



Healthcare Giant Aspires to Increase Business Continuity with Robust IAM Resilience Platform:

A Use Case in Today's Volatile Market



The pandemic and COVID-19 has transformed the digital workspace, with Healthcare organizations feeling the pains of overloaded hospitals, healthcare providers, claims, and in and outpatient concerns. Technology has become a necessary tool to both ease the processes and workflows of various organizations, and yet the concern of failure and crashes, breaches and cyberattacks is increasing.

When a global financial crisis affects such a critical industry, business continuity is an unquestionable priority.

Recent cyberattacks in hospitals, like the one experienced at Ross Memorial Hospital in Ontario, prove there is an ongoing and essential demand for healthcare institutions to maintain a strong back-up and recovery strategy with effective implementation. The hospital reported a Code Grey, used in the cases of utility loss, such as water or electricity, as well as cyberattacks impairing critical IT systems. In the institution's efforts to maintain business continuity and provide optimal care to patients, they are working with cybersecurity experts and investigating the issue. A [source](#) also indicates that the road to recovery for various institutions experiencing similar cyberattacks, like Tallahassee Memorial HealthCare, have gone as far as having to resort to manual paperwork for administrative processes and the usual digital prescriptions. A hospital in Maryland also reported being victims of a ransomware attack in February 2023, with limitations to the patient care services.

The need for cost-effective tools that help healthcare institutions take proactive measures to back up their data and equip themselves with a robust disaster recovery platform is not only essential, it's vital to human survival. These organizations must find solutions to minimize downtime, maximize productivity, and ensure global health concerns are not affected by technological mishaps. Healthcare organizations today are taking action and responsibility, recognizing the critical factor technology plays in the industry. One organization reached out directly expressing a need to ensure failover time is critically low, with the need for data to be fully accessible and recoverable in the case of an event so physicians can continue to work.

Recent market research has broken down mind blowing statistics that prove the pertinence of IAM protection and recovery solutions for healthcare institutions:



In the last two years, 93% of healthcare organizations have encountered a breach.



Of the aforementioned 93%, downtime was a serious issue for 43% of these healthcare organizations that were victims of breaches, affecting everything from patient care, ROI, physician, and physician or healthcare providers' efficiency and productivity, along with reputational damage.



IT teams are wasting time and energy on managing access and permissions to critical IT systems for entities and identities in healthcare organizations, dedicating 15 hours a week that accumulated to nearly a whopping 800 hours a year!



An astounding 61% of healthcare organizations surveyed indicated that they have a IGA (Identity Governance Administration) solution implemented, clearly illustrating a need for cost-effective governed access management.



And lastly, of the IT and IT Security decision makers in healthcare surveyed, 95% openly stated that prioritizing identity security is either important, absolutely vital, and some indicated it was the prioritized investment within their organization.

Both RTO (Recovery Time Objective) and RPO (Recovery Point Objective) are essential considerations within healthcare organizations, along with compliances and budgets.

Let's investigate one organization's use case, as they approached our team with their concerns and parameters.

Use Case:

Large Scale Healthcare Organization With Multiple On-Site Facilities



What are the Critical Needs of Healthcare Institutions in Today's Digital Workforce?

A large scale enterprise healthcare organization with 15,000 stakeholders and employees inclusive, (on-site, corporate, hospitals and contractors), with 100 applications stored in the IT infrastructure voiced their concerns about how they could optimize failover processes. Failover time and processes are the transfer of mission-critical applications to a remote or backup server required to maintain operations and business continuity in the event of an IT infrastructure crash, breach or full on downtime due to failures. The time is essentially the amount of time required to recover the data backed up so operations and business can continue as usual.

The organization also expressed the need to allow healthcare professionals, like physicians, nurses, and especially wards like triage and emergency to bounce back into full operations in the case of a disaster and full system crash or failure. There is no time to waste. Lives are at stake and sensitive data and fully operational productivity and agility is a 24/7 need in hospitals. Any resources housing data on a corporate, internal and external level maintain vulnerable assets that could save a life. If IT systems are inaccessible and at stake, human lives are also at risk.

Compliances and Regulations: Measures to Meet Them and Protect the Enterprise

As always, the healthcare sector is ridden with static and dynamically growing compliance requirements. Protecting their mission-critical assets to maintain workflows and discretion of data is both apparent and an industry must. Certifications and compliance requirements like HIPAA, PCI and HITRUST are standard, and lowering risk of data compromise is now pertinent more than ever. Acquiring a cost-effective tool that enables business continuity with a disaster recovery and back-up solution for all mission-critical assets housed in the healthcare institution's IT infrastructure is without question a means to an end. Audits become a lower risk and smoother process, plus acquiring cyber insurance becomes an easier endeavor. Organizations can expect to bounce back into fully operating facilities with minimal down time and lowered to zero RPO, plus a quick recovery time with shorter RTO. This healthcare institution indicated that meeting these compliances was not only a must, it was becoming a growing concern that required a robust yet cost-effective access and business continuity solution.



Healthcare Budgets:




A Powerful, Cost-Effective Plan and Platform For Business and Access Continuity

The global financial crisis, inflation and budget cuts are particularly visible and evident in the healthcare industry. Finding a cost-effective solution to ensure business continuity with IT infrastructure within hospitals and large-scale healthcare organizations is truly a dire need today.

Reputational risk and the lives of millions are at stake if a seriously critical medical facility loses their ability to operate due to IT infrastructure crashes, lockouts or issues with accessing mission-critical assets and resources.

This organization in particular had already experienced the wounds of an AWS East deployment crash, and they were challenged with Okta's inability to help the organization transition their data to another AWS region. With a strong access and business continuity platform, this organization benefits from a seamless transition to any cloud-based infrastructure, AWS included. Plus the unparalleled benefit of reduced and low RTO is a massive advantage and upper hand when the delicate nature of human lives are at stake and physicians simply need to work.

With 4000 working physicians in the picture, there was a need to present a product and solution to their c-level management and tech team that would answer the following demands and questions:

-  What does the failover process look like in the case of a system failure, crash, breach or full on IT infrastructure event?
-  What is the expected failover time for an organization with our numbers?
-  What is our recovery time so we can plan for patient care immediately or as quickly as possible in the event of an IT disaster or crash?

Acsense unlocks three essential requirements of the organization's overall business continuity plan, empowering businesses with:



The ability to protect identities, access and permissions data



Investigation tools to effectively and quickly identify affected system components



Recovery solutions of production systems to any point-in-time, or failover of the entire organization to work from a secondary access control system in the case of inaccessibility due to lockouts, cyberattacks, system failures or any compromise of service.

About:

Acsense is a cutting-edge easy to use IAM resilience platform that caters to both workforce and customer IAM requirements with a unified solution. Our platform boasts one-click recovery, continuous data verification, routine testing, and the ability to detect alterations between Points in Time, fortifying the resilience of your IAM system.

acsense is backed by Joule Ventures, Gefen Capital, Fusion and independent investors.

To learn more visit www.acsense.com



Subscribe to our newsletter.



Follow us on LinkedIn.

