A1 Digital

WHITEPAPER

Bestmöglicher Schutz für dezentrale Netzwerke

Wie Unternehmen mit SD-WAN, Mikrosegmentierung, Zero Trust und dem Einsatz von KI ein Höchstmaß an Sicherheit für ihre IT- und OT-Infrastrukturen, Prozesse und Anwendungen schaffen – und sich durch die Nutzung von Network as a Service (NaaS) von technischen und monetären Beschränkungen befreien.

Von Philipp von Strobl-Albeg

Inhalt

Vorwort

Der Autor Philipp von Strobl-Albeg erläutert, welche sicherheitstechnischen Verbesserungen beim Einsatz zeitgemäßer Schutzkonzepte, Technologien und Dienstleistungen entstehen und beleuchtet die zugrunde liegenden Verfahren – verständlich und mit dem Blick von oben.

Traditionelle Netzwerke und Sicherheitsstrukturen sind von unseren aktuellen Arbeitsweisen einfach überfordert. Im Zuge fortschreitender digitaler Transformation stehen Unternehmen vor immensen technischen Herausforderungen, allen voran mit der rasant steigenden Komplexität, die sich aus der Vielfalt der Systeme, Plattformen und Prozesse ergibt, die bruchlos miteinander arbeiten sollen.

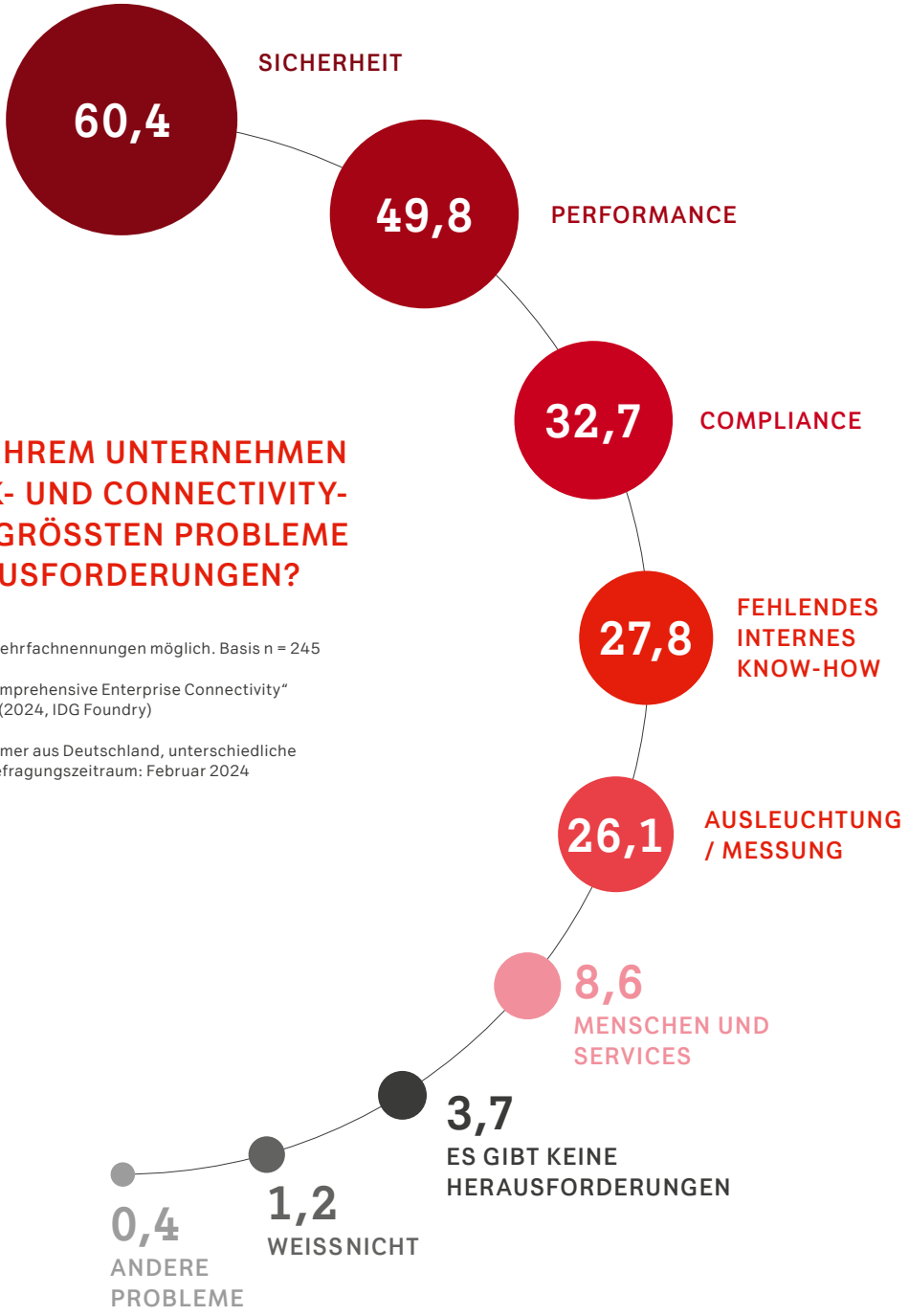
Das alles im Blick und sicherheitstechnisch im Griff zu behalten, bringt Netzwerkverantwortliche immer öfter an ihre Grenzen. Denn mit jeder neuen Virtualisierung, jedem zusätzlichen CloudDienst und jeder Standortvernetzung steigt der Komplexitätsdruck, ganz zu schweigen von all den RemoteWork und Mobil Anwendungen, die es heute ebenfalls zu verwalten und abzusichern gilt.

WAS SIND IN IHREM UNTERNEHMEN IM NETZWERK- UND CONNECTIVITY-BEREICH DIE GRÖSSTEN PROBLEME UND HERAUSFORDERUNGEN?

Angaben in Prozent. Mehrfachnennungen möglich. Basis n = 245

Quelle: Studie „Comprehensive Enterprise Connectivity“ (2024, IDG Foundry)

305 Studienteilnehmer aus Deutschland, unterschiedliche Branchen, Befragungszeitraum: Februar 2024



Netzwerke unter Komplexitätsdruck

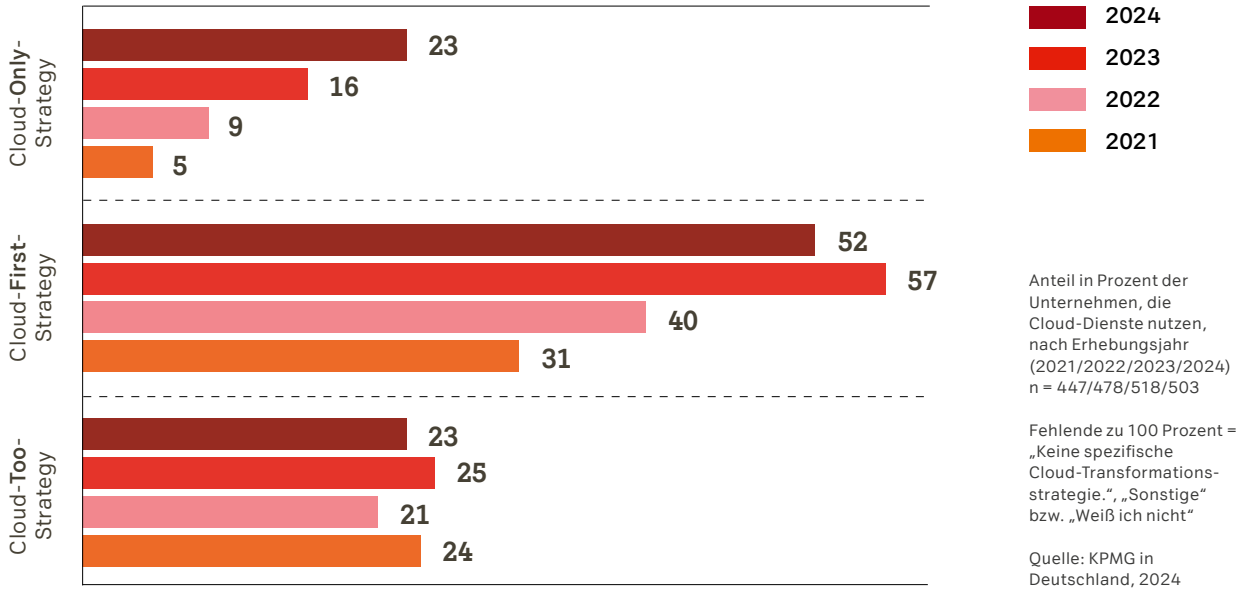
Je stärker Unternehmen ihre Ressourcen dezentralisieren und in die Cloud verlagern, und je mehr Arbeit außerhalb der Firmenzentrale stattfindet, desto größer wird der Steuerungs- und Verwaltungsaufwand – folglich vermehren sich auch Angriffsvektoren und damit Sicherheitsrisiken.

Tatsächlich erweisen sich traditionell angelegte Netzwerke und ihre Richtlinien immer häufiger als Hemmschuh für eine zukunftsorientierte, skalierbare und cloudgestützte Weiterentwicklung von Unternehmen. Denn einst bewährte Verfahren zur Verwaltung und Absicherung von Infrastruktur, Daten und Anwendungen greifen heute nur noch eingeschränkt oder gar nicht mehr.

Das Dilemma beginnt schon auf der Verbindungsebene. Für konventionelle WAN-Router ist heute oft schon die Priorisierung der Datenpfade und Anwendungen eine überkomplexe Aufgabe. Das führt zu verzögerter Verfügbarkeit und langsamen Ladezeiten, zu Störungen bei der Videokommunikation mit Kunden, Partnern und Kollegen sowie zu frustrierten Mitarbeitern in der IT.

CLOUD-TRANSFORMATIONSSTRATEGIE IM ZEITVERLAUF

Welche der folgenden Strategien trifft am ehesten auf die Cloud-Transformation in Ihrem Unternehmen zu?



Anteil in Prozent der Unternehmen, die Cloud-Dienste nutzen, nach Erhebungsjahr (2021/2022/2023/2024) n = 447/478/518/503

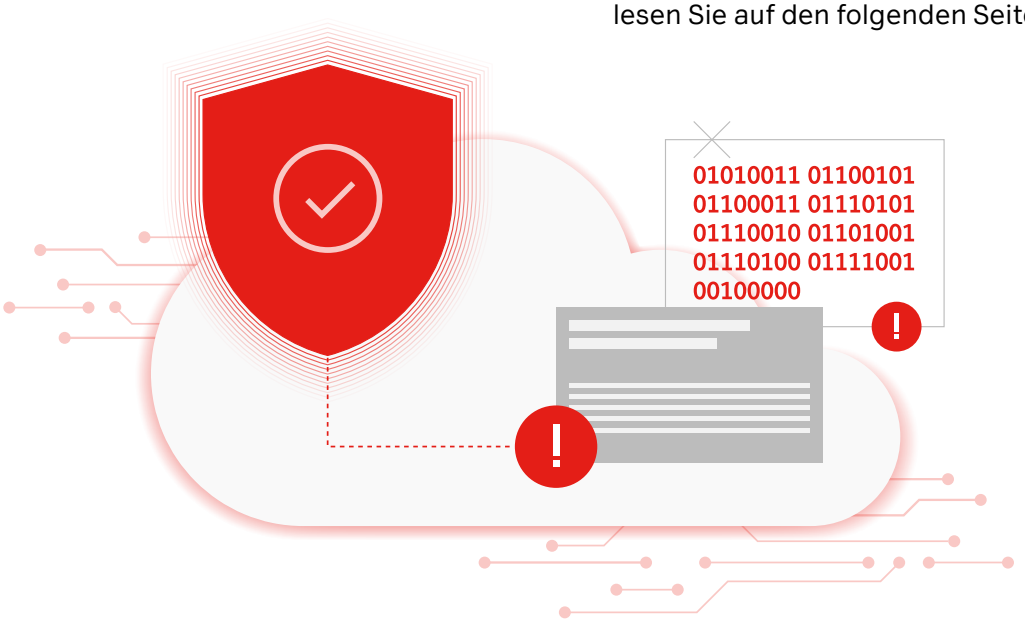
Fehlende zu 100 Prozent = „Keine spezifische Cloud-Transformationsstrategie.“, „Sonstige“ bzw. „Weiß ich nicht“

Quelle: KPMG in Deutschland, 2024

Und das ist nur die Spitze des Eisbergs. Denn angesichts der Vielfalt der genutzten Internetverbindungen, Apps und Cloud-Plattformen haben beispielsweise die als demilitarisierte Zonen (DMZ) angelegten Netzwerksegmente im Ernstfall kaum noch Sicherheitseffekte. Und hat ein Angreifer erst einmal einen Fuß in der Tür zum Netzwerk, kann er sich darin, Stand heute, relativ frei und schadenbringend entfalten.

Netzwerksicherheit und -leistungsfähigkeit – viele der betroffenen Unternehmen sehen akuten Handlungsbedarf.

Wie schwach es um die Netzwerksicherheit und -leistungsfähigkeit bei zunehmender Digitalisierung bestellt ist, haben nicht nur Analysten und ITK-Anbieter erkannt. Auch viele der betroffenen Unternehmen sehen akuten Handlungsbedarf. Was sie jetzt und für die Zukunft brauchen: eine flexibel belastbare Netzwerkinfrastruktur, einfachere Richtlinienplanung und deren Umsetzung, und natürlich wirksame Schutzkonzepte. Welche das sind und was sie leisten können, lesen Sie auf den folgenden Seiten.



Zero Trust – Vertraue nichts und niemandem

Der Haupt-Hoffnungsträger für den umfassenden Schutz der eigenen IT und Daten heißt Zero Trust Network Access (kurz ZTNA, oder noch kürzer ZT). Dieser Ansatz fußt auf der Prämisse, dass jedes System, jedes Gerät, jeder Nutzer und jede Verbindung – innerhalb und außerhalb des Netzwerks – zu jedem Zeitpunkt kompromittiert und angreifbar sein kann.

Ohne vorherige Überprüfung der Identität und „Vertrauenswürdigkeit" darf also nichts und niemand auf vernetzte Ressourcen zugreifen. Konsequent umgesetzt erstreckt sich ZTNA daher auf jedwede

- **Infrastruktur** und ihre **Komponenten**
- **Endgeräte**
- **Netzwerkgeräte**
- **virtuelle Server** und **Speicher**
- **Cloud-Komponenten** und **Dienste** (wie PAAS, IAAS, SAAS etc.)
- **Anwendungen**
- **Workloads**

sowie jeden einzelnen User innerhalb und außerhalb des Unternehmens, der auf physische und virtuelle Netzwerkteile sowie Anwendungen zugreift.

Grundlage für wirksamen ZTNA ist eine granulare Netzwerksegmentierung über alle Instanzen und Applikationen hinweg, die sogenannte **Mikrosegmentierung** (s. Infokasten, S. 6). Diese fächert die gesamte physische und virtuelle Infrastruktur eines Unternehmens fein auf und erfasst zugleich die Anwendungen und Workloads der einzelnen User und Gruppen.

Mikrosegmentierung macht es möglich, sicherheitstechnische Unbedenklichkeit kontinuierlich mit mehrfachen Kontrollen der jeweiligen ID und ihrer Richtlinienkonformität zu prüfen und das gesamte Geschehen im Netzwerk automatisch auf verdächtige Abweichungen hin zu untersuchen.

Mikrosegmentierung macht es möglich, sicherheitstechnische Unbedenklichkeit kontinuierlich zu prüfen und zu untersuchen.

Was leistet Mikrosegmentierung

Mikrosegmentierung gliedert die Assets der Infrastruktur in kleine Einheiten (Benutzer, Geräte, Endpunkten, Anwendungen) und ermöglicht so eine einfachere Absicherung von Workloads. Damit wird unbefugtes Eindringen in Unternehmenssysteme sehr schwierig, und falls es doch einmal dazu kommt, bleibt der Schaden auf den einzelnen, isolierten Bereich beschränkt.

So helfen die auf Mikrosegmente angewendeten Regeln schnell, einfach und gezielt beim Schutz von Ressourcen wie Smartphones, Laptops oder E-Mails, die oft mit eigenen Betriebssystemen laufen, deren Schwachstellen IT-Verantwortlichen nicht zentral und automatisiert mit Patches beseitigen können.

Mikrosegmentierung empfiehlt sich auch für Produktionseinrichtungen (Stichwort: OT-Geräte), Medizintechnik oder Industrieautomaten/Roboter, die in Workflows bzw. Prozesse eingebunden sind. Oder anders gesagt: Je feiner die Segmentierung, desto kleiner werden die Angriffsflächen.

VORTEILE ZTNA

- ✓ **Schutz der einzelnen Anwendungen und Workloads auf den Clients auch über verteilte Infrastrukturen hinweg, wie etwa in einer Multi-Cloud-Umgebung. Die granulare Einschränkung der Verbindungen hält mögliche Angreifer fern und begrenzt zudem interne Schwachstellen.**
- ✓ **Zeit- und Ressourcenersparnis durch zentral verwaltete Policies, Qualifizierung des Clients und wiederverwendbare Sicherheitsrichtlinien sowie schnelle Anpassungen an Compliance-Anforderungen durch API-basierte Automatismen der Richtlinien (OS, Endpunkte und Anwendungen).**
- ✓ **Erhöhte Sicherheit durch Überprüfung des Clients auf sein Sicherheitsniveau („Posture Check“).**
- ✓ **Infrastruktur-unabhängige Segmentierung und Umgebungssegregation der Systeme, Beispiel: Produktivdaten der Infrastruktur, die On-Premise liegen, lassen sich höchst granular von den Systemen und Entwicklungsumgebungen in der Public Cloud abschotten.**
- ✓ **Transparenz in Echtzeit durch zentralisierte Übersicht für alle Verbindungen im Netzwerk reduziert den Zeitaufwand für die Bewertung und Behebung von Problemen. Angriffe lassen sich schneller erkennen und abwehren.**

Schutz im Sinne von Zero Trust ergibt sich also durch die mehrfache Authentifizierung/Autorisierung von fein segmentierten Zugriffspunkten und Nutzerkonten, vor allem aber durch die leicht anpassbaren Richtlinien für den Zugriff.

Hierbei sind nach außen weder Verbindungspfade noch Anwendungen sichtbar, das heißt, Hacker haben deutlich weniger Angriffsflächen als bisher. Auch können sie sich nicht mehr lateral im ganzen Netzwerk bewegen. Stattdessen bleiben sie in dem kleinen Segment hängen, zu dem sie sich Zugriff verschafft haben, und können dort, wenn überhaupt, nur kurzfristig Schaden anrichten.

SD-WAN in Kürze

Geht es um die wirksame und kosteneffiziente Vernetzung von Standorten und hybrider IT bei gleichzeitiger Vermeidung und Abwehr von Cyberattacken, hat sich die SD-WAN-Technologie in den letzten Jahren als probates Mittel erwiesen. Diese Technologie findet bei Unternehmen zunehmend Anklang.

Vereinfacht gesagt ermöglicht SD-WAN eine unkomplizierte und verständliche Konfiguration der Anforderungen und Richtlinien für die sichere Übertragung von Applikationen jeder Art.

Dabei arbeitet SD-WAN radikal anders als traditionelle Netzwerkbetriebssysteme. Diese sind meist zentralisiert angesiedelt und arbeiten mit statischen Einstellungen für das gesamte Wide Area Network (WAN). Die Folge: Je mehr unterschiedliche, zunehmend cloudbasierte Anwendungen und Plattformen die Netzwerkadministratoren verbinden müssen, desto schwieriger und aufwändiger wird die Steuerung und Verwaltung.

Je mehr unterschiedliche, zunehmend cloudbasierte Anwendungen und Plattformen die Netzwerkadministratoren verbinden müssen, desto schwieriger und aufwändiger wird die Steuerung und Verwaltung.

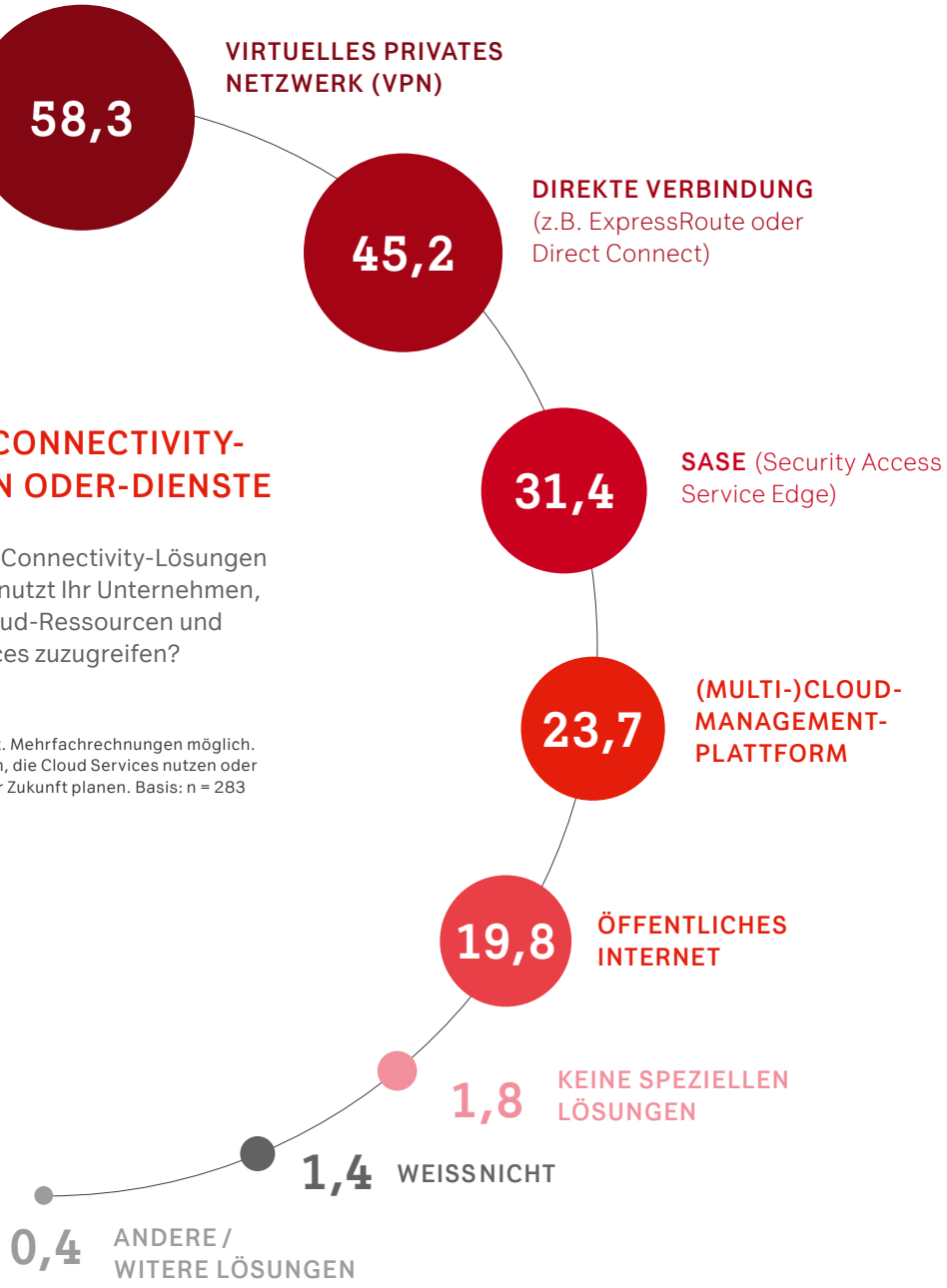
Ein SD-WAN hingegen basiert auf einer Softwareplattform, die benötigte Funktionen und Spezifikationen für alle Netzwerkebenen (von der Orchestrierung bis hin zur Steuerung einzelner Datenpakete) flexibel bereitstellt. Damit entfallen komplizierte Pfadzuordnungen, die dadurch verursachten Leistungsminderungen und die Betriebsrisiken, wie wir sie kennen.

Die (manuelle) Nachjustierung und Überwachung von Internetverbindungen und -anwendungen wird mit SD-WAN automatisiert. Der hohe Grad an Automatisierung und Intelligenz erhöht die Stabilität im Datenverkehr. Das führt zu konsistenterer Verfügbarkeit der Performance (kritische) Anwendungen und geringerer Störungsanfälligkeit, was sich in erheblicher Leistungsverbesserung niederschlägt – etwa bei Videokonferenzen, kollaborativen Tätigkeiten oder beim Streaming. Mit SD-WAN gehören ruckelnde Verbindungen, Tonausfälle oder gar Datenverluste der Vergangenheit an.

CLOUD-CONNECTIVITY-LÖSUNGEN ODER-DIENSTE

Welche Cloud-Connectivity-Lösungen oder-Dienste nutzt Ihr Unternehmen, um auf Cloud-Ressourcen und -Services zuzugreifen?

Angaben in Prozent. Mehrfachrechnungen möglich. Filter: Unternehmen, die Cloud Services nutzen oder dies in absehbarer Zukunft planen. Basis: n = 283



„Die Integration einer unternehmensweiten Sicherheitslösung in unser Netzwerk mit applikationszentrierter Sichtweise entspricht genau unseren Vorstellungen. Mit dem Einsatz von A1 Digital SD-WAN gehören die Beeinträchtigungen in der Sprach- und Videokommunikation im gesamten Unternehmen und über alle Standorte hinweg der Vergangenheit an."

Hubert Willberger
Senior Systems Engineer bei der Arineo GmbH

VORTEILE VON SD-WAN

Unternehmen, die bereits mit SD-WAN arbeiten, berichten, dass sie mit einer softwaredefinierten Netzwerkauslegung folgendes erzielen:

- ✓ Stressarme, zuverlässige Standortvernetzung
- ✓ Kostenoptimierung bei Infrastruktur, Verwaltung und Personal
- ✓ Vereinfachte betriebliche Abläufe (IT und OT) mit hoher Netzwerkzuverlässigkeit
- ✓ Intelligente Orchestrierung und Pfadzuordnung
- ✓ Beschleunigung und Stabilität von SaaS- und sonstigen Cloud-Anwendungen (durch Minimierung von Latenz, Jitter und Datenverlust)
- ✓ Mehr Agilität
- ✓ Einfachere und tiefere Einbettung von Netzwerkrichtlinien
- ✓ Mehr Sicherheit durch granulare Richtlinienkontrolle
- ✓ Besseres Monitoring
- ✓ Einfachere Anwendungsanalysen
- ✓ Höhere Qualität der Services und verbesserte Nutzererfahrung
- ✓ Programmierbarkeit, erhöhte Flexibilität
- ✓ Mehr Automatisierung
- ✓ Leistungsfähigere, zeitgemäße Schnittstellen/API

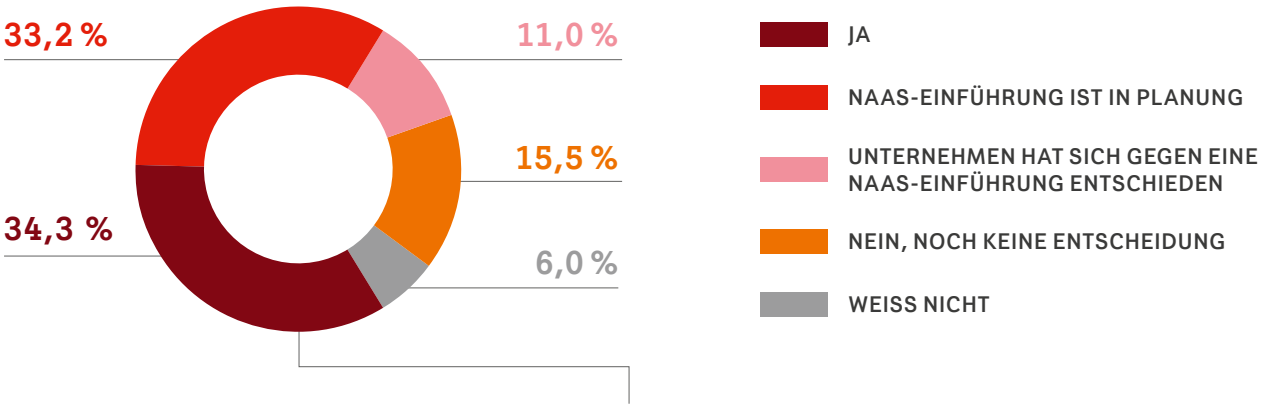
Network as a Service (NaaS)

Fachkräftemangel auf der einen Seite, Investitionsstau, Cloud-Sourcing-Strategien und Budgetbeschränkungen auf der anderen – um ein komplettes Team für die Cybersicherheit und Netzwerkverwaltung aufzubauen, fehlt es in vielen Unternehmen schlicht an Ressourcen.

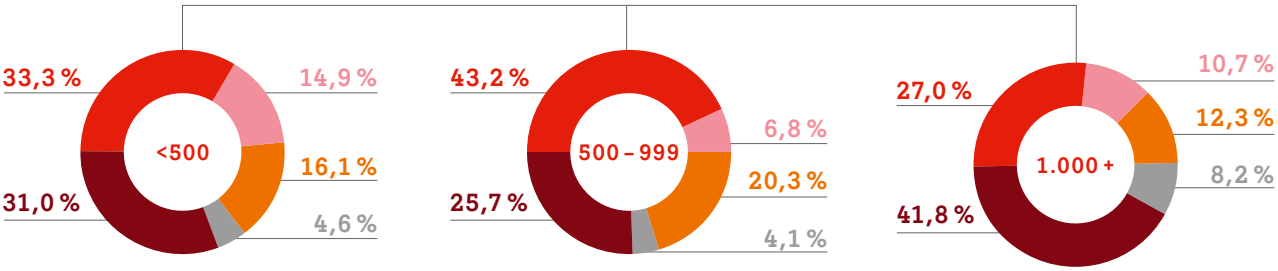
Abhilfe bietet NaaS. Denn mit diesen Diensten können Unternehmen hochmoderne, auf Skalierung und Resilienz ausgerichtete Technik und Funktionen nutzen, die mit konventionellen Netzwerken und unterbesetzten IT-Teams bisher nicht erreichbar waren – und müssen dafür kein Investitionskapital binden.

Bei A1 Digital erleben wir täglich, wie sehr NaaS den Kundenunternehmen dabei hilft, sicherer und flexibler zu arbeiten. Für sie ist NaaS der Schlüssel zu einer effizienteren und flexibeleren Nutzung ihrer Ressourcen (On Premise oder Cloud), zu erhöhter Cybersicherheit und zufriedeneren Anwendern.

SETZT IHR UNTERNEHMEN NETWORK AS A SERVICE (NAAS) EIN?



ERGEBNIS SPLIT: UNTERNEHMENSGRÖSSE (ANZAHL BESCHÄFTIGTE)



Angaben in Prozent. Filter: Unternehmen, die Cloud-Services nutzen oder dies in absehbarer Zukunft planen. Basis: n = 283

Mit NaaS an Ihrer Seite

Mit der individuell angepassten SD-WAN-Vernetzung und dem kompetenten Service-Teams bei A1 Digital haben Unternehmen die Sicherheit ihrer Netze durchgängig im Blick, ohne in zusätzliches Personal oder IT-Ausstattung investieren zu müssen. Denn die Experten und Plattformen für Ihren optimierten Netzwerkbetrieb stellen wir. Und die Dienste, die Sie nutzen, gehen als OPEX in Ihre Bilanz.

Bei der Planung unterstützen Sie unsere hochqualifizierten Fachleute auf ganzer Linie und schneiden die Services dann punktgenau auf Ihre Bedürfnisse zu. Welches Servicemodell für Ihr Unternehmen und Ihre Cloud-Strategie das Beste ist, ermitteln wir gemeinsam mit Ihren kaufmännischen und technischen Entscheidern. Letztlich können wir Ihr gesamtes Netzwerk managen, inklusive der Internet- und Cloud-Provider, mit denen Sie arbeiten.

Lassen Sie sich von uns beraten und erfahren Sie, wie sich Aufwand und Kosten für Ihre Vernetzungsinfrastruktur senken lassen, wie Sie Standorte und Mitarbeiter besser verbinden, sich wirksam vor Cyberattacken schützen und effektiver arbeiten können!

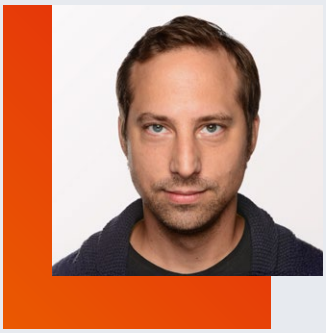
IHR KONTAKT

Holger Hartwig
Cybersecurity Experte

A1 Digital Deutschland GmbH
Unicorn Kustermannpark
Rosenheimer Str. 116
81669 München | Deutschland
M +49 162 338 08 39
holger.hartwig@a1.digital

Der Autor

Philipp von Strobl-Albeg
Leitung NaaS Delivery & Service Management



Philipp von Strobl-Albeg leitet das Team für NaaS Delivery & Service Management bei A1 Digital. Er besitzt langjährige Erfahrung in den Bereichen SD-WAN sowie Cybersecurity und hat ein tiefgreifendes Verständnis für Servicemanagement, IT-Infrastruktur und Sicherheit by Design. Philipp und sein Team unterstützen die Kunden von A1 Digital und gewährleisten eine erfolgreiche Customer Journey mit Network as a Service und komplementären Produkte.

A1 Digital

Kontakt Deutschland
A1 Digital Deutschland GmbH
Unicorn Kustermannpark
Rosenheimer Str. 116
81669 München | Deutschland

info@a1.digital
www.a1.digital

Kontakt Österreich
A1 Digital International GmbH & Co KG
Lassallestraße 9
1020 Wien | Österreich

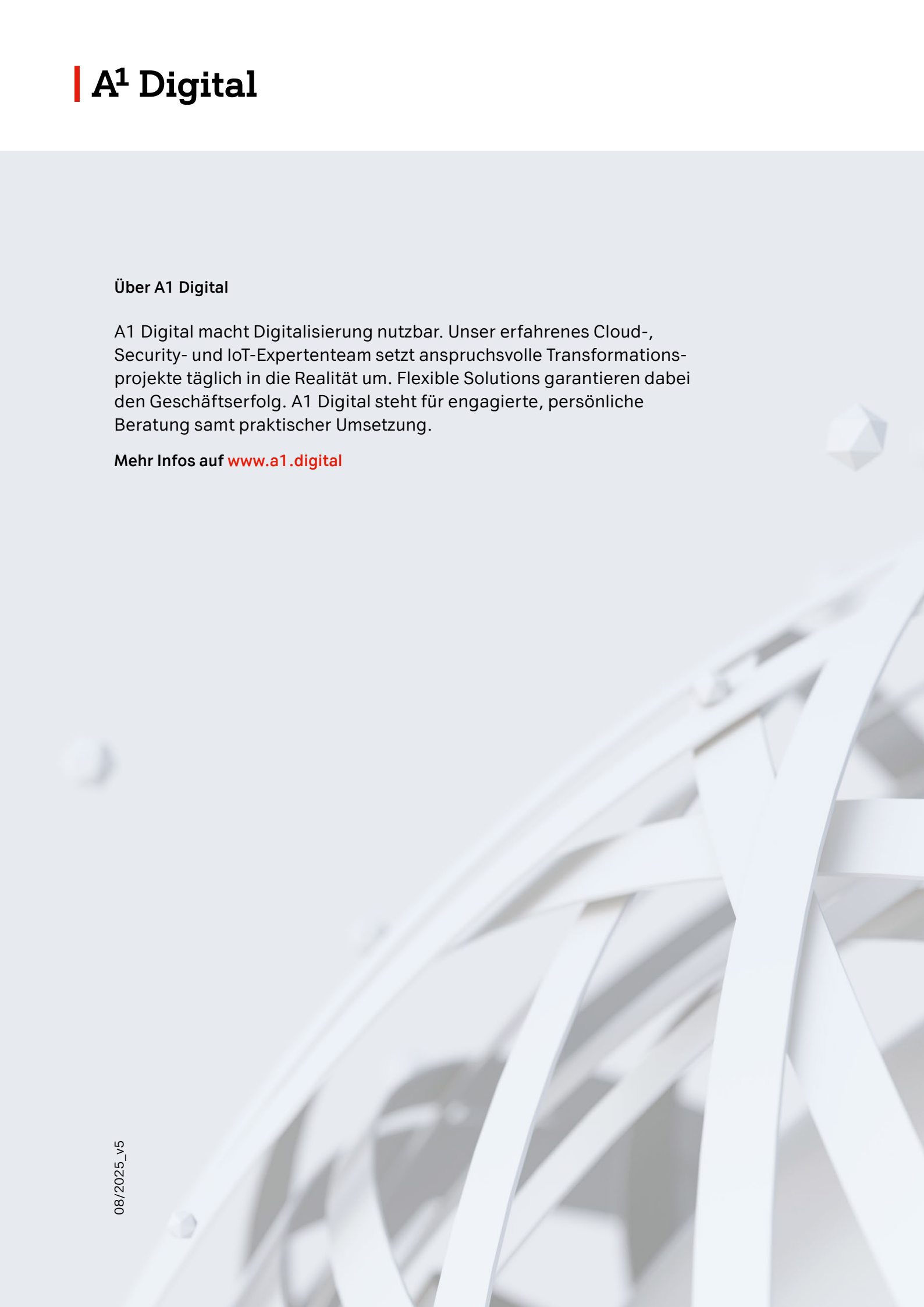
info@a1.digital
www.a1.digital

A1 Digital

Über A1 Digital

A1 Digital macht Digitalisierung nutzbar. Unser erfahrenes Cloud-, Security- und IoT-Expertenteam setzt anspruchsvolle Transformationsprojekte täglich in die Realität um. Flexible Solutions garantieren dabei den Geschäftserfolg. A1 Digital steht für engagierte, persönliche Beratung samt praktischer Umsetzung.

Mehr Infos auf www.a1.digital



08/2025_v5