Fast and Simple BDR for Healthcare

Quorum®

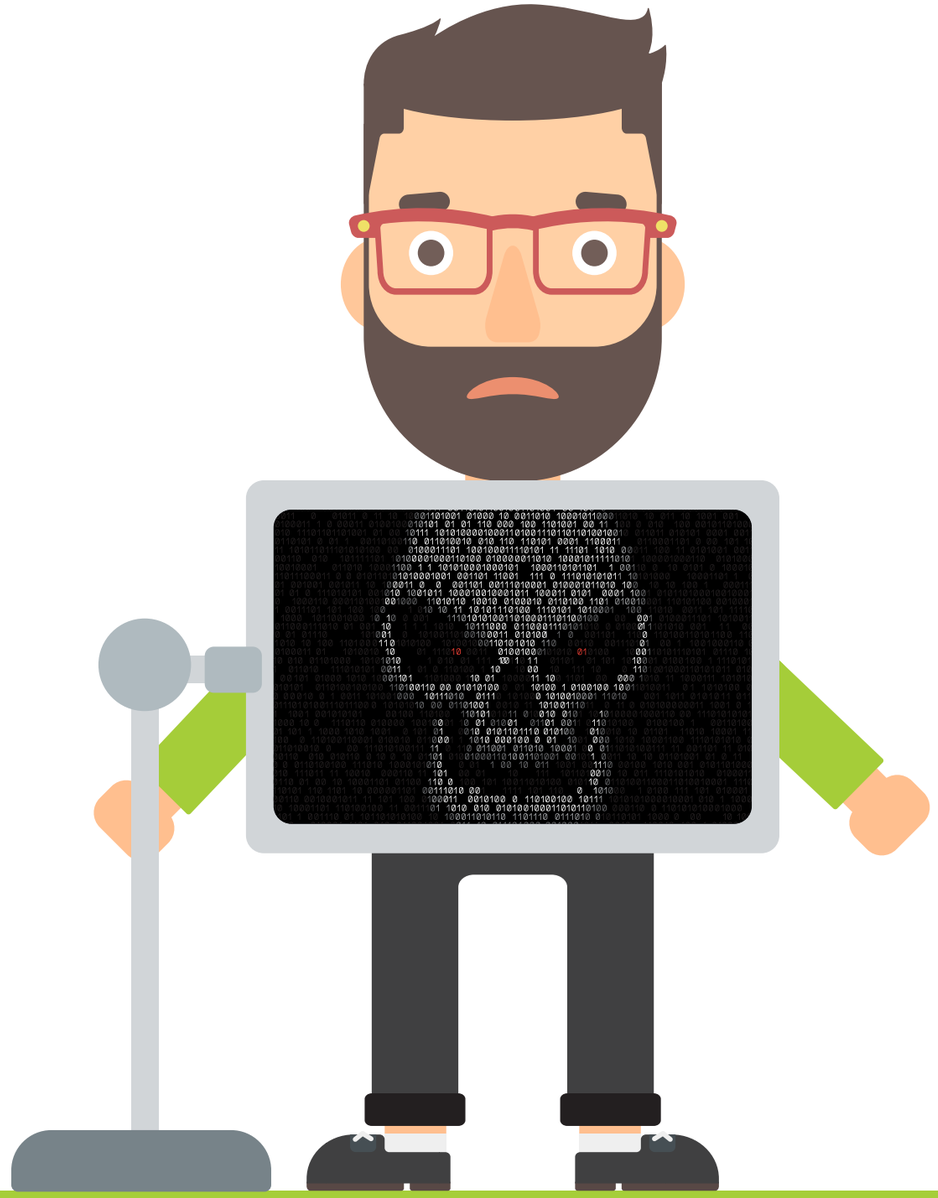
COMPLIANCE, SECURITY AND UPTIME: THE TRIPLE THREAT

Backup and disaster recovery is important for every business—but there's no arguing it's more important for some industries than others. For healthcare IT leaders, maintaining uptime isn't just about keeping the workforce productive. Ensuring doctors have access to critical medical data can be a matter of life and death.

While cyberattacks reach across all industries, healthcare has become the most attacked industry in the world. Insurance companies, hospitals, clinics, billing agencies and other companies must protect their data from well-organized criminal rings—rings that are relentless, well-funded and technically adept. ePHI data and personal details such as social security numbers, medical histories and family information are a top target for cybercriminals. And safeguarding healthcare IT servers and data isn't the only concern. The team must also monitor and manage their data assets in a way that meets complex HIPAA and other compliance regulations. If they don't, they face the fines and penalties of failed audits.

Another factor in healthcare IT vulnerability: the evolution of medical technology, such as patient portals, cloud-based apps and networked medical devices and equipment. Remote access means that sensitive data flows between laptops, portable devices, network servers and more as physicians travel between hospitals and clinics, and medical personnel consult with other staff. These tools help physicians provide optimal care and engage patients in their own health and well-being. Yet these technologies present healthcare IT teams with a formidable challenge when it comes to backup and disaster recovery.

Just one server failure or attack can stop physicians from accessing the ePHI they need to make vital treatment decisions. To protect patient well-being, healthcare IT teams and the users they serve must have round-the-clock access to a resilient and reliable IT infrastructure. For them, BDR is more than just a simple replication of healthcare data as disaster insurance; a solution must provide immediacy, flawless reliability, and advanced security and compliance. Leaders must approach their recovery strategy as a critical factor in improving patient outcomes, empowering physicians and protecting sensitive data. Immediate access to accurate data—whether retrieving the medical history of an unconscious car accident victim or triaging care for a cancer patient—is of profound significance for both healthcare organizations and their patients.



THE DANGEROUS TRAP OF WEAK BDR

Risk, delay and *unsafe* are never positive words when it comes to healthcare. Yet many organizations are still relying on BDR solutions that put their reputations and their patients at risk.

The most common justification for staying in the dark ages of BDR: cost. Many IT leaders, who've long since transcended the day-to-day details of backing up data, testing systems and failing over, dismiss their teams' complaints. They don't see the invisible costs that accompany a typical legacy BDR system. In reality, most traditional systems drain a team's most valuable resources: time, budget and staff productivity. Engineers who could focus on innovative advancements are instead spending hours testing backups and babysitting slow data migration, or losing days to downtime.

Other leaders believe their current solutions are adequate—not perfect, but as good as it gets in the world of backup and disaster recovery. And there was a time when that was probably true. But recent advances in BDR have ushered in a new world of speed, efficiency and performance even after a crippling IT event—and healthcare IT is positioned to benefit the most from them.

THE RISK INVOLVED IN SLOW OR UNRELIABLE BDR CAN HAVE A CATASTROPHIC IMPACT ON A HEALTHCARE ORGANIZATION IN MULTIPLE WAYS.

1

Their backups are unprotected, untested and unreliable.

Whether it's a collection of tapes in a remote data center, or cloud replicas that haven't been encrypted, too many IT teams are relying on backups that can be stolen, corrupted, breached or worse. When disaster hits and they need to quickly failover, the doctors are working from outdated or incomplete information.

2

Long delays in recovery endanger patients and frustrate staff and physicians.

A medical records clerk who can't retrieve a file; a rotating physician who needs to access test results while traveling between clinics; an operating room surgery paused when medical records aren't available; even a "minor" outage can have severe repercussions when it brings normal healthcare operations to a halt.

3

Multi-vendor solutions create chaos and roadblock resolution.

With different point solutions that don't always work well together, efficiency nosedives as the team spends hours managing vendors, trying to get answers from third-party support teams, and manually compensating for the gaps between systems. Inevitably a security vulnerability or failover obstacle sabotages recovery right when it's needed.

4

Long periods of downtime invite Ransomware attacks.

Criminals know that hospitals must have access to their patient and medical data no matter what, making them a prime target for Ransomware attacks. If the team can't immediately failover to a protected and up-to-date replica, they may be forced to pay the ransom demands as a matter of survival.

5

Compliance gaps damage brand reputations and impose harsh penalties.

Most healthcare organizations are subject to multiple sets of compliance regulations, such as PCI for those credit card numbers in the hospital billing records and HIPAA for the protected health information. Yet while some teams will follow compliance regulations as a blueprint for their production environment, their replica environments are neglected—resulting in failed audits and regulatory fines.

While some industries may skate by with a mediocre BDR solution, healthcare IT teams simply cannot afford to compromise.

PROTECTING HEALTHCARE IT WITH STRONGER BDR

When evaluating backup and disaster recovery solutions, keep your eye on the data triumvirate: security, speed and performance. Better technology may deliver higher efficiency, it's true, but almost every BDR solution will bill itself as the best technology the industry has to offer. To identify the genuinely best solution for your healthcare IT team, look for the following traits—and don't settle for anything less.

Demand the fastest backup and recovery in the industry.

There was a time when epic downtime couldn't be helped. That time is over. While some leading BDR solutions are still too complicated and insufficient for speedy recovery, some solutions can get you back on top in just minutes, thanks to appliances with 25,000 IOPS. This near-instant recovery is the deciding factor when it comes to protecting your reputation and your users' data.

PRO TIP

Incorporating virtual machines (VMs) that function as copies of your servers usually means faster and more complete recovery for all of your important files and applications. When you failover, you land in an environment that matches yours in every way - keeping the entire show running.

Insist on full recovery.

Some teams still assume that fast recovery involves making Sophie's Choice in terms of which systems and servers they'll call up first. But today's typically complex healthcare organization can't afford to service only a portion of its users; choosing between a laboratory database and patient medical histories will leave some portion at risk no matter what. It also results in an expensive loss of productivity when the insurance company staff stop working while the team resurrects the claims processing system. Look for a solution that recovers all of your mission-critical systems.

Reliability must be a given.

While some solutions promise consistent uptime, digging beneath the surface often reveals other factors that can impact recovery. Ask if the solution uses an isolated sandbox environment that lets you do patch testing, upgrades and configuration changes before moving into production. You want a solution that stands alone, so any failures in your production environment won't impact your recovery. Also look for application consistent backups that ensure you'll never sacrifice transactions; crash consistent backups can frequently lose data in motion.

Embrace the cloud.

On-premises backups can play a valuable role in any organization's BDR plan, but the cloud adds the flexibility, cost savings and uptime insurance so required for healthcare IT teams. Not only will most manual maintenance, testing and upgrades vanish, cloud elasticity and scalability can accommodate your fluctuations in demand without wasting unused resources. Cloud BDR also helps organizations expand regionally or globally by liberating them from the need to build more and more datacenters. You can offer the same reliability and convenience for physicians no matter where they are, no matter where a disaster may strike – and you can failover and recover without even standing up from your desk.

Minimize chaos with a unified solution.

IT leaders who haven't kept pace with BDR advances often assume they can't get high availability, disaster recovery and cloud failover from a single product. They tend to be accustomed to patchwork solutions that cobble together hardware from multiple sources and countries, and third-party support. The result is extensive time devoted to managing different vendors and trying to integrate solutions that don't work smoothly together. Today unified solutions are available, which means you can get all your needs met with one vendor. Every component of your BDR system will work smoothly together in a cohesive efficiency, with a single team that understands your needs, your challenges and your configuration. Any support will come directly from the same engineers who built the solution.

Prioritize security.

With medical and personal data being sought after by skilled criminals, every backup must be protected as the final line of defense. Data centers should offer Tier 1 architecture and be monitored at all times; data migration, cloud tenancy and remote access should all be architected with strong security controls. Backups should be protected by encryption in motion and at rest, with cloud backups passing through a 128 bit AES encrypted session over a 256 bit AES VPN tunnel. Any link used to connect or upload your data should be secured through SSL or other protocols as well.

Look for built-in compliance.

To avoid the painful repercussions of a failed audit, ask vendors if their solution can meet your regulatory needs. Be specific about the local, federal and international regulations you're required to meet, such as securing data or retaining certain types of data for mandatory time periods. While HIPAA is important, it's not the only compliance game in healthcare town. Look at all of your data in all of your systems and find a solution that meets the standards of any regulatory institution that might audit you.

Ensure your replica environments perform at full speed and power.

Surgeons, nurses, ER clerks, respiratory therapists and lab techs need accurate data snapshots around the clock. Your BDR solution must be able to deliver backups that perform as well as your production environment. A sluggish replica environment will be viewed as only a micro-improvement over outright downtime if staff cannot easily access databases to retrieve critical records. The counterpart to immediate recovery is a solution that spins up replicas as fast as your normal environment.

Unlock simplicity with advanced automation.

Today's best BDR solutions feature a number of tools that can erase complexity and labor-intensive processes. A few to look for: incremental snapshots that let you skip full backup processes while still offering single file retrieval or a runnable virtual machine. A simple, one-click failover process not only saves time, but ensures that any team member can failover, even without training. Any complicated failover model with too many steps will sabotage recovery. Automated testing, all-in-one dashboards and more can simplify your IT life and liberate your best engineers from tedious administrative tasks like testing backups and managing multiple data centers. Simple, automated processes will reduce errors, boost team productivity and ensure you can failover quickly when you need to.

FORTIFYING THE FUTURE OF HEALTHCARE IT

With the rise of healthcare technology, both patients and medical personnel are finding new ways to manage treatment plans, strengthen the patient-doctor relationship, and advance patient well-being. The challenge of mounting data will only increase, requiring healthcare IT teams to secure, store and manage their information accurately while investing in new tools to maintain its availability. Only the best BDR solutions can secure valuable healthcare data and position systems for rapid, efficient recovery.

While downtime can damage every type of business, it can impact human lives in healthcare IT establishments. To protect patient well-being and keep medical staff productive, the healthcare industry must make advanced backup and disaster recovery a top priority. Trying to address the above challenges with traditional BDR will not offer sufficient protection. Leaders that cling to yesterday's solutions will put their patients at risk, but those who evolve will empower their physicians and staff to deliver a new level of reliability and safety in patient care.