



Compass Health erzielt mit der Arcserve UDP Appliance einen vereinheitlichten virtuellen Datenschutz



INDUSTRIE: Gesundheitswesen

UNTERNEHMEN: Compass Health

MITARBEITER: 340



Compass Health stellt qualitativ hochwertige und umfassende Gesundheitsdienstleistungen für Patienten in East Lansing, Michigan (USA) bereit.

HERAUSFORDERUNG

Compass Health ist ein neuer multidisziplinärer Klinikverbund, der ein hochleistungsfähiges System zum Schutz vor Datenverlust aufbauen musste. Zudem sollte eine Lösung für standardisierte Backup-Prozesse und die Migration der Daten in eine hochgradig virtualisierte IT-Umgebung installiert werden.

LÖSUNG

Die Arcserve UDP Appliance ermöglicht nicht nur die granulare Datenwiederherstellung, sondern unterstützt auch den effizienten und effektiven Schutz der virtualisierten Daten. Zudem zeichnet sich die Lösung durch ein für die Klinik ausgezeichnetes Preis-Leistungs-Verhältnis aus.

NUTZEN

Dank der Arcserve UDP Appliance hat Compass Health den Zeitaufwand für das Backup drastisch verringern können. Ein weiterer wichtiger Faktor ist, dass die IT-Abteilung jetzt auch in der Lage ist, virtuelle Server schnell wiederherzustellen.

BUSINESS

Spitzenqualität in der Patientenbetreuung

Compass Health mit Sitz in East Lansing, Michigan ist ein schnell wachsender multidisziplinärer Klinikbetreiber, der sich auf die Spezialgebiete Onkologie, Neurochirurgie, Urologie und Dermatologie fokussiert. 40 Ärzte und 300 Fachkräfte bieten ihren Patienten erstklassige medizinische Dienstleistungen.

HERAUSFORDERUNG

Heterogene Backup-Systeme vereinheitlichen und Virtualisierung ermöglichen

Compass Health muss die Integrität und Verfügbarkeit seiner Patientendaten schützen, um den Anforderungen an medizinische Spitzenleistungen gerecht zu werden. Unglücklicherweise war genau der Schutz dieser Daten zu Beginn das große Problem.

Unter dem Dach von Compass Health haben sich mehrere Anbieter von Gesundheitsdienstleistungen zusammengeschlossen – und jeder kam mit seiner eigenen IT-Infrastruktur.





„Als ich übernahm, hatte eine Klinik beispielsweise seit mehr als eineinhalb Jahren die Bänder auf ihrem fünf Jahre alten Server nicht mehr gewechselt. Im Prinzip haben sie mit einem Produktions-Server ohne Backups gearbeitet“, erinnert sich Carl Seibold, IT Director bei Compass Health.



Das Ergebnis: Ein komplexes Gebilde von einfachen Scheduling-Programmen, Electronic Medical Record (EMR)-Systemen im Wert von mehreren Millionen US-Dollar und teils veralteten Backup-Lösungen, welches den jungen Firmenverbund verwundbar machten.

„Als ich übernahm, hatte eine Klinik beispielsweise seit mehr als eineinhalb Jahren die Bänder auf ihrem fünf Jahre alten Server nicht mehr gewechselt. Im Prinzip haben sie mit einem Produktions-Server ohne Backups gearbeitet“, erinnert sich Carl Seibold, IT Director bei Compass Health.

Eine andere Klinik hatte zwar bessere Lösungen im Einsatz. Doch als Seibold versuchte, die Daten von einem Fax-Server wiederherzustellen, war dies mit dem vorhandenen Bandlaufwerk nicht mehr möglich.

Dem Management von Compass war die Wichtigkeit des Datenschutzes bewusst, um den Fortbestand („Business Continuity“) der Organisation gewährleisten zu können.

Doch die Bereitschaft der einzelnen Sparten und Tochterbetriebe, neue Lizenzen zu erwerben, war gering und verkomplizierte die IT-Zusammenlegung noch mehr. Diese Betriebsteile hatten sich zum Teil gerade in ein neues Konstrukt eingekauft und scheuten Doppelkosten.

Als Übergangslösung implementierte Seibold effektivere Backup-Lösungen in jeder Klinik. Die Daten der jeweiligen Subbetriebe waren so wenigstens geschützt und – wenn auch sehr zeitaufwändig – verwaltbar.

Seibold erklärt: „Alleine für die Backups habe ich zuvor im Schnitt acht bis zehn Stunden pro Woche gebraucht. Und für das



Seibold erklärt: „Alleine für die Backups habe ich zuvor im Schnitt acht bis zehn Stunden pro Woche gebraucht. Und für das Wiederherstellen von einzelnen Maschinen hätte ich nochmal acht bis zwölf Stunden aufbringen müssen. Ich wollte eine Lösung, mit der ich z.B. nach einem Brand in einem Gebäude in der Lage wäre, alle Daten innerhalb weniger Stunden in einem anderen Büro zur Verfügung stellen zu können. Das war eine gewaltige Herausforderung.“



Wiederherstellen von einzelnen Maschinen hätte ich nochmal acht bis zwölf Stunden aufbringen müssen. Ich wollte eine Lösung, mit der ich z.B. nach einem Brand in einem Gebäude in der Lage wäre, alle Daten innerhalb weniger Stunden in einem anderen Büro zur Verfügung stellen zu können. Das war eine gewaltige Herausforderung.“

Seibold ist auch ein vehementer Befürworter von Virtualisierung – doch leider war die Infrastruktur für den Datenschutz, die er übernommen hatte, nicht wirklich für virtualisierte Umgebungen ausgelegt.

LÖSUNG

Robuster virtueller Datenschutz

Compass Health benötigte eine vereinheitlichte Backup-Lösung, die Patientendaten zuverlässig und dauerhaft schützt. Gleichzeitig sollte sie eine hoch-virtualisierte Umgebung ermöglichen – und zwar zu einem Preis, der sinnvoll in das Budget der Kliniken passte.





„Mir war klar, dass die Umgebung zu 100% virtualisiert sein sollte. Es war das eindeutige Ziel, nicht nur im Laufe der Zeit von einer Hardware-Plattform auf eine andere zu migrieren, sondern auch einheitlich Daten wiederherstellen zu können“, erklärt Seibold.



Die Lösung sollte außerdem einfach zu testen, problemlos zu verifizieren und schnell bei der Datenwiederherstellung sein.

„Mir war klar, dass die Umgebung zu 100% virtualisiert sein sollte. Es war das eindeutige Ziel, nicht nur im Laufe der Zeit von einer Hardware-Plattform auf eine andere zu migrieren, sondern auch einheitlich Daten wiederherstellen zu können“, erklärt Seibold. Auf der Suche nach einer robusten Datenschutzlösung evaluierte Seibold u.a. Veeam, Acronis und Arcserve.

Am Ende entschied er sich für die Arcserve UDP Appliance.

„Ich war von Anfang an überzeugt. Meiner Meinung nach kann nichts Arcserve mit der virtualisierten Umgebung übertreffen“, fasst Seibold zusammen. „Acronis hatte einfach nicht die Technologie, die ich suchte. Und Veeam hatte große Probleme bei der granularen Datenwiederherstellung.“

Heute schützt Seibold die Daten über neun virtuelle Server hinweg im Datacenter der Hauptverwaltung sowie über virtuelle Hosts in entfernten Kliniken.

NUTZEN

Eliminierung der Komplexität reduziert das Risiko von Datenverlust und IT-Zeitaufwand

Mit der Arcserve UDP Appliance steht der Datenschutz bei Compass Health auf soliden Beinen. Durch die Arcserve De-Duplikation und Kompression hat Seibold das Datenvolumen von ursprünglich 18 TB auf 5,4 TB auf der Appliance reduzieren können.

Wichtiger noch ist, dass beim Test der Disaster Recovery bestätigt wurde, dass Daten problemlos auf den virtuellen Servern wiederhergestellt werden können.

„Mein Aufwand für das Verwalten der Backups hat sich auf 10-15% reduziert“, resümiert Seibold. „Und die meiste Zeit verbringe ich jetzt für Testläufe – um sicherzustellen, dass das virtuelle Backup ohne Probleme verläuft – und nicht mehr für das Beheben von Fehlern und Ausnahmen.“

„Ich werde am Sonntagabend ein paar Stunden damit verbringen, eine der virtuellen Maschinen zu testen und eine komplette Datenwiederherstellung zu machen. Mehr gibt es nicht zu tun“, so Seibold weiter. „Wenn ich Änderungen am Upgrade-Server vornehme, werfe ich nur einen Blick auf das Dashboard. Dann noch die Checkbox überprüfen um sicherzugehen, dass der neue Server abgesichert ist, sobald er in Betrieb geht – und schon kann es losgehen.“

Würde Seibold Arcserve anderen Unternehmen im Gesundheitssektor empfehlen?

Seibold antwortet ohne zu zögern: „Habe ich – und werde ich.“



Mehr Informationen auf [arcserve.com](https://www.arcserve.com)