

ZUKUNFTSSICHERE DATENSPEICHERUNG
HEALTHCARE-DATEN
LANGFRISTIG SCHÜTZEN

Steigendes Datenwachstum aus PACS & Co., Ransomware-Schutz, strenge regulatorische Vorgaben und enormer Kostendruck: IT-Abteilungen in Kliniken und Krankenhäusern stehen bei der langfristigen Datenspeicherung vor einer Vielzahl an Herausforderungen und Unsicherheiten.

Dieses Whitepaper gibt einen Überblick, wie Sie eine sichere, flexible und effiziente Speicherung und Archivierung von Gesundheitsdaten gewährleisten können, die den steigenden Anforderungen dauerhaft standhält.

INHALTSVERZEICHNIS

1. HERAUSFORDERUNGEN BEI DER HEALTHCARE-DATENSPEICHERUNG	3
2. DATENWACHSTUM BEWÄLTIGEN.....	5
3. IT-BUDGETS EFFIZIENT NUTZEN	6
4. ZEIT- UND ARBEITSAUFWÄNDE VERRINGERN	7
5. CYBER-ANGRIFFE ABWEHREN	9
6. DATENINTEGRITÄT UND VERFÜGBARKEIT SICHERSTELLEN	11
7. COMPLIANCE & VORSCHRIFTEN EINHALTEN	12
8. KOMPLEXITÄT DER INFRASTRUKTUR REDUZIEREN.....	14
9. ITERNITY HEALTHCARE-LÖSUNGEN.....	15
10. ZUSAMMENFASSUNG	16



ZUKUNFTSSICHERE DATENSPEICHERUNG SO SCHÜTZEN SIE IHRE HEALTHCARE-DATEN

In Kliniken und Krankenhäusern ist die Verfügbarkeit, Sicherheit und Integrität von Gesundheitsdaten entscheidend, um die Patientenversorgung sicherzustellen. Der Einsatz der richtigen Speicherlösung hat nicht nur indirekten Einfluss auf das Patientenwohl, sondern auch auf die Effizienz des Krankenhauses. Während immer modernere Bildgebungsverfahren zu einem rasanten Anstieg der Datenmengen führen, nimmt die IT-Komplexität und Anzahl der Cyber-Angriffe zu. Hinzu kommt der Mangel an IT-Fachkräften und enormer Kostendruck. Die Speicher- und Archiv-Infrastruktur muss mit dieser Entwicklung Schritt halten – oder einen Schritt voraus sein.

1. HERAUSFORDERUNGEN BEI DER HEALTHCARE-DATENSPEICHERUNG

Die Digitalisierung und der technologische Fortschritt versprechen ungeahnte Möglichkeiten für Kliniken und Krankenhäuser, werden jedoch oft durch altbekannte Herausforderungen ausgebremst.

Im Hinblick auf die Datenspeicherung verfolgen IT-Abteilungen das Ziel, mit begrenzten Budgets und Ressourcen langfristige Planungs- und Zukunftssicherheit herzustellen, steigende Datenmengen zu bewältigen und Risiken zu minimieren. Die grundlegenden Herausforderungen bei der Datenspeicherung im Gesundheitswesen sind:



Steigendes Datenwachstum: Bildgebende Verfahren von MRT-, CT-, Ultraschall- und Röntgengeräten, telemedizinische Möglichkeiten, die Digitalisierung der Pathologie und die Einführung der digitalen Patientenakte führen zu einem massiven Datenwachstum.



Eng gestrickte IT-Budgets und langwierige IT-Beschaffung: Fehlende finanzielle Mittel für den IT-Betrieb, kaum Geld für Investitionen, komplexe Beschaffungsprozesse mit vielen Involvierten – Die IT steht vor der Herausforderung, die Kosten und Aufwände für die Datenspeicherung zu senken und gleichzeitig die Effizienz der Infrastruktur zu erhöhen.



IT-Fachkräftemangel: Wachsenden Anforderungen stehen IT-Abteilungen mit Personal- und Zeitmangel gegenüber. Stellenbesetzungsprobleme im IT-Bereich sind branchenweit ein massives Problem - besonders gravierend jedoch im Gesundheitswesen.



Schutz vor Cyber-Angriffen: Kliniken und Krankenhäuser stehen zunehmend im Visier von Cyber-Angriffen. Adäquate Schutzmaßnahmen sind Pflicht, um die Patientenversorgung und den Betrieb nicht zu gefährden.



Schutz der Datenintegrität und Verfügbarkeit: Die Patientengesundheit steht im Fokus. Die Integrität und Verfügbarkeit von kritischen Gesundheitsdaten muss ohne Wenn und Aber gesichert und langfristig geschützt werden.



Einhaltung regulatorischer Vorgaben: Strenge und sich weiterentwickelnde Vorgaben (KRITIS, DSGVO, IT-Sicherheitsgesetz 2.0, NIS2, HIPAA, RöV, ...) sorgen für eine höhere Informationssicherheit und stellen zugleich komplexe Anforderungen an die langfristige Datenarchivierung.



Technologischer Wandel: Der schnelle technologische Fortschritt ohne klare Aussicht, welche Technologien sich in Zukunft durchsetzen werden, erschweren die Planungs- und Investitionssicherheit.



Komplexe Infrastruktur: IT-Abteilungen müssen die Anforderungen verschiedenster Abteilungen umsetzen. Dies führt zur Administration vielfältiger Anwendungen und historisch gewachsener Silo-Architekturen, wodurch die IT-Infrastruktur an Komplexität gewinnt.



Standortsicherung: Kliniken und Krankenhäuser müssen ihre Existenz und Zukunftsfähigkeit sichern – aus Sicht des digitalen Wandels, betriebswirtschaftlichen Gesichtspunkten und unter Berücksichtigung aller Möglichkeiten der IT.

Die Summe der Herausforderungen legt die Messlatte für IT-Verantwortliche in Kliniken und Krankenhäusern sehr hoch. Die folgenden Seiten geben einen Überblick, wie die einzelnen Herausforderungen im Hinblick auf die Archivierung und Speicherung von Gesundheitsdaten zukunftssicher bewältigt werden können.

2. DATENWACHSTUM BEWÄLTIGEN

Die Digitalisierung und Vernetzung in Kliniken und Krankenhäusern schreitet kontinuierlich voran. Die Weiterentwicklung der medizinischen Bildgebungsverfahren, neue Möglichkeiten der Telemedizin und die Einführung der digitalen Patientenakte verbessern nicht nur die Patientenversorgung, sondern sorgen auch für exponentiell steigende Datenmengen.

Ein Großteil des Datenwachstums ist auf medizinische Bilddaten wie CT-Scans, MRTs, EKG-, Ultraschall- und Röntgenaufnahmen zurückzuführen. Dies sind mehrheitlich unstrukturierte Daten, welche z. B. in der Radiologie, Onkologie oder Pathologie erzeugt und in PACS-Applikationen oder Vendor Neutral Archives (VNA) gespeichert werden. Da sich Bildgebungstechnologien kontinuierlich weiterentwickeln und immer höhere Auflösungen bereitstellen, steigen auch die erzeugten Dateigrößen. So verwundert es nicht, dass ein einziges Krankenhaus jährlich dutzende bis hunderte Terabytes oder gar Petabytes an Daten generiert.

Auch der demografische Wandel und die damit verbundene höhere Lebenserwartung der Bevölkerung stellen einen wichtigen Treiber für steigende Datenmengen dar. Werden Menschen älter, steigt auch die Anzahl an Pflegebedürftigen, orthopädischen Verletzungen und chronisch Kranken. Dementsprechend werden telemedizinische Technologien, z. B. für das Monitoring der Patienten zu Hause, verstärkt zum Einsatz kommen, was für umfangreichere digitale Patientenakten sorgt.

Auch Daten aus der Genomforschung, der Einsatz von Wearables, Telekonsilen und Videoaufnahmen in der Chirurgie, Abrechnungs- und Dokumentenmanagement sowie regelmäßige Daten-Backups tragen wesentlich zum Datenwachstum bei. Bedenkt man, dass bestimmte Daten bis zu 30 Jahre aufbewahrt werden müssen, wird schnell klar, dass bei der langfristigen Datenspeicherung dringender Handlungsbedarf geboten ist.



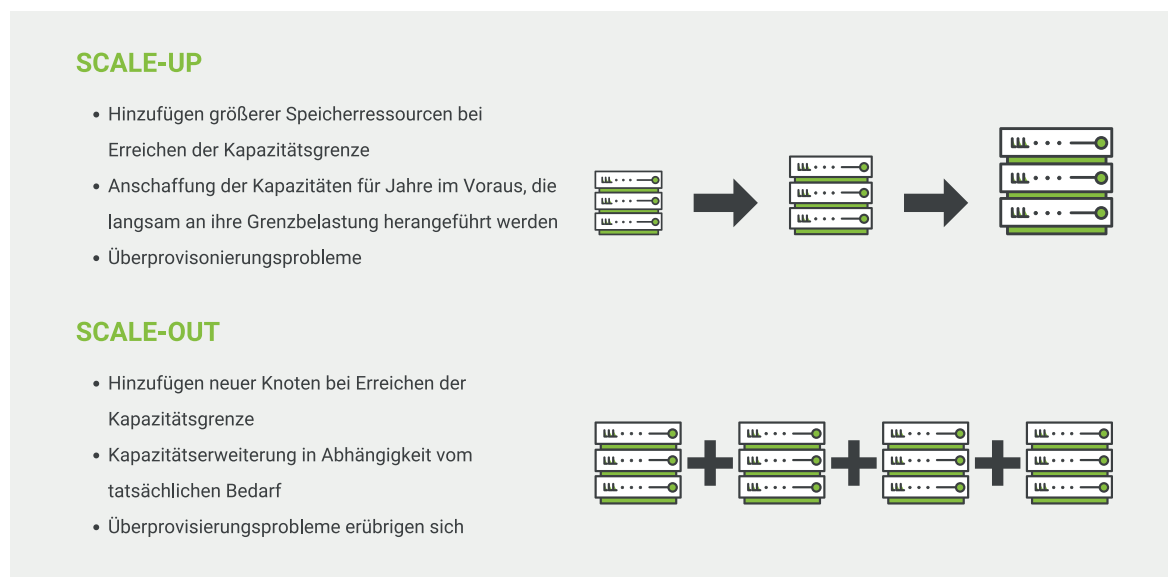
Wie Gesundheitseinrichtungen diese Herausforderung lösen können

Um dem exponentiellen Datenwachstum gerecht zu werden, braucht es hochskalierbare Speicherlösungen, die sich flexibel an den tatsächlichen Bedarf anpassen und erweitern lassen.

Hier empfehlen sich horizontal skalierbare Speicherlösungen (Scale-out). Eine Scale-out Architektur ermöglicht ein einfaches Aufrüsten der Speicherkapazität. Dabei wird die Gesamtleistung beispielsweise von einem Verbund (Cluster) einzelner Knoten (Nodes) erbracht. Wächst der Speicherbedarf, lassen sich zusätzliche Knoten einfach und im laufenden Betrieb hinzufügen. Mit dieser modularen Architektur kann die Gesamtkapazität gemäß dem tatsächlichen Bedarf beliebig und schrittweise ausgebaut werden. Speicherplatz muss nicht für Jahre im Voraus gekauft werden und kostspielige Über- oder Unterdimensionierungen sind hinfällig.

Neben der einfachen Erweiterung der Speicherkapazität bietet eine Scale-out Architektur viele weitere Vorteile, wie z. B. eine flexible Kapazitätsplanung, ein einfaches Speichermanagement, Zeiteinsparungen und Effizienzsteigerungen.

Ein weiterer interessanter Trend, welcher sich durch die gesamte IT-Landschaft zieht, sind „as-a-Service“-Modelle. Bei diesen fallen die Investitionskosten zu Beginn weg und es wird nur bedarfsgerecht die tatsächliche Nutzung und der Service bezahlt. Der Fokus liegt somit auf den Betriebskosten (Opex) und nicht auf den Investitionskosten (Capex). Die Anwendung einer solchen Strategie ermöglicht hohe Flexibilität und Kosteneffizienz und kann heutzutage auch im eigenen Rechenzentrum aufgebaut werden – beispielsweise mit HPE GreenLake oder Fujitsu uSCALE – wodurch die Vorteile von Cloud- und On-Premises-Datensicherung verknüpft werden.



3. IT-BUDGETS EFFIZIENT NUTZEN

Mit den zunehmenden Datenmengen steigen auch die Kosten und Aufwände diese Daten zu verwalten. Angesichts der Silo-Architekturen, die noch in vielen Gesundheitseinrichtungen vorherrschen, fehlenden IT-Fachkräften und eng gestrickten IT-Budgets hat die Frage nach Kosteneinsparungen und der Steigerung der IT-Effizienz höchste Priorität.

Um dieses Spannungsfeld zu überwinden, sollten sich Gesundheitseinrichtungen auf die Optimierung der IT-Speicherinfrastruktur sowie auf die Reduktion der Gesamtkosten und administrativen Aufwände fokussieren.



Wie Gesundheitseinrichtungen diese Herausforderung lösen können

Der Bedarf an effizienten und kostengünstigen Archivspeicherlösungen ist im Gesundheitswesen besonders hoch. Ziele wie Kosteneffizienz, Flexibilität und Skalierbarkeit lassen sich mit einer software-basierten Speicherinfrastruktur erreichen. Dieses Modell ermöglicht ein einheitliches, zentrales Speichermanagement aller Archiv-, Backup-, Forschungs- und administrativen Daten über die

gesamte IT-Umgebung hinweg. Dabei werden die Hardware-Komponenten zu einem einzigen „Pool“ zusammengefasst, der sich wie eine homogene Speicherumgebung verhält. Durch diese Konsolidierung lassen sich der Administrationsaufwand für die IT-Mitarbeiter und die Arbeitskosten deutlich reduzieren.

Aufgrund der Unabhängigkeit von bestimmter Hardware oder Technologien können Gesundheitseinrichtungen gängige, kostengünstige Standard-x86-Server einsetzen und damit Anschaffungs- und Lizenzkosten sparen.

Eine software-basierte Scale-out Architektur bietet im Vergleich zu proprietären Lösungen ein einfaches Finanzierungsmodell (Pay-as-you-grow), da Speicherplatz erst bei tatsächlichem Bedarf angeschafft werden muss, ohne bereits im Vorfeld Kapitalkosten für überdimensionierte Kapazitäten zu verursachen.

Laufende Betriebskosten können durch Managed Services gesenkt werden. Dabei wird die Betreuung des Speichersystems an einen Service Provider oder den Hersteller ausgelagert. Für die interne IT fällt damit so gut wie kein Zeit- und Personalaufwand an, wodurch sich die Administrationskosten deutlich senken lassen. Die Kosten für die Managed Services sind in der Regel transparent und planbar. Zusätzliche Einsparpotenziale liefern beispielsweise die gewonnenen Effizienzzuwächse und der Wegfall von Kosten für die Suche und Einstellung neuer Mitarbeiter, den Aufbau von speziellem Anwenderwissen und Schulungen.

4. ZEIT- UND ARBEITSAUFWÄNDE VERRINGERN

Fehlendes IT-Fachpersonal stellt für viele Kliniken und Krankenhäuser ein massives Problem dar. Die meisten Einrichtungen konkurrieren mit anderen Branchen, die oftmals attraktivere Rahmenbedingungen für IT-Spezialisten bieten können. So kämpfen laut einer Studie des Deutschen Krankenhausinstituts e.V. (DKI) und der BDO AG Wirtschaftsprüfungsgesellschaft 47% der befragten deutschen Krankenhäuser mit Stellenbesetzungsproblemen im IT-Bereich.¹

Da in Zukunft nur bedingt mit einer Verbesserung der Personalsituation zu rechnen ist, müssen Gesundheitseinrichtungen dieser Herausforderung mit aufwandsreduzierenden Maßnahmen, Externalisierung und Automatisierung begegnen. So kann die knappe „Ressource Mensch“ für strategisch wichtige Tätigkeiten eingesetzt und die Produktivität der IT-Mitarbeiter erhöht werden.



Wie Gesundheitseinrichtungen diese Herausforderung lösen können

Managed Services können hier eine effektive Lösung bieten und finden in Gesundheitswesen immer mehr Anklang. Mit diesem Konzept übernimmt ein externer Dienstleister das Management des Speichersystems; dazu gehört unter anderem die Administration, das Update- und Patchmanagement, das Monitoring, Trend-Berechnungen der Kapazität, Fehlerbehebung und die Wartung des Systems.

Die Vorteile liegen auf der Hand: Die Auslagerung der täglichen Basisaufgaben schafft der internen IT Freiraum für Kernaufgaben, strategische Themen und die Weiterentwicklung der IT. Auch das Problem des Fachkräftemangels lässt sich Managed Services entschärfen – ganz einfach, weil kein eigenes

¹ „Das digitale Krankenhaus“, Deutsches Krankenhausinstitut e.V. (DKI) & BDO AG Wirtschaftsprüfungsgesellschaft, 2019

Personal für das Speichersystem bereitgestellt werden muss und der Dienstleister das entsprechende Know-how liefert.



137.000 offene Stellen für IT-Fachkräfte



Durchschnittlich vergehen 7,1 Monate bis eine IT-Stelle besetzt werden kann.



70% der Unternehmen erwarten, dass sich der IT-Fachkräftemangel verschärfen wird.

Quelle für die Inhalte: Bitkom, „Trotz Krieg und Krisen: In Deutschland fehlen 137.000 IT-Fachkräfte“, 2022

Darüber hinaus bieten Managed Services eine höhere IT-Sicherheit und -Stabilität. So kann sich eine Einrichtung stets darauf verlassen, dass immer die neuesten Updates und kritischen Sicherheitspatches installiert sind. Schlupflöcher, die findige Cyberkriminelle aufspüren könnten, lassen sich damit wirkungsvoll schließen.

Zusammengefasst können Kliniken und Krankenhäuser mithilfe externer, spezialisierter Experten die IT-Effizienz erhöhen und gewährleisten, dass Speicherabläufe langfristig gesichert sind.

Werden Managed Services dann noch mit einer klinikweiten Zentralisierung der Datenspeicherung gepaart, lassen

sich weitere Synergieeffekte in Bezug auf die Aufwände und Kosten nutzen. Ein sinnvolles Szenario ist beispielsweise, dass Archiv-, Forschungs- und Backup-Daten auf einer einzigen zentralen Plattform gespeichert und vom Dienstleister betreut werden, was die IT-Komplexität um einen beachtlichen Anteil senkt.

Wie können Gesundheitseinrichtungen mit Managed Services die Aufwände bei der langfristigen Datenspeicherung senken?

Leistungen im Rahmen von Managed Services	Vorteile für Kliniken und Krankenhäuser
■ Einfache Installation und Bereitstellung des Speicher- und Archivsystems durch den Service Provider ■ Einrichtung von Konfigurationen	■ Schnell verfügbares Speichersystem ■ Schonung der internen personellen Ressourcen & Zeitgewinn für Kernaufgaben ■ Präzise und effiziente Umsetzung durch gebündeltes externes Know-how ■ Kein Aufbau von multidisziplinären internen Teams für die Implementierung
■ Übernahme der Basisaufgaben wie z. B. Administration, Fehlerbehebung, Update-Management sowie Wartung ■ Bereitstellung von Expertenwissen	■ Mehr Zeit für Kernthemen und die strategische Weiterentwicklung der IT ■ Höhere IT-Effizienz durch externes Know-how ■ Entschärfung des IT-Fachkräftemangels ■ Keine Schulungen und Aufbau von Fachwissen für die eigenen Mitarbeiter nötig
■ Integriertes 24/7 Monitoring des gesamten Set-ups (Speichersoftware, -hardware, Netzwerk-Verbindungen und Kapazität) ■ Aktive Überwachung mithilfe von Alarm- und Benachrichtigungsfunktionen ■ Überwachung und Behebung von Hardwarefehlern	■ Jederzeitige Sicherstellung der Integrität, Sicherheit und Verfügbarkeit der Daten

Leistungen im Rahmen von Managed Services	Vorteile für Kliniken und Krankenhäuser
■ Kundendashboard zur Kontrolle der wichtigsten Kennzahlen	■ Jederzeitige einfache Überwachung des Speichersystems mit Informationen über den gesamten Status und die Kapazität
■ Überwachung und Schutz der Datenintegrität	■ Geschützte Datenintegrität und automatische Behebung von Fehlern
■ Überwachung und Trend-Berechnung der Kapazität ■ Kapazitätserweiterung während des Betriebs möglich	■ Unterstützung beim Kapazitätsmanagement ■ Minimierte Downtimes
■ Planung und Einspielung von Feature- und Patch-Releases sowie Updates des Betriebssystems	■ Kein Wartungsaufwand ■ Deutlich schnelleres Einspielen von Updates und Patches im Vergleich zur internen Umsetzung ■ Neuester Stand der Technik ■ Weniger Sicherheitslücken, die von Cyberkriminellen ausgenutzt werden können

5. CYBER-ANGRIFFE ABWEHREN

Die Gewährleistung der IT-Sicherheit ist aktuell eine der größten Herausforderung für viele Kliniken und Krankenhäuser und hat sich in den letzten Jahren dramatisch verschärft. Cyberkriminelle spekulieren darauf, dass bei kritischen Infrastrukturen aufgrund der empfindlichen Unterbrechung des Betriebs ein besonders hoher Druck herrscht und deshalb eine höhere Bereitschaft zur Zahlung von Lösegeldern besteht.

Dabei können Manipulationen und Veränderung von Daten durch Unberechtigte weitreichende Konsequenzen haben, da sie einen direkten Einfluss auf das Patientenwohl nehmen können. Angesichts der digitalen Patientenakte sind verschärfte Schutzmechanismen gegen Cyber-Angriffe noch wichtiger. Wenn alle Patientendaten zentral gespeichert werden, reicht eine einzige erfolgreiche Attacke, um hochsensible Daten zu manipulieren oder zu stehlen.



Wie Gesundheitseinrichtungen diese Herausforderung lösen können

Die beste Verteidigung gegen Cyber-Angriffe sind saubere, nicht kompromittierte Backup-Daten. Da diese inzwischen selbst im Visier der Angreifer stehen, müssen diese besser geschützt werden. Neben der Backup-Software müssen IT-Abteilungen deshalb auch die Speicherinfrastruktur berücksichtigen. Konkret geht es darum, Backups auf Storage-Ebene vor Verschlüsselung und Löschung zu schützen, eine schnelle Wiederherstellung zu garantieren und die IT-Angriffsfläche zu minimieren.

Zu den derzeit effektivsten Waffen gegen Ransomware-Angriffe zählt die unveränderliche Datenspeicherung (**Immutability**). Dabei werden Backups und Archivdaten für einen fest definierten Zeitraum mit einer WORM-Versiegelung versehen und können weder von der Ransomware noch von böswilligen Mitarbeitern geändert, manipuliert oder gelöscht werden. Im Fall eines Angriffs steht somit immer eine saubere Datenkopie bereit, die im Rahmen der Disaster Recovery wiederhergestellt werden

kann. Hohe Kosten durch Ausfallzeiten und fehlgeschlagene Wiederherstellungsversuche lassen sich dadurch reduzieren.



Unveränderliche Datenspeicherung zum Schutz vor Änderungen, Verschlüsselung und Löschen durch Ransomware und Insider Attacks.

Die unveränderliche Datenspeicherung kann durch WORM Storage, was bereits in der revisionssicheren Archivierung genutzt wird, oder S3 Object Lock umgesetzt werden. S3 Object Lock wird von allen großen Backup-Softwareherstellern unterstützt, ermöglicht granulare WORM-Richtlinien und fügt einen zusätzlichen Schutz gegen Objektänderungen und -löschung hinzu. Das ist nicht nur in der Cloud möglich, sondern auch S3-kompatibel im eigenen Rechenzentrum.

Damit bietet die unveränderliche Datenspeicherung ein ähnliches Sicherheitsniveau wie Air-Gaps, welche beispielsweise mit Tapes realisiert werden können. Der große Nachteil von Air-Gaps liegt jedoch darin, dass

Mitarbeiter während des laufenden Betriebs nicht lesend auf Daten zugreifen können, die Wartung der Systeme zeitaufwändig ist und die Wiederherstellung sehr lange dauern kann. Unveränderliche Datenspeicherung, welche auf On-Premises-Systemen realisiert wird, liefert hier eine weitaus praktikablere Storage-Methode mit 24/7-Datenzugriff.

Auch im Vergleich zu Public Cloud Storages liefern On-Premises-Speicherlösungen einschlägige Vorteile. Die Hoheit über die Daten bleibt im Krankenhaus, während gleichzeitig eine unbegrenzte Skalierbarkeit, hohe Performance und Kosteneffizienz erreicht werden kann. Außerdem wollen oder dürfen viele Gesundheitseinrichtungen bestimmte Daten nicht in die Cloud auslagern und setzen daher auf die datenschutzrechtlich sicherere On-Premises-Variante.

Neben dem Schutz der Backups und Archivdaten auf Speicherebene sollten IT-Abteilungen auch die IT-Angriffsflächen minimieren. Um Daten vor Social Engineering Attacks, menschlichen Fehlern oder böswilligen Mitarbeitern zu schützen, helfen geschlossene software-basierte Speichersysteme – insbesondere auf Basis von gehärteten Linux-Systemen – die keinerlei Benutzerzugriff auf Seite der Anwender bieten. Statt der Inhouse-Betreuung wird das Speichersystem dabei im Rahmen von Managed Services von einem externen Dienstleister gemanagt. Sicherheitsrisiken, die auf dem Faktor Mensch gründen, lassen sich so minimieren. Auch das Update- und Patch-Management übernimmt meist der Managed Services Anbieter und sorgt so dafür, dass das Speichersystem auf dem aktuellen Stand ist

und Sicherheitslücken geschlossen bleiben. Ein weiterer Faktor, der nicht zu unterschätzen ist, stellt die steigende IT-Komplexität dar. Je mehr IT-Systeme eingesetzt werden, umso höher das Risiko unentdeckter Schlupflöcher. Durch die Konsolidierung mehrerer Speicherquellen in einer zentralen Storage-Plattform lassen sich nicht nur Synergien in Bezug auf Kosten und Aufwände erzielen, sondern auch Sicherheitslücken schließen.



Erfahren Sie im Backup-Guide [„So schützen Sie Ihre Backups vor Ransomware-Angriffen“](#) mehr über verlässliche und effektive Schutzmaßnahmen vor hochprofessioneller Ransomware.

Wichtig ist auch die 3-2-1-1-0 Backup-Regel: Mindestens drei Sicherungskopien der Daten sollten erstellt werden. Diese Kopien sollten auf zwei verschiedenen Medien gespeichert und eine Kopie an einem externen Standort aufbewahrt werden. Eine Kopie davon sollte offline oder unveränderlich gespeichert werden. Zu guter Letzt sollte die IT sicherstellen, dass die Backups fehlerfrei sind.

6. DATENINTEGRITÄT UND VERFÜGBARKEIT SICHERSTELLEN

Im Gesundheitswesen steht das Patientenwohl im Fokus. Eine Beeinträchtigung der Datenintegrität oder -verfügbarkeit kann nicht nur einen Reputations- und Vertrauensverlust einer Gesundheitseinrichtung bewirken, sondern auch rechtliche Konsequenzen nach sich ziehen und vor allem einen direkten Einfluss auf die Patientenversorgung nehmen.

Dabei gibt es zahllose Beispiele von Daten, die für die Patientenversorgung ausschlaggebend sind. Das wohl griffigste Beispiel ist die digitale Patientenakte. Diese Akte sammelt alle relevanten Informationen eines Patienten – z. B. über Diagnosen, Anamnese, Befunde, Behandlungen oder Medikationen. Liegen diese Daten nicht in korrekter oder vollständiger Form vor oder sind sie im Ernstfall nicht verfügbar, kann dies ein Risiko für die Behandlung eines Patienten darstellen. Deshalb ist es von entscheidender Bedeutung, die Integrität von Gesundheitsdaten während ihrer Aufbewahrungsfrist zu sichern und eine unterbrechungsfreie Verfügbarkeit der Daten zu garantieren.



Wie Gesundheitseinrichtungen diese Herausforderung lösen können

Software-basierte Speicherlösungen ermöglichen Gesundheitseinrichtungen die Integrität sensibler Gesundheits- und Geschäftsdaten dauerhaft zu schützen sowie Beeinträchtigungen und Ausfälle der Datenverfügbarkeit im Klinikbetrieb zu minimieren.

Die WORM Speicherung (Write Once Read Many) stellt einen besonderen Fall der Archivierung dar, mit dem die Unveränderlichkeit der Archivdaten sichergestellt wird. Diese Technologie sorgt dafür, dass Daten während der Aufbewahrungsdauer nicht mehr verändert, gelöscht oder manipuliert, sondern nur noch gelesen werden können. WORM Speicherung ist in vielen Ländern für steuerrelevante Geschäftsunterlagen oder Daten in regulierten Branchen, wie dem Gesundheitswesen, gesetzlich vorgeschrieben.

Ein effektiver Weg die Datenintegrität darüber hinaus zu sichern, stellen Datenvalidierungen und Fehlerprüfungen dar. Dabei wird die Datenkonsistenz mithilfe von Prüfsummen validiert, indem jeder Datei ein Hash-Wert beigelegt wird, der veränderte oder manipulierte Daten sichtbar macht. Einen Schritt weiter geht die automatische Reparatur fehlerhafter Daten, z. B. mit Self-Healing. Dabei werden Daten auf mehreren Zielen gespeichert (Replikation) und kontinuierlich geprüft. Die Selbstheilungsfunktion erkennt beschädigte Objekte und ersetzt diese automatisch mit den validen replizierten Daten. Dadurch haben Anwender kaum Berührungspunkte mit Datenintegritätsschutz und können sich dauerhaft auf das Archivsystem verlassen.

Um im Katastrophenfall eine korrekte Version der Daten wiederherstellen zu können, sind auch regelmäßige Backups elementar. Doch auch bei Backups besteht inzwischen die verstärkte Gefahr

durch Ransomware Angriffe, weshalb diese auch auf Speicherebene eines besonderen Schutzes bedürfen. Sozusagen die sichere Aufbewahrung der Sicherungskopie – das klingt logisch, ist in vielen Kliniken jedoch noch eine dringende Baustelle.

Eine Replikation von Daten in physisch getrennte Systeme oder verschiedene Standorte sorgt für die Verfügbarkeit kritischer Daten und bildet die Basis für eine Disaster Recovery Strategie. Bei der synchronen Replikation werden aktuelle Datenbestände auf mehreren Speicherplätzen (Cluster-Knoten) gleichzeitig vorgehalten. Folglich erhält die vorgelagerte Anwendung, die diese Daten auf das Speichersystem schreibt, nur dann die Information, dass ein Vorgang erfolgreich abgeschlossen wurde, wenn dieser auf mehreren Cluster-Knoten durchgeführt wurde. Dies gewährleistet, dass alle Kopien immer auf dem neuesten Stand sind und bietet einen hohen Schutz vor Datenverlust.

Wenn jedoch die Entfernung zwischen den Clusterknoten sehr groß ist – wie bei interkontinentalen Distanzen – werden Dateioperationen langsamer. Hier kommt die asynchrone Replikation ins Spiel. Wenn die Latenzzeit zwischen den Clusterknoten hoch ist, werden die Daten zuerst auf dem schnellsten Element im Cluster vorgehalten und die Replikation auf den anderen langsamen Speicherelementen/ Clusterknoten erfolgt im Hintergrund. Auf diese Weise ist die einfache Ausdehnung eines einzelnen Clusters auf weit entfernte Rechenzentren möglich, auch für interkontinentale Distanzen (WAN). Zusätzlicher Vorteil ist hierbei die Sicherung kritischer Daten im Fall eines Standortausfalls, von regionalen Katastrophen oder menschlichen Fehlern, da immer mindestens ein Datensatz an einem entfernten Standort aufbewahrt wird.

7. COMPLIANCE & VORSCHRIFTEN EINHALTEN

In Bezug auf den Datenschutz und die Archivierungspflichten zählt das Gesundheitswesen zu den am strengsten regulierten Branchen. Vorschriften wie die DSGVO, das IT-Sicherheitsgesetz 2.0, NIS2, die Röntgenverordnung, HIPAA oder das eHealth-Gesetz regeln den Umgang, die Verarbeitung und den Schutz der Daten sowie die Aufbewahrungspflichten und -fristen. Da die Ausgestaltung der Vorgaben ständigen Änderungen unterliegt, haben Kliniken bei der Umsetzung mit einer enormen Komplexität und Unsicherheit zu kämpfen.

Klinische Unterlagen wie beispielsweise Arztbriefe, Krankenhausberichte, Aufzeichnungen und Aufnahmen aus der Röntgen- und Strahlendiagnostik, Diagnosen oder Befunde umfassen hochsensible personenbezogene Daten. Daher verwundert es nicht, dass diese Daten einem besonderen Schutz unterliegen. So gilt für ärztliche Dokumentationen und Unterlagen in der Regel eine 10-jährige Aufbewahrungsfrist. Für bestimmte Daten, wie z. B. Aufzeichnungen zur Röntgenbehandlung oder Dokumente über die Anwendung von Blutprodukten, gelten sogar Zeiträume von 30 Jahren. Während dieser Aufbewahrungsfristen müssen die Daten rechtskonform archiviert und nach Ablauf der Aufbewahrungs- bzw. Verjährungsfrist gelöscht werden.

Am 7. Mai 2021 trat das IT-Sicherheitsgesetz 2.0 in Kraft. Bundesrat und Bundestag haben damit ein dringendes Upgrade der Informationssicherheit vollzogen. Mit der Neuauflage des Gesetzes gehen erweiterte Pflichten für einen größeren KRITIS-Betreiberkreis einher. Unter anderem wurden die Vorgaben für die Cyber-Sicherheit verschärft. So gehören Systeme mit Angriffserkennung nun zu

den verpflichtenden technischen und organisatorischen Sicherheitsmaßnahmen. Darüber hinaus sind KRITIS-Betreiber dazu verpflichtet, ihre informationstechnischen Systeme auf den neusten Stand der Technik zu bringen, um Störungen zu vermeiden. Zu den weiteren Änderungen zählen verschärfte Melde- und Registrierungspflichten bei Störungen, eine Erhöhung der Bußgelder bei Verstößen und eine Stärkung der Kompetenzen des BSI (Bundesamt für Sicherheit in der Informationstechnik) als Cyber-Sicherheitsbehörde.

Was zählt zu den kritischen Infrastrukturen (KRITIS)?

Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Gemäß der BSI-KritisV zählen Kliniken und Krankenhäuser ab 30.000 stationären Behandlungsfällen pro Jahr als kritische Infrastruktur. KRITIS-Betreiber gemäß den definierten Schwellwerten fallen unter die Vorgaben des IT-Sicherheitsgesetzes 2.0 und erben zusätzlich die Vorgaben des NIS2.

Das Whitepaper „[Rechtliche Anforderungen an die Datenarchivierung in Deutschland](#)“ gibt einen Überblick, welche Anforderungen eine Archivspeicherlösung erfüllen muss, um die gesetzlichen Regelungen des IT Sicherheitsgesetzes 2.0, des NIS2 sowie der DSGVO und GoBD umzusetzen.

Die am 16.01.2023 in Kraft getretene EU-Richtlinie Network and Information Systems Directive 2 (NIS2) hat zum Ziel, die Widerstandsfähigkeit von Netz- und Informationssystemen in der EU gegenüber Cyber-Bedrohungen noch weiter zu erhöhen. NIS2 gilt für alle Unternehmen und Einrichtungen aus 18 definierten Sektoren (u.a. Gesundheitswesen), die mehr als 50 Beschäftigte unterhalten oder einen Jahresumsatz von mehr als 10 Mio Euro erwirtschaften. Somit fallen alle deutschen Krankenhäuser und nahezu alle MVZ unter die Vorgaben des NIS2.

Das IT-Sicherheitsgesetz 2.0 erfüllt bereits einen Großteil der Vorgaben der NIS2-Richtlinie. Zu den verschärften Regelungen, die die Datenarchivierung betreffen, gehören strengere Anforderungen an das Daten- und Zugriffsmanagement.

Die Neuerungen der NIS2 müssen bis zum 17.10.2024 in nationales Recht umgesetzt werden. In Deutschland werden die erweiterten IT-Sicherheitsvorgaben der EU unter anderem im NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG, auch „IT-Sicherheitsgesetz 3.0“) aufgegriffen.

Auszug der gesetzlichen Aufbewahrungsfristen

Daten	Aufbewahrungsfrist	Gesetzliche Grundlage
Abrechnungsunterlagen	Bis zu 10 Jahre	§ 147 Abs. 3 Abgabenordnung
Arztbriefe und Krankenhausberichte	10 Jahre	§ 10 Abs. 3 Berufsordnung, § 630f Abs. 3 BGB, § 57 Abs. 2 BMV-Ä
Ärztliche Behandlungsunterlagen	10 Jahre	§ 10 Abs. 3 Berufsordnung, § 630f, Abs. 3 BGB, § 57 Abs. 2 BMV-Ä

Befunde	10 Jahre	§ 10 Abs. 3 Berufsordnung, § 630f, Abs. 3 BGB, § 57 Abs. 2 BMV-Ä
EEG/EKG-Streifen	10 Jahre	§ 10 Abs. 3 Berufsordnung, § 630f, Abs. 3 BGB, § 57 Abs. 2 BMV-Ä
Röntgen-/Strahlendiagnostik (Röntgenaufnahmen, ärztliche Aufzeichnungen)	10 Jahre	§ 28 Abs. 3 RöV, § 85 Abs. 3 StrlSchV
Röntgen-/Strahlenbehandlung (Aufzeichnungen, Berechnungen)	30 Jahre	§ 28 Abs. 3 RöV § 42 Abs. 1, § 85 Abs. 3 StrlSchV
Dokumentation über die Anwendung von Blutprodukten und gentechnisch hergestellten Plasmaproteinen zur Behandlung von Hämostase Störungen	30 Jahre	§ 14 Abs. 3 Transfusionsgesetz



Wie Gesundheitseinrichtungen diese Herausforderung lösen können

Die meisten Regelungen wie die DSGVO, das IT-Sicherheitsgesetz 2.0, NIS2, GoBD oder HIPAA stellen ähnliche Anforderungen an die Datenspeicherung. Generell geht es darum, umfassende Maßnahmen zu implementieren, die dafür sorgen, dass Daten während ihres gesamten Lebenszyklus vor Beschädigung, Änderung, Manipulation, Verlust oder Löschung geschützt sind und die Sicherheit von IT-Systemen erhöht wird. Dies gilt für Archiv-, Backup- und bestimmte administrative Daten.

WORM-Datenspeicherung, Retention Management, Verschlüsselung und automatische Datenintegritätsprüfungen sind unerlässlich. Darüber hinaus muss sichergestellt werden, dass notwendige Maßnahmen ergriffen werden, um den Zugriff auf IT-Systeme und Daten zu kontrollieren und nachvollziehbar zu protokollieren. NIS2 legt zudem Anforderungen an die Authentifizierung und Autorisierung von Benutzern fest, um sicherzustellen, dass nur autorisierte Benutzer auf Daten zugreifen können.

8. KOMPLEXITÄT DER INFRASTRUKTUR REDUZIEREN

Die Healthcare-IT hat sich in den letzten Jahrzehnten enorm weiterentwickelt. Kliniken und Krankenhäuser haben seither signifikante Investitionen in Software und die IT-Infrastruktur getätigt. So sind selbst in einem mittelgroßen Krankenhaus hunderte IT-Applikationen im Einsatz. Dazu gehören z. B. PACS, KIS, RIS, ECM, DMS, Finanz- oder HR-Systeme, um nur einige zu nennen.

Nichtsdestotrotz ist die IT-Infrastruktur in vielen Kliniken und Krankenhäusern teilweise veraltet und intern wie extern zu wenig vernetzt. Behandlungs- und verwaltungsbezogene Daten werden oft in dedizierten Silos gespeichert, welche historisch gewachsen sind und die IT-Komplexität immens erhöhen. Angesichts der heutigen Anwendungsvielfalt sind diese Silo-Architekturen weder wirtschaftlich noch zweckmäßig. Da die Systeme getrennt voneinander verwaltet werden müssen, entsteht ein hoher Administrationsaufwand und damit steigende Kosten.

Die Daten aus den unterschiedlichen Anwendungen haben zudem eigene Speicheranforderungen und Abhängigkeiten. So werden in PACS-Anwendungen medizinische Bilddaten gespeichert – eine flexible Skalierbarkeit ist hier von großer Bedeutung. Bei der Archivierung von Rechnungen hingegen liegt das Augenmerk auf gesetzlichen Aufbewahrungsfristen und Revisionssicherheit. Zu guter Letzt sollten die redundanten Ausgaben für Support- und Wartungsverträge vieler einzelner Lösungsanbieter nicht unbeachtet bleiben.



Wie Gesundheitseinrichtungen diese Herausforderung lösen können

Um die Komplexität der IT-Infrastruktur mit Hinblick auf die Datenspeicherung zu verringern, gilt es, die einzelnen Speicherkomponenten zu konsolidieren und zentralisieren. Ein software-basierter Ansatz ermöglicht ein einheitliches Management über die gesamte Healthcare-Speichenumgebung hinweg – sowohl für Archiv-, Forschungs- und Backup-Daten. Sämtliche Archivierungsfunktionen werden damit gebündelt zur Verfügung gestellt. Das aufwändige Verwalten vieler einzelner Silo-Lösungen erübrigt sich und durch die Trennung von Software und Hardware entstehen keine Abhängigkeiten von bestimmten Herstellern und Technologien.

Für Kliniken ist es ausschlaggebend mit technologischen Weiterentwicklungen Schritt zu halten und künftigen Änderungen – z. B. steigende Datenmengen, Hardware-Innovationen oder Wechsel von Anwendungen – dauerhaft standzuhalten. Aufgrund des technologischen Fortschritts ist jedoch unklar, welche Technologie sich in der Zukunft durchsetzen wird. Hier bietet eine software-basierte Architektur maximale Flexibilität, da aufgrund der Hardware-Unabhängigkeit beliebige Hersteller, Technologien und Hardware eingesetzt werden können. So können beispielsweise traditionelle Festplattenspeicher, Cloud-Speicher oder Hybridlösungen je nach Anforderung flexibel miteinander kombiniert werden.

Um die Anbindung verschiedener Applikationen auf der einen Seite (z. B. Backup-Software wie Veeam oder Commvault, PACS, KIS, ECM, E-Mail) und verschiedenen Speichersystemen auf der anderen Seite zu vereinfachen, sind offene Lösungen gefragt. Dies wird durch offene Schnittstellen und gegenseitige Validierungen ermöglicht und erlaubt eine saubere Integration in die IT-Infrastruktur sowie ein nahtloses Zusammenspiel mit bestehenden oder künftigen Healthcare-Anwendungen. Optimalerweise lassen sich File- und Object Storage in einer Lösung vereinen, z. B. durch die Unterstützung von NFS, SMB und S3 als Schnittstellen.

Wie in den vorangegangenen Kapiteln aufgezeigt, können auch Managed Services einen erheblichen Beitrag zur Senkung der IT-Komplexität und Aufwände beitragen.

9. ITERNITY HEALTHCARE-LÖSUNGEN

Die Speicher- und Archivlösungen von iTernity schützen Healthcare-Daten vor Beschädigung, Verlust, Löschung und Änderung. Kliniken und Krankenhäuser können damit komplexe Compliance-Anforderungen erfüllen, ihr Datenwachstum bewältigen und gleichzeitig ihre Gesamtkosten und IT-Aufwände senken.

Die software-basierten Speicherlösungen bieten dank Hardwareunabhängigkeit größtmögliche

Flexibilität, reduzieren die Infrastruktur-Komplexität und schützen langfristig IT-Investitionen. Damit gestalten Kliniken und Krankenhäuser ihre Langezeitspeicherung und Archivierung zukunftssicher.

- **Archiv-Middleware iCAS:** iCAS ist eine Middleware für Retention Management und revisionssichere WORM-Archivierung. Die Software passt sich an die bestehende IT-Infrastruktur in Kliniken und Krankenhäuser an und ergänzt diese um Compliance, Datenintegritätsschutz und langfristige Verfügbarkeit.
- **Scale-out Plattform iCAS FS:** iCAS FS ist eine skalierbare Speicherplattform und ermöglicht zukunftssichere Healthcare-Datenspeicherung und Compliance bei geringen Gesamtkosten. Dank Managed Storage und integriertem Monitoring können IT-Aufwände und Risiken minimiert werden. Die software-basierte Speicherplattform ermöglicht Gesundheitseinrichtungen, mit geringen Datenmengen zu starten und das Speichersystem schrittweise und unbegrenzt zu erweitern. iCAS FS kann für die revisionssichere Archivierung, als sicheres Backup-Speicherziel sowie zur Entlastung der Primärspeicher eingesetzt werden.

Eine Vielzahl an Healthcare Lösungen wurde auf die reibungslose Zusammenarbeit mit iTernity getestet und validiert, u. a. Lösungen von Allgeier Medial IT, Change Healthcare, Dedalus Healthcare, GE Healthcare, Philips Healthcare, Quest Diagnostics, Sectra und Visus, u.v.m. iCAS und iCAS FS wurden außerdem durch die KPMG auf DSGVO-, GoBD- und GeBüV-Compliance geprüft und zertifiziert.

10. ZUSAMMENFASSUNG

Intelligente Speicher- und Archivierungslösungen bilden das Fundament, um die vielfältigen Herausforderungen von Kliniken und Krankenhäusern langfristig zu lösen. Während software-basierte Scale-out Architekturen die Speicherkapazitäten für stetig wachsende Datenvolumen bereitstellen, sorgen Automatisierung und Managed Services für eine Reduktion der IT-Komplexität und des Verwaltungsaufwands. So können Kliniken mit steigenden Anforderungen flexibel wachsen und gleichzeitig ihre Effizienz erhöhen.

Im Gesundheitswesen sind die Gewährleistung der Patientenversorgung und der Schutz von Patientendaten das zentrale Ziel. Die Datenintegrität und -verfügbarkeit lassen sich mit verschiedenen Schutzmaßnahmen sicherstellen. Die Auswirkungen durch Systemausfälle oder korrumpierte Daten können damit auf ein Minimum reduziert werden. Auch in Bezug auf Cyber-Angriffe bieten moderne Archivierungs- und Speicherlösungen einen wichtigen Schutz. Durch Sicherstellung der Unveränderlichkeit von Daten und begrenzte Zugriffspunkte wird die Angriffsfläche für Ransomware minimiert.

Um die langfristige Wirtschaftlichkeit sicherzustellen, empfehlen sich software-basierte Archiv- und Speichersysteme, die auf Standard-x86-Servern aufbauen. Aufgrund der Hardwareunabhängigkeit kann die zugrunde liegende Speicherhardware frei gewählt und flexibel angepasst werden. Das verschafft Kliniken und Krankenhäusern die nötige Agilität, um mit den steigenden IT-Anforderungen und dem technologischen Fortschritt Schritt zu halten. Zu guter Letzt ermöglicht die Summe aus einer software-basierten Speicherarchitektur, Scale-out Storage, Managed Services und Automatisierung eine deutliche Reduzierung der IT-Gesamtkosten.

LESEN SIE MEHR

- Erfahren Sie in zahlreichen [Referenzstories](#), wie Kliniken und Krankenhäuser in der Praxis von unserem software-basierten Ansatz profitieren
- Sehen Sie im [Video](#), wie das Städtische Klinikum Karlsruhe seine Datenarchivierung modernisiert
- [ESG Kostenvergleich](#): Wie Kliniken und Krankenhäuser bei der langfristigen Datenspeicherung 53% Gesamtkosten und 61% Verwaltungsaufwand einsparen können
- Erfahren Sie in der [Webinar-Aufzeichnung](#) mehr über Ransomware-Schutz von Archiven und Backups
- Entdecken Sie unsere software-basierten Archiv- und Speicherlösungen [iCAS Middleware](#) und [iCAS FS Scale-out Speicherplattform](#)
- Melden Sie sich zum [iTernity Newsletter](#) an, um über alle News & Events auf dem Laufenden zu bleiben

GRENZENLOSE SKALIERBARKEIT FÜR BEGRENZTE IT-BUDGETS

iCAS FS ist eine Scale-Out Speicherplattform für Archiv, Backup und geschäftskritische Daten aller Art. Die software-basierte Lösung ist grenzenlos skalierbar und besticht mit geringen Gesamtkosten, einfacher Handhabung und hoher Flexibilität.



53% Kosteneinsparung im Vergleich zu Public Cloud Storage und Sie behalten die Hoheit über Ihre Daten



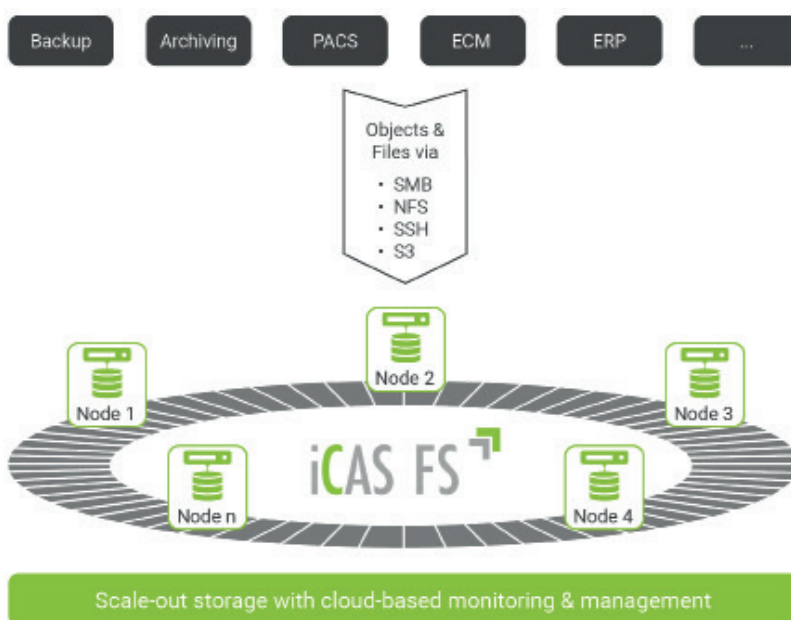
Klein starten, unbegrenzt wachsen: Scale-out in einer software-basierten Speicherplattform



Die Vorteile der Public Cloud im eigenen Rechenzentrum: hohe Flexibilität, einfache Skalierbarkeit, geringer Aufwand



Kein Aufwand, keine Sorgen: Managed Services mit Monitoring, Administration und Fehlerbehebung



iCAS FS ermöglicht zukunftsichere Datenspeicherung und Archivierung bei geringen Gesamtkosten. Die Plattform eignet sich optimal für den Schutz von Daten aus verschiedenen Anwendungen und Quellen und ermöglicht revisionssichere Archivierung, Ransomware-sichere Backup Speicherung sowie die Entlastung Ihrer Primärspeicher.

Die software-basierte Architektur baut auf Standardhardware und einem Linux Betriebssystem auf. Dank WORM Speicherung, S3 Object Lock, Retention Management, Verschlüsselung und Audit Trail werden Compliance und Sicherheit groß geschrieben, was auch durch die KPMG bestätigt wurde.



MÖCHTEN SIE MEHR ERFAHREN?

Vereinbaren Sie eine Demo oder diskutieren Sie Ihre Anforderungen mit uns:
info@iternity.com | +49 761 590 34 810 | www.iternity.com/demo