung.“
>
> Cisco Business Resiliency Networking-Umfrage 2020



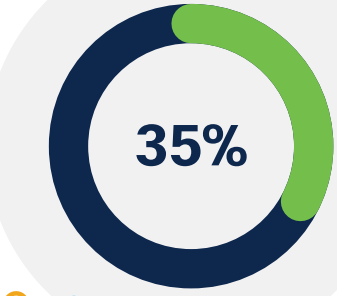
So ist es keine Überraschung, dass heute die Hälfte aller Netzwerkfachleute die Netzwerkautomatisierung als eine entscheidende Voraussetzung für die Sicherstellung der Kontinuität von Services und Leistung während einer Disruption bezeichnen.

Quelle: Cisco Global Networking Trends Report 2020

Überlegungen zum Netzwerk: NetOps-Teams können durch ein schrittweises Vorgehen eine kontinuierliche Verbesserung erreichen und schnell auf zunehmende Disruptionen und Bedrohungen reagieren:

- **Automatisieren Sie sich wiederholende administrative Aufgaben** wie Netzwerkbereitstellung, Konfiguration und Image-Verwaltung, um den Verwaltungsaufwand zu verringern und die Compliance in jedem Bereich zu verbessern.
- **Automatisieren Sie den Netzwerkzugriff, das Onboarding und die Segmentierung,** um Gruppen von verteilten Benutzern und Dingen zu schützen und die Ausbreitung von Cybersicherheitsangriffen einzudämmen.
- **Automatisieren Sie Netzwerkrichtlinien innerhalb des Unternehmensrechenzentrums** mit anwendungszentrierter Segmentierung, die Anwendungen und Daten schützt und den Workloads folgt.
- **Automatisieren Sie Richtlinien über das Rechenzentrum hinaus in die Cloud** mit einem Cloud-Betriebsmodell, das konsistente Anwendungsrichtlinien über Vor-Ort- und Hybrid-Cloud-Umgebungen hinweg liefert.
- **Automatisieren Sie die richtlinienbasierte End-to-End-Multidomain-Segmentierung,** um ein konsistentes, durchgehendes Zero-Trust-Zugriffsmodell von Benutzern und Dingen bis hin zu Workloads zu erstellen.

> „35 % planen, dass ihre Netzwerke bis 2022 in allen Bereichen Intent-Based sein sollen – gegenüber nur 4 % im Jahr 2019.“
>
> Cisco, Global Networking Trends Report 2020



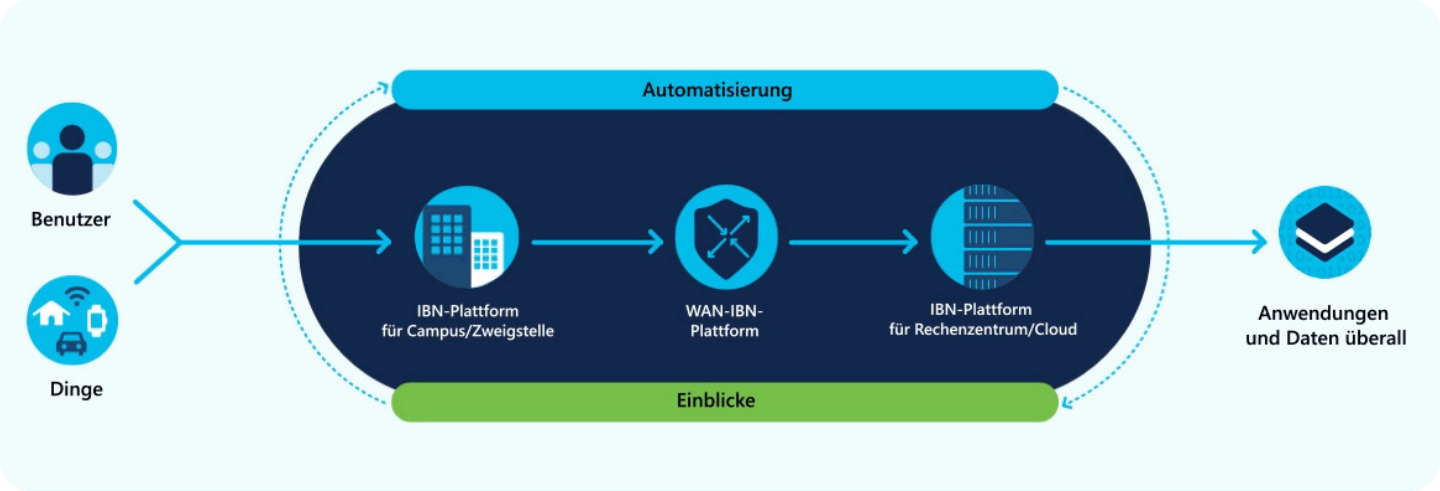


Abbildung 5: Automatisierung und Einblicke vom Benutzer bis zur Workload überall

Erfahren Sie, wie Sie Richtlinien über mehrere Netzwerkdomänen hinweg automatisieren können

Betrieb – KI-gestützt

Trend Nr. 5: Betrieb – Nutzung KI-gestützter Netzwerkanalysen für intelligentere Einblicke

Die Komplexität und der Umfang moderner Netzwerke sowie die daraus resultierende Flut von Ereignissen und Problemen, die auf mehrere unterschiedliche Überwachungsplattformen ein strömt, können überwältigend und ineffektiv sein, insbesondere wenn eine Disruption auftritt.

> „4.400: Durchschnittliche Anzahl der monatlichen Ereignisse im Zusammenhang mit Wireless in einem Unternehmensnetzwerk. *“
>
> Quelle: Cisco Telemetry: Cisco DNA Center, 2020

* Basierend auf über 600 Unternehmensnetzwerken. Zu den Ereignissen gehören Onboarding-Fehler/-Zeiten, Funkmoduldurchsatz und DHCP-Antwortzeit/-Fehler. Diese Ereigniszahlen wurden bereits durch KI-gestütztes dynamisches Baselining reduziert.

Es liegt auf der Hand, dass NetOps-Teams Unterstützung durch fortschrittliche Analysefunktionen benötigen, um schnell fundierte Entscheidungen zur Problembehebung treffen zu können.

Durch den Einsatz KI-gestützter Netzwerkanalyse- und ML-Verfahren (Machine Learning) können NetOps-Teams Probleme viel besser bearbeiten und lösen.

> „Cisco AI Network Analytics, eine Anwendung in Cisco DNA Center, löst monatlich weltweit 2,6 Millionen „Ereignisse“ in 15.080 lösbare „Probleme“ auf – eine Reduzierung um 99,4 %. *“
>
> Quelle: Cisco Telemetry: *Cisco DNA Center*, 2020

* Basierend auf über 700 Unternehmensnetzwerken weltweit.

Aufgrund dieser Reduzierung können die Teams all ihre Anstrengungen auf die wirklich wichtigen Dinge konzentrieren, die negative Auswirkungen auf das Geschäft haben können.

Und dieses Thema ist nicht mehr auf das Unternehmensnetzwerk beschränkt. Da heute die meisten Netzwerktransaktionen außerhalb des traditionellen Unternehmensnetzwerks beginnen oder enden, benötigen NetOps-Teams auch für die öffentlichen Netzwerke, mit denen sie verbunden sind, Transparenz und Analysen. Dies ist besonders wichtig in Zeiten ungewöhnlicher Belastungen, wie zum Beispiel während der aktuellen Pandemie.

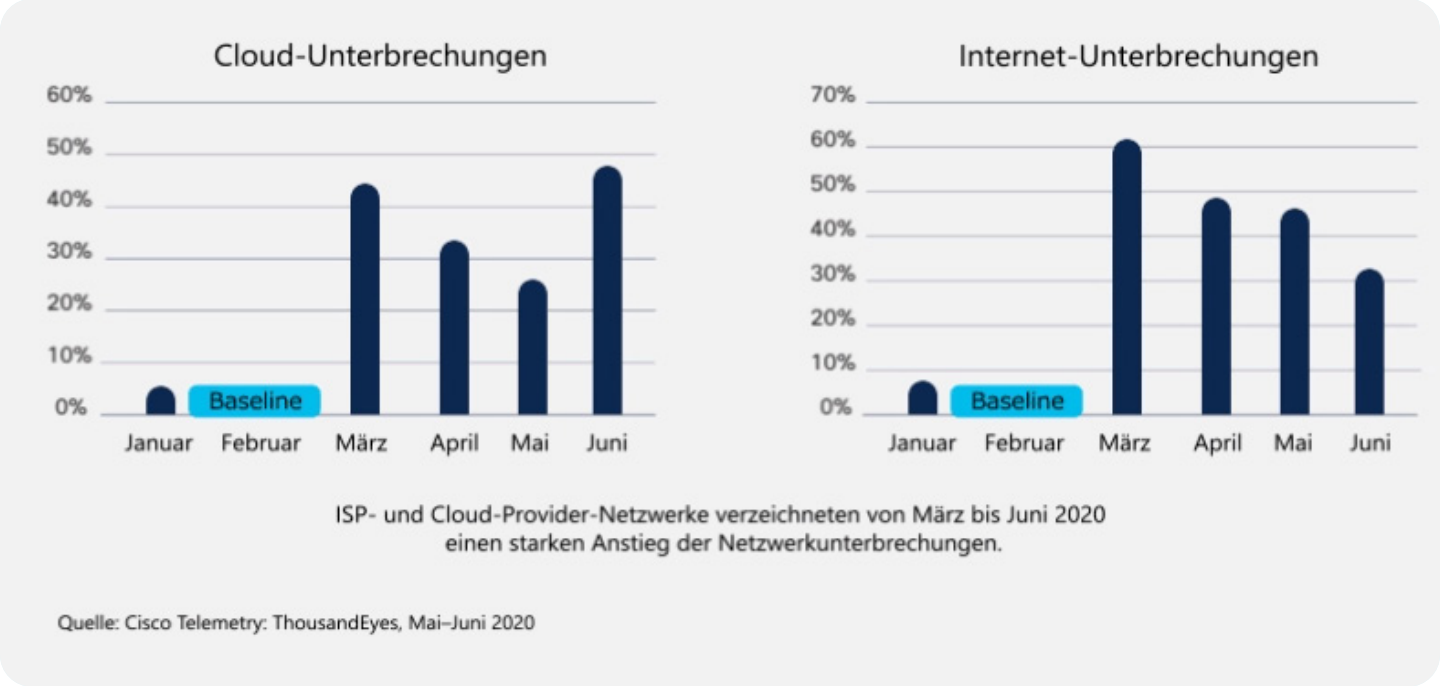
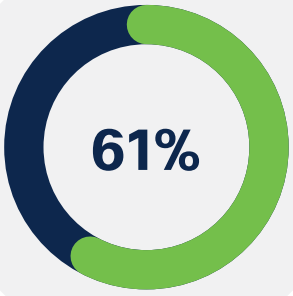


Abbildung 6: Unterbrechungen von Cloud- und Internet-Services nehmen während der Pandemie zu

> „Cisco ThousandEyes ermittelte zwischen Februar und März 2020 einen 61%igen Anstieg der Zahl der Netzwerkunterbrechungen in ISP-Netzwerken und einen 44%igen Anstieg in Netzwerken von Cloud-Providern.“
>
> Cisco ThousandEyes, „Internet Performance Report: COVID-19 Impact Edition“, 2020



Überlegungen zum Netzwerk: Um die Flut an Ereignissen bewältigen zu können, sollten NetOps-Teams KI-gestützte Netzwerkanalyse- und -Assurance-Systeme einsetzen, um Folgendes zu erreichen:

- **Genauere Erkennung:** Verbessern Sie die Genauigkeit der automatischen Problem- und Anomalienerkennung innerhalb von Netzwerkdomänen und darüber hinaus.
- **Schnellere Problembehebung:** Korrelieren Sie Ereignisse, um die wahrscheinlichste Ursache von Problemen und Anomalien zu erkennen und klar zu beschreiben.
- **Automatisierte Richtlinienverwaltung:** Identifizieren Sie Geräte, Anwendungen und Trends und bieten Sie empfohlene Aktualisierungen der Richtlinien an.
- **Weniger Leistungseinbußen:** Identifizieren Sie Muster und Trends und liefern Sie kontextbezogene Einsichten, die proaktive, korrigierende und präventive Maßnahmen beschleunigen.
- **Intelligence-basierte Vergleiche:** Stellen Sie Intelligence und Analysen bereit, anhand derer Netzwerkadministratoren ihre Netzwerkleistung mit globalen, branchenspezifischen oder regionalen Benchmarks vergleichen können.

Erfahren Sie, wie Sie KI-gestützte Einblicke nutzen können, um Ihre Netzwerke besser zu verwalten:

Netzwerkeinblicke für das Rechenzentrum

Schlussfolgerung

Verbesserung der Business Resiliency mit einer modernen Netzwerkplattform

Störende Ereignisse werden uns und unsere Netzwerke während unseres gesamten Berufslebens immer wieder vor Herausforderungen stellen. Es ist an der Zeit, neu darüber nachzudenken, wie Ihre **Netzwerkstrategie Ihre Business Resiliency-Strategie** stärkt, und die neuen Netzwerkfähigkeiten zu priorisieren, die am notwendigsten sind, um der nächsten großen Disruption einen Schritt voraus zu sein.

Die automatisierten, KI-gestützten Einblicke von Intent-Based Networks bieten eine leistungsstarke Plattform, mit der Sie sich an alle Umstände anpassen können. Sie liefern die Agilität, Sicherheit, Intelligence und Schnelligkeit, die zur Unterstützung der Widerstandsfähigkeit in allen Bereichen erforderlich sind:

- **Belegschaft:** Befähigen Sie Ihre Mitarbeiter mit sicherer Leistung der Enterprise-Klasse und Zugriff auf ihre Anwendungen dazu, von zu Hause, im Büro und an jedem anderen Ort sicher zu arbeiten.
- **Arbeitsumgebung:** Ermöglichen Sie Ihren Mitarbeitern die sichere Rückkehr ins Büro durch Wi-Fi-gestützte Überwachung, Warnungen und Einblicke
- **Workload:** Erleichtern Sie den Einsatz von Multicloud-Modellen zur Erhöhung der Widerstandsfähigkeit und schützen Sie Daten und Anwendungen unabhängig davon, wo sich die Workloads befinden – in öffentlichen Clouds wie auch in Rechenzentren vor Ort.
- **Betrieb:** Automatisieren Sie End-to-End-Netzrichtlinien und -segmentierung und vereinfachen Sie administrative Aufgaben bei gleichzeitiger Verbesserung der Transparenz, Reduzierung von Warnmeldungen und Beschleunigung der Problembehebung..

In dieser neuen Normalität ist es entscheidend, ein anpassungsfähiges Netzwerk zu haben, um alles zu unterstützen, was die Zukunft bringt. Wenn Sie über Ihre Business Resiliency-Strategie nachdenken, erörtern Sie, welche Schlüsselrolle Ihr Netzwerk im Rahmen dieser Strategie spielen kann.

Hier erhalten Sie weitere Informationen zu Business Resiliency

Weitere interessante Inhalte

Business resiliency | Webinare

Cisco Digital Network Architecture (Cisco DNA)

C96-744591-00 12/20