arcserve®

Aktueller Bericht zum Stand der Datenausfallsicherheit im Unternehmen

Einblicke und Denkanstöße Ihrer Mitbewerber zur Bewertung und Verbesserung der Datensicherheit in Ihrem Unternehmen.

Unabhängige Umfrage im Auftrag von Arcserve

Zusammenfassung für die Geschäftsleitung

Vorwort

Die Datenausfallsicherheit ist für die meisten Unternehmen heutzutage ein Thema, dem sie höchste Priorität einräumen sollten. Und Ihr Unternehmen bildet da vermutlich keine Ausnahme. Mit dem geradezu explosiven Anwachsen und der Verbreitung von KI-gestützten Anwendungen erhöht sich auch das Risiko, Opfer eines Ransomware-Angriffs oder einer Datenschutzverletzung zu werden, da die Cyberkriminellen immer neue Wege finden, um Ihre Cyberabwehr zu überlisten oder zu überwinden. Sogar das Federal Bureau of Investigation (FBI) gab erst vor Kurzem eine Warnung in Bezug auf die zunehmende Bedrohung durch Cyberkriminelle heraus, die künstliche Intelligenz einsetzen, um „die Geschwindigkeit, den Umfang und die Automatisierung von Cyberangriffen zu erhöhen“[1].

Gleichzeitig arbeiten mehr und mehr Unternehmen an eigenen KI-Initiativen – dazu gehört vielleicht auch Ihres. Derlei Projekte erfordern fast immer die Verarbeitung riesiger geschützter Datenbestände und kommen zum Stillstand, wenn diese Daten verloren gehen oder gestohlen werden. Nach Abschluss des Modelltrainings müssen die Trainingsdaten aus Gründen der Governance und der Einhaltung von Vorschriften aufbewahrt werden (z. B. um eine Prüfung der Modellvorhersagen auf Voreingenommenheit zu unterstützen).

97 %
der Befragten stimmen zu, dass ihre gesicherten Daten „mäßig“ oder „extrem“ wichtig für den Erfolg ihres Unternehmens sind.

69 %
der Befragten gaben an, dass die Geschäftskontinuität nicht garantiert werden könnte, wenn sie den Zugang zu ihren Daten verlieren würden.

Alle bereits bekannten Risiken für Ihre Daten bestehen aber ebenfalls weiterhin: böswillige Akteure (insbesondere bei Remote-Arbeit), versehentliche Benutzerfehler, Naturkatastrophen usw.

Arcserve hat eine Umfrage für erfahrene IT-Fachleute in Auftrag gegeben, die direkt mit den Themen Datensicherung und -sicherheit beauftragt wurden, um ein besseres Verständnis darüber zu erhalten, wie kleine und mittelständische Unternehmen mit diesen neuen Herausfoderungen umgehen. Wir freuen uns sehr darüber, die daraus gewonnenen Erkenntnisse mit Ihnen zu teilen und möchten auch einige unserer Gedanken in Bezug auf die Verringerung des Risikos von Datenverlust und Ausfallzeiten beifügen.

Wir hoffen, dass dieser Einblick in die Herausforderungen, denen sich Ihre Mitbewerber in Bezug auf die Datensicherung stellen müssen und wie sie ihnen entgegnen Sie dabei unterstützen wird, die Strategie Ihres Unternehmens in Bezug auf die Ausfallsicherheit Ihrer Daten und deren potenziellen Lücken zu bewerten. Sie könnten sogar dazu beitragen, Ihre Empfehlungen an interne Entscheidungsträger zu untermauern.

Ihr Team von Arcserve

1 FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence. 8. Mai 2024

Die Beteiligung der Führungskräfte ist wichtig. 1 von 4 haben es noch nicht.

Die Implementierung von Best Practices in Bezug auf die Datensicherung und Cybersicherheit mit effizienten Technologien erfordert Investitionen in IT und andere Bereiche. Die Zustimmung der Führungskräfte, die die finanziellen Entscheidungen in Ihrem Unternehmen treffen, ist unabdingbar.

Zu viele Manager räumen der Datenausfallsicherheit immer noch keine Priorität ein und unsere Umfrage bestätigt dies. In Gesprächen mit kleinen und mittelständischen Unternehmen hören wir Dinge wie „Wir sind zu klein, die Angreifer haben uns gar nicht auf dem Schirm.“. Die harte Realität ist, dass sie genau das doch tun. Wenn sie dann allerdings „ins Visier genommen“ werden, dann sind sie vermutlich zu klein, um von der Allgemeinheit wahrgenommen zu werden.

Über 25 %
der Befragten konnten nicht eindeutig bestätigen, dass die Führungskräfte ihres Unternehmens sich um die Sicherung der Unternehmensdaten Gedanken machen.

Und dennoch ...

69 %
der Befragten gaben an, dass die Geschäftskontinuität nicht garantiert werden könnte, wenn sie den Zugang zu den unternehmenseigenen Daten verlieren würden.

Eine erfolgreiche Initiative im Bereich Datenausfallsicherheit beginnt ganz oben. Die Führungskräfte und der Vorstand müssen einverstanden sein und an einem Strang ziehen. Wie jede Initiative, die Veränderungen hervorbringt, benötigt sie jedoch die Unterstützung und auch die unternehmensweite Zustimmung aller Mitarbeitenden, und zwar abteilungsübergreifend. Sie erfordert auch eine Abstimmung und das Engagement von Partnern und Service Providern.

Der Bericht der Cybersecurity & Insfrastructure Security Agency „Making a Business Case for Security“[2] enthält wertvolle Ratschläge, wie man den Vorstand dazu bringt, mitzumachen.

Die Invesitionen in Datensicherung steigen an

Die Befragten gaben an, dass ihr IT-Unternehmen bereits einen Großteil ihres IT-Budgets für Datensicherung und -wiederherstellung aufwendet.

Die hohe Standardabweichung (21 %) bei den Antworten untermauert jedoch die obige Feststellung, dass eine beträchtliche Anzahl von Unternehmen in diesem Bereich immer noch deutlich zu wenig investiert. Vermutlich zwingen begrenzte IT-Gesamtbudgets die IT-Verantwortlichen zu schwierigen Abwägungen.

Die folgenden Daten sind allerdings beruhigend:
Die überwältigende Mehrheit der IT-Leiter möchte ihr Budget für die Datensicherung erhöhen.

22 %
beträgt der durchschnittliche Anteil des IT-Investitionsbudgets der befragten Unternehmen, der für Datensicherung und -wiederherstellung bereitgestellt wird.

89 %
der befragten Unternehmen erwarten zum Beispiel, dass sie ihr Datensicherungs-budget in Zukunft erhöhen müssen.

Für sie könnte der Security Budget Benchmark Report 2023 interessant sein, denn er zeigt auf, dass das durchschnittliche IT-Sicherheitsbudget um 6 % gestiegen ist. Insgesamt ist dies ein Wachstum, das 65 % langsamer ist als zuvor.[3] In vielen Fällen muss sich das Wachstum im Bereich Datensicherung jedoch deutlich beschleunigen.

Selbst wenn jetzt der Datensicherung ein höheres Budget zugewiesen wird, bleibt die Frage, wie die Unternehmen dieses am besten einsetzen.

Es ist wichtig, den Kompromiss zwischen einem kunterbunten Flickenteppich individuell konfigurierter, fein abgestimmter Komponenten und einer integrierten, einheitlichen Lösung, die ihre Aufgabe zuverlässig erfüllt, abzuwägen. Erstere bieten Ihnen möglicherweise einzigartige Anpassungsmöglichkeiten, während letztere einfacher zu implementieren sind und schneller einen Mehrwert bieten.

2 Making a Business Case for Security I An Interagency Security Committee Best Practice. Ausgabe 2023
3 2023 Security Budget Benchmark Summary Report

Disaster Recovery und Geschäftskontinuität

Teil 1: Der Countdown läuft

Wie hoch wären die Kosten (monetärer Art und Rufschädigung), wenn Ihr Unternehmen nicht mehr auf seine Daten zugreifen kann.

Hier einige Angaben aus seriösen Quellen:

Nur 31 %
der Befragten sind sich sicher, dass sie ihre verlorenen Daten innerhalb von 24 Stunden wiederherstellen könnten.

Finanzielle Risiken	Compliance-Risiken	Risiken in Bezug auf die Rufschädigung
• **2,7 Mio. US-Dollar:** durchschnittliche Wiederherstellungskosten bei einem Ransomware-Angriff ohne Lösegeldzahlungen (Sophos State of Ransomware 2024) • **2 Mio. US-Dollar:** durchschnittliche Lösegeldzahlung, +50 % gegenüber dem Vorjahr • **9.000 US-Dollar/Minute:** durchschnittliche Kosten für Ausfallzeiten in großen Unternehmen (Forbes) • **5 Mio. US-Dollar/Stunde** für Organisationen mit hohem Risiko (Finanzwesen, Gesundheitswesen) • **4,4 Millionen US-Dollar:** durchschnittliche Kosten einer Datenschutzverletzung im Jahr 2023	• **USA:** Data Privacy Act, CCPA • **Europa:** DSGVO • **Japan:** Act on Protection of Personal Information (APPI)	• Beschädigte Beziehungen zu Kunden, Partnern und Interessengruppen

Ist es hinnehmbar, dass Unternehmen mehr als 24 oder 48 Stunden brauchen, bis sie ihre Daten wiederhergestellt haben?

Wir haben diese Frage gestellt und als Antwort ein klares Nein bei jeweils zwei von drei Unternehmen erhalten.

Nur 34 %
der Befragten geben an, dass ihr Unternehmen mehr als 48 Stunden dafür einrechnen darf, seine Daten wiederherzustellen, ohne dass die Geschäftskontinuität signifikant beeinträchtigt wäre.

Teil 2: Übung macht den Meister

Die gute Nachricht ist, dass die meisten Unternehmen (70 %) angeben, wöchentliche oder monatliche Datenwiederherstellungsübungen durchzuführen, aber mehr als ein Fünftel der Unternehmen testet ihre Systeme nicht häufig genug.

Regelmäßige Datenwiederherstellungsübungen sind unerlässlich, da sie dazu beitragen, dass die Recovery Time Objective (RTO) und Recovery Point Objective (RPO) des Unternehmens im Katastrophenfall eingehalten werden können.

70 %
der Befragten geben an, dass ihr Unternehmen wöchentliche oder monatliche Übungen in Bezug auf die Datenwiederherstellung durchführt, um die Geschäftskontinuität zu wahren.

Bereits bekannte Risiken: Viele haben ihre Lektion gelernt. Und es war nicht einfach. Manche gehen das Ganze mit einem übermäßigen Selbstvertrauen an.

Viele IT-Verantwortliche, mit denen wir gesprochen haben, sind erfahrene Veteranen. Sie wurden schon häufiger mit dem Szenario konfrontiert und haben gesehen, wie diese Risiken nur allzu real wurden.

Etwa die Hälfte der Befragten hat mit „Ja“ geantwortet, als wir sie gefragt haben, ob sie schon einmal entscheidende Umsatzverluste wegen Datenverlusten hinnehmen mussten.

Denken Sie einmal über diese Erkenntnis und ihre Auswirkungen auf die Führungskräfte eines Unternehmens nach. Für diejenigen, die sich auf die Steigerung der Einnahmen und die Kontrolle der Kosten konzentrieren, sollte diese Aussicht auf einen evtl. Rückgang der Einnahmen ein Weckruf sein. Es hat uns allerdings nicht überrascht, dass die Befragten ihren Standpunkt selbstbewusst verteidigten:

47 %
der Befragten hat angegeben, dass ihr Unternehmen schon einmal entscheidende Umsatzverluste wegen evtl. Datenverluste hinnehmen musste.

Die IT-Führungskräfte, mit denen wir gesprochen haben, sind überwiegend sehr zuversichtlich, dass sie in der Lage wären, Bedrohungen für ihre Daten durch Altlasten wie Fehlverhalten von den eigenen Mitarbeitenden und Naturkatastrophen zu erkennen und zu beseitigen.

86 %
der Befragten gaben an, dass ihr Unternehmen entweder „sehr“ oder „ausgesprochen“ zuversichtlich ist, Naturkatastrophen zu erkennen und ihnen zu entgegnen.

Der Verizon Data Breach Investigations Report (DBIR) aus dem Jahr 2024 stellte fest, dass bei **25 Prozent** der Datenschutzverletzungen Benutzer innerhalb des Unternehmens beteiligt waren.4 Nach Angaben der NOAA gab es bis Juli 2024 bereits fünfzehn bestätigte Wetter- oder Klimakatastrophen in den USA, die Schäden von **jeweils mehr als 1 Milliarde Dollar** verursacht haben.

Diese „etablierten“ Bedrohungen in Bezug auf Datenverluste sind inzwischen hinreichend bekannt. Und nein, es werden nicht weniger werden.

Überrascht haben uns dagegen die Antworten auf unsere Folgefragen. Lässt sich dieses Maß an Vertrauen dadurch erklären, dass sie die bewährten Verfahren der 3-2-1-1-Backup-Strategie anwenden?

Es scheint eher so zu sein, dass eines von vier Unternehmen sich bei dem Thema überschätzt.

23 %
der Befragten geben an, dass ihr Unternehmen eine 3-2-1-1-Backup-Strategie noch nicht eingeführt hat und weitere 6 % sind sich nicht sicher, ob dem so ist.

Ransomware: Weitreichende Auswirkungen und dauerhafte Konsequenzen

Schon gewusst?

Die letzte „1“ in 3-2-1-1 steht für unveränderliche Speicherung von Backups, die für die Wiederherstellung im Notfall und die Vermeidung von Datenverlusten unerlässlich ist. Unveränderliche Backups werden in einem einmalig beschreibbaren und mehrfach lesbaren (WORM) Format gesichert, das von unbefugten Benutzern weder geändert noch gelöscht werden kann und bietet damit eine letzte Verteidigungslinie gegen Datenverlust.

Angesichts der sich entwickelnden Bedrohungslage und der Zunahme von Ransomware-Services (RaaS) ist es eine Frage von WANN und nicht OB man Opfer eines Ransomware-Angriffs wird.

Viele IT-Führungskräfte haben angegeben, dass sie darauf vorbereitet sind. Die Praxis zeigt jedoch, dass nach einem Angriff nicht immer alle Daten wiederhergestellt werden können.

80 %
der befragten Unternehmen mussten sich bereits mit einem Ransomware-Angriff auseinandersetzen.

30 %
ist der durchschnittliche Prozentsatz der Daten, die die Befragten nach einem erfolgreichen Ransomware-Angriff nicht wiederherstellen konnten.

Und der Wiederherstellungsvorgang bleibt nach wie vor zeitaufwendig und stört den Geschäftsbetrieb.

Es wurde offensichtlich, dass die meisten Unternehmen es sich nicht leisten können, mehr als 48 Stunden für die Wiederherstellung nach einem Datenvorfall zu benötigen, um Umsatzeinbußen zu vermeiden.

82 %
der von Ramsomware betroffenen Befragten behaupten, dass sie ihre Daten innerhalb von 48 Stunden wiederherstellen können, 18 % geben an, dass ihnen das nicht möglich ist.

Naturkatastrophen, Fehler von Mitarbeitenden im Unternehmen und Ransomware gehören heute zum Alltag. Was sich für diese Risikofaktoren geändert hat, ist, dass sich die Wahrscheinlichkeit, dass sie eintreten, deutlich erhöht hat. Und auch die Auswirkungen, falls (wenn) sie eintreten.

Vorbereitung ist die beste Verteidigung: Das Ziel sollte eine robuste Infrastruktur für die Datenausfallsicherheit sein, die Ihre Schutz-, Sicherungs- und Wiederherstellungskomponenten in einer einheitlichen Datensicherungsumgebung konsolidiert und als Teil einer 3-2-1-1-Sicherungsstrategie implementiert.

SaaS-Anwendungen Eine unterschätzte Säule der Datenausfallsicherheit

SaaS-Anwendungen spielen in fast jedem Unternehmen heute eine wichtige Rolle.

Etwa 82 % der Befragten gab an, dass ihre Unternehmen zehn oder mehr SaaS-Anwendungen einsetzen, was das Ausmaß und ihre Bedeutung in modernen Unternehmen unterstreicht. Diese Anwendungen generieren und verwenden eine Menge Daten, die von entscheidender Bedeutung sind, wenn es darum geht, dass die Unternehmen problemlos arbeiten und ihre Kunden glücklich machen können.

Viele Unternehmen sind sich dennoch nicht bewusst, wie es sich mit den Daten verhält, die von diesen Anwendungen verarbeitet werden.

Nur ein Bruchteil von SaaS-Anwendungen wird von den Unternehmen selbst überwacht und gesichert.

59 %
der befragten Unternehmen verwenden 10 bis 30 SaaS-Anwendungen

19 %
verwenden sogar zwischen 30 und 50

30 %
der SaaS-Anwendungen werden nicht überwacht/gesichert

Von den 70 %, die überwacht/gesichert werden, sind 40 % ausgelagert/unbeaufsichtigt.

SaaS-Daten unterliegen in der Regel dem Modell der geteilten Verantwortung, bei dem der Eigentümer der Daten (d. h. Ihr Unternehmen) für die Datensicherung und die Datenwiederherstellung verantwortlich ist.

Beispiel: Das Shared Responsibility Model von Microsoft

	Customer	Microsoft
Preparation	• Geschäftskontinuität und Katastrophenvorbereitung • Dokumentation der bekannten guten Zustände • Überwachung und Datenaufbewahrung • Operative Sicherheit	• Funktionen für die Identitäts- und Zugangsverwaltung • Tools für die Dokumentation • Verfügbarkeit und Konsistenz von Protokollen • Plattform-Sicherheit
Recovery	• Wiederherstellen von wiederherstellbaren Ressourcen • Wiederherstellen von vorherigen Konfigurationen	• Verfügbarkeit von wiederherstellbaren Ressourcen (zeitlich begrenzt) • Verfügbarkeit von APIs

Und dennoch: unter den 40 % der im Rahmen unserer Umfrage Befragten, die angaben, dass ihre Unternehmen wegen einer Verletzung von SaaS-Anwendungen im vergangenen Jahr einen Datenverlust hinnehmen mussten, geben nur knapp über die Hälfte (51 %) ihrem SaaS-Provider die Schuld daran.

In diesem zusätzlichen Kontext wird die Bedeutung von SaaS-Backup-Lösungen noch einmal besonders deutlich, da sie ein hohes Maß an Sicherheit und Autonomie für Unternehmen bieten, die ihre SaaS-Daten sichern wollen, ohne sich auf die SaaS-Anbieter zu verlassen.

Die Auswirkungen der Nichteinhaltung von Vorschriften

Die Anforderungen an die Einhaltung der Vorschriften gibt es seit Jahrzehnten und sie werden immer strenger. Gleichzeitig wird es immer schwieriger, die Einhaltung der Vorschriften zu gewährleisten, da die IT-Infrastruktur immer komplexer wird.

So wurden beispielsweise durch die jüngste NIS2-Richtlinie der EU der Erfassungsbereich der Branche erweitert und neue Vorschriften eingeführt.
Weltweit gibt es in der Entwicklung befindliche rechtliche Rahmenbedingungen, die in Zukunft ähnliche Auswirkungen haben könnten.

Etwa die Hälfte aller Befragten hat bestätigt, dass ihre Unternehmen bereits mit Geldbußen aufgrund unzureichender Datenschutzmaßnahmen belegt wurden.

Die Einhaltung der einschlägigen Vorschriften wie DSGVO, CCPA und HIPAA ist nicht nur für den Ruf Ihres Unternehmens von entscheidender Bedeutung. Wenn Sie dies nicht tun, kann Sie das sogar richtig teuer zu stehen kommen.

NIS2-Richtlinie, Artikel 21, Paragraph 2:
Die Maßnahmen … beruhen auf einem All-Gefahren-Ansatz, der darauf abzielt, Netz- und Informationssysteme sowie die physische Umgebung dieser Systeme vor Zwischenfällen zu schützen, und umfassen mindestens Folgendes:.

Abschnitt (c): Geschäftskontinuität, wie z. B. die Verwaltung von Backups und Disaster Recovery sowie Krisenmanagement5

43 % der befragten Unternehmen wurden aufgrund nicht adäquater Datensicherungsmaßnahmen mit Geldbußen belegt.

Und wie geht das am besten? Die harte Tour besteht darin, dass Ihre internen Teams Beratung und Anleitung durch Dritte suchen müssen. Einfacher geht es, wenn Sie eine Lösung für die Datenausfallsicherheit mit integrierten Hebeln für die Einhaltung der Vorschriften, wie Zugriffskontrollen und Versionskontrolle, einsetzen.

5 RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

Zusammenfassung

Auch wenn Unternehmen ihre Datensicherungspraktiken und ihre Ausfallsicherheit inzwischen verbessern, bleiben das Risiko von Datenverlusten und die Bedeutung der Gewährleistung der Geschäftskontinuität für IT-Verantwortliche ein wichtiges Thema. Gleichzeitig gibt es sichtbare Diskrepanzen zwischen den Erwartungen und der Realität, da Unternehmen sich zwar zur Datensicherung bekennen, aber weiterhin unter den Folgen von Datenverlusten leiden.

Und das kommt nicht überraschend. Mit Ransomware und anderen potenziellen Bedrohungen sehen sich die Unternehmen, ob klein oder groß (und alle, die dazwischen sind) mit neuen Risiken konfrontiert. Die IT-Verantwortlichen wollen in allen Bereichen zusätzliche Investitionen in Datenschutz, Datensicherung und Notfallwiederherstellung tätigen. Die Befolgung von Best Practices vor Ort kann dazu beitragen, den Schutz trotz begrenzter Budgets zu maximieren.

Als Pionier auf dem Gebiet der Datenausfallsicherheit ist Arcserve gut darauf vorbereitet, Ihnen zu helfen. Arcserve Unified Data Protection (UDP) und Arcserve SaaS Backup sind kosteneffiziente Lösungen für die Ausfallsicherheit von Daten. Sie sind einfach zu implementieren und bieten schnell einen Mehrwert, indem sie die Wiederherstellung sicherstellen und so Ausfallzeiten und Datenverluste minimieren.

Arcserve beantwortet Ihnen gerne alle Fragen und zeigt Ihnen, wie Sie Ihre Daten, wo immer diese auch gespeichert sind, besser schützen können. Möchten Sie weitere Informationen erhalten?
Dann setzen Sie sich unter arcserve.com/de/contact-us mit uns in Verbindung.
Entdecken Sie alle Arcserve-Funktionen unter arcserve.com/de/products-overview
Sie erreichen uns unter info@arcserve.com

METHODIK

Arcserve war es ein Anliegen, ein besseres Verständnis darüber zu erlangen, wie Führungskräfte im Bereich Datensicherheit im Falle einer Datenschutzverletzung oder eines Ausfalls ihre Daten wiederherstellen. Darum hat Arcserve ein unabhängiges Marktforschungsunternehmen damit beauftragt, 150 Führungskräfte im Bereich Datensicherheit in den USA in Bezug auf die Themen Datenwiederherstellung und Datenausfallsicherheit zu befragen. Das Team der Befragten besteht zu gleichen Teilen aus kleinen und mittleren Unternehmen (< 1000 Mitarbeiter) und größeren Unternehmen (zwischen 1000 und 5000 Mitarbeitern). Die Fehlermarge für diese Umfrage beträgt +/- 6,9 % bei einem Konfidenzniveau von 95 %.

Damit Sie Arcserve Datenausfallsicherheit in Aktion erleben können, fordern Sie jetzt unter arcserve.com/de/request-demo eine Demo an!

Über Arcserve

Arcserve ist weltweit einer der Top-5-Anbieter von Datensicherungslösungen und einer einheitlichen Plattform für die Datenausfallsicherheit. Unabhängig von Standort und Komplexität bietet das Unternehmen eine Komplettserie von Best-in-Class-Lösungen zum Verwalten, Sichern und Wiederherstellen aller Daten-Workloads für KMU bis hin zu großen Unternehmen an. Mit den Lösungen von Arcserve werden komplexe Datensicherungsaufgaben vereinfacht. Sie bieten erstklassige, kosteneffiziente, agile und massiv skalierbare Datensicherung und Sicherheit für alle Datenumgebungen. Dazu gehören On-Prem-, Off-Prem- (einschließlich DRaaS, BaaS und Cloud-to-Cloud), Hyper-Converged- und Edge-Infrastrukturen. Über fast drei Jahrzehnte entwickelt das Unternehmen nunmehr preisgekrönte IP und setzt dabei kontinuierlich den Fokus auf Innovation. Damit ist gewährleistet, dass Partner und Kunden einschließlich MSPs, VARs, LARs und Endbenutzer die Daten-Workloads und -Infrastrukturen der nächsten Generation rasch und unkompliziert bewältigen können.