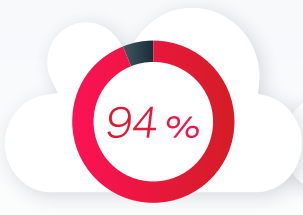
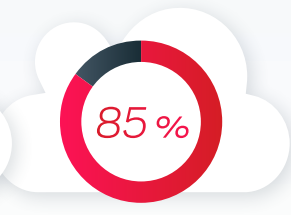
Bewältigung der wichtigsten Schmerzpunkte der Cloud

Cloud-Strategien werden zunehmend komplizierter.

Wenn Unternehmen ihre Ressourcen in die Cloud verlagern, erkennen sie häufig, dass ein schlecht verwalteter Speicher zu erheblichen Kosten führen kann. Obwohl die Cloud zahlreiche Vorteile bietet, schafft sie auch neue Herausforderungen: Sicherheitsrisiken, Ungewissheit, Kosten und Komplexität.



der Unternehmen verfügen derzeit über eine Multicloud-Strategie[1]



der Unternehmen werden bis 2025 einen Cloud-First-Ansatz verfolgen[2]

Herausforderung Nr. 1

Cybersicherheit ist ein schwieriger Bereich

Ransomware und andere Formen von Malware sind ein riesiges Problem, das sich ständig verschlimmert.

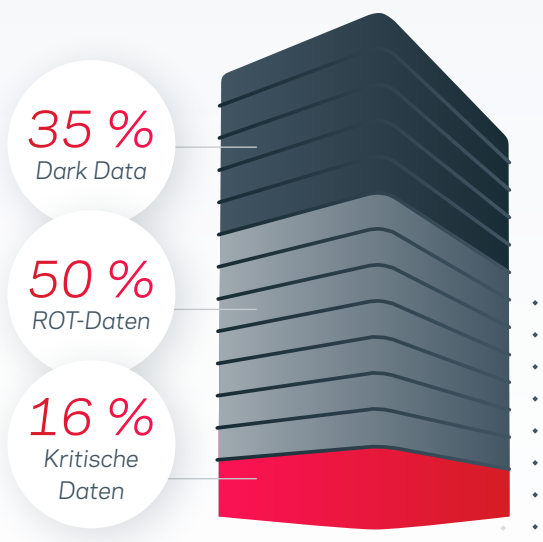
- Allein im ersten Halbjahr 2022 gab es 2,8 Milliarden Malware-Angriffe. Das entspricht einem Anstieg von 11 % im Vergleich zu den vorangegangenen sechs Monaten.[3] Die Folge: Auch die Zahl der Schwachstellen und die Kosten gehen steil in die Höhe.
- Die durchschnittlichen Kosten eines Angriffs betrugen 2021 1,85 Millionen USD.[4]
- Veritas fand heraus, dass 77 % der Unternehmens- und IT-Leiter überrascht sind, wie hoch die Ausgaben für Datenmanagement- und Cybersicherheits-Tools waren.[1]
- Mängel bei der Cybersicherheit sind kostspielig und können zu Umsatzeinbußen, Geldstrafen, Anwaltskosten sowie Marken- und Reputationsschäden führen.

Herausforderung Nr. 2

Ungewissheit, Dark Data und mangelnde Transparenz sind gefährlich

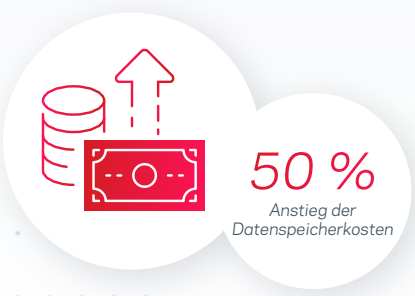
Die Datensichtbarkeit vom Edge über den Core bis zur Cloud ist für den Schutz und die Ausfallsicherheit der Daten von entscheidender Bedeutung.

- Die meisten IT-Fachkräfte sind nicht in der Lage, den gesamten Daten-Footprint ihres Unternehmens zu verfolgen. Dadurch wird es schwieriger, alle Daten zu schützen, potenzielle Bedrohungen wie Malware zu erkennen und Kosten und Komplexität zu optimieren.
- Laut einer Studie von Veritas mangelt es den Umfrageteilnehmern an Klarheit über ihre Daten. Im Durchschnitt bestehen diese zu 35 % aus Dark Data, zu 50 % aus redundanten, veralteten oder trivialen (ROT) Daten und nur zu 16 % aus geschäftskritischen Daten.[5]



Herausforderung Nr. 3

Die Kosten können ungezügelt wachsen



Da die ohnehin schon hohen Anforderungen an die Datenspeicherung ständig zunehmen, schießen auch die Kosten in die Höhe.

- Herkömmliche Datenspeicherlösungen optimieren die Nutzung nicht, was dazu führt, dass sich doppelte und nicht benötigte Daten an mehreren Standorten ansammeln.
- Die Kosten für die Datenspeicherung sind in den letzten Jahren stetig gestiegen: laut McKinsey & Co. um 50 % in den letzten 5+ Jahren.[6]
- Durch Deduplizieren und Komprimieren von Daten und deren anschließende Speicherung auf einer günstigeren Speicherebene können Unternehmen im Vergleich zu Cloud-nativen Snapshots Speichereinsparungen von bis zu 99 % erzielen.[7]

Herausforderung Nr. 4

Komplexität ist die neue Norm

Durch die Nutzung verschiedenster Tools, Technologien und Ressourcen entstehen zusätzliche Schichten isolierter IT-Administration und -Verwaltung.

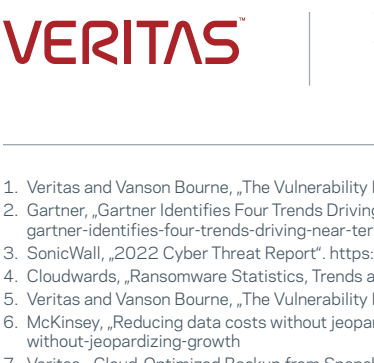
- Cloud-native Tools lassen sich zwar schnell aktivieren, sie können Daten jedoch nicht in Multicloud-Frameworks verwalten, was zu einer höheren Tool-Diversität und einer höheren betrieblichen Komplexität führt.
- Um die Komplexität zu bewältigen, müssen Unternehmen Lösungen einführen, die ein komplexes einheitliches Datenmanagement ermöglichen und optimieren, den Schutz und die Sicherheit der Daten verbessern und eine elastische, skalierbare Cloud-native Architektur unterstützen.

45 %
der Anwendungen sind über mehrere Clouds verteilt

83 %
der Unternehmen mangelt es an den Ressourcen und der Expertise, um sie angemessen zu verwalten[8]

Herausforderung Nr. 5

Die Cloud erfordert immer noch einen hohen manuellen Aufwand



Um häufige und kostspielige manuelle Fehler zu vermeiden, ist Automatisierung unabdingbar. Deren Wert zeigt sich insbesondere in den folgenden entscheidenden Anwendungsfällen:

- Autonome Datenmanagementtechnologie, die Daten automatisch und intelligent schützt und gleichzeitig Konformität, Sicherheit und Kostenoptimierung gewährleistet.
- Künstliche Intelligenz (KI), maschinelles Lernen (ML) und andere Automatisierungs- und Autoskalierungsfunktionen, die eine skalierbare und elastische Cloud-native Architektur unterstützen.
- Appliances, Container und Microservices, die die Fähigkeiten Cloud-nativer Frameworks maximieren.

Das Modell der geteilten Verantwortung sorgt für falsche Annahmen.

Es besteht nach wie vor viel Verwirrung und Unklarheit hinsichtlich des Modells der geteilten Verantwortung zwischen Cloud-Service-Anbietern und ihren Kunden. Theoretisch verstehen zwar die meisten, dass die Anbieter von Cloud-Diensten für die Ausfallsicherheit der Cloud und die Kunden für die Ausfallsicherheit ihrer darin gespeicherten Daten verantwortlich sind. Die praktische Umsetzung kann jedoch vage sein und führt häufig dazu, dass Daten und Anwendungen ungeschützt und angreifbar bleiben.

Mit einer ausgereiften Plattform, die moderne Multicloud-Umgebungen unterstützt, ermöglicht Veritas mehr Kontrolle und Risikosenkung und überschaubarere Kosten. Gleichzeitig wird sichergestellt, dass Sie Ihren Teil im Modell der geteilten Verantwortung erfüllen.

Veritas verändert alles

Veritas bietet Technologie der nächsten Generation, die Datenmanagement, Ausfallsicherheit, Cybersicherheit und Nachhaltigkeit in der Cloud revolutioniert.

Weitere Informationen finden Sie unter ***www.veritas.com/de/de/solution/cloud-data-security***

Tel.: 0800-724 40 75
Theatinerstr. 11, 80333 München

https://www.veritas.com/de/de
Für Kontaktinformationen weltweit besuchen Sie:
veritas.com/de/de/company/contact

1. Veritas and Vanson Bourne, „The Vulnerability Lag". https://www.veritas.com/content/dam/Veritas/docs/reports/GA_ENT_AR_Veritas-Vulnerability-Gap-Report-Global_V1414.pdf
2. Gartner, „Gartner Identifies Four Trends Driving Near-Tern Artificial Intelligence Innovation", 7. September 2021. https://www.gartner.com/en/newsroom/press-releases/2021-09-07-gartner-identifies-four-trends-driving-near-term-artificial-intelligence-innovation
3. SonicWall, „2022 Cyber Threat Report". https://www.sonicwall.com/2022-cyber-threat-report/
4. Cloudwards, „Ransomware Statistics, Trends and Facts for 2022 and Beyond", 22. März 2022. https://www.cloudwards.net/ransomware-statistics/
5. Veritas and Vanson Bourne, „The Vulnerability Lag". https://www.veritas.com/content/dam/Veritas/docs/reports/GA_ENT_AR_Veritas-Vulnerability-Gap-Report-Global_V1414.pdf
6. McKinsey, „Reducing data costs without jeopardizing growth", 31. Juli 2020. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/reducing-data-costs-without-jeopardizing-growth
7. Veritas, „Cloud-Optimized Backup from Snapshot and Autoscaling in NetBackup 10." https://www.veritas.com/content/dam/www/en_us/documents/technical-documents/TB_netbackup_cloud_optimized_backup_snapshot_V1510.pdf
8. Flexera, „2022 State of the Cloud Report". https://info.flexera.com/CM-REPORT-State-of-the-Cloud?lead_source=Website%20Visitor&id=Flexera.com-PR

V1609 09/22