Agility

For confidentiality reasons, the customers profiled in these case studies will be referred to as "The Banking Institution" and "The Practice."

DRaaS Case Studies

Data Protection and Disaster Recovery Combine to Meet Banking Needs

Background

When The Banking Institution's disaster recovery hardware was set to end with no option to renew due to their current equipment reaching end of life. Their options were to replace the equipment with new hardware, or to find a hosted solution. They determined that a hardware replacement cost would be approximately 38% higher than a managed solution,

Requirements

One of the biggest challenges for any financial institution is the sensitivity of customer data, as they must adhere to stringent financial security requirements. Not only was The Banking Institution in need of a secure solution that could hold up to industry standards of PCI and FINRA compliance, but hey also needed a solution that had he capacity to store all of their data and would be compatible with their existing environment, which was 95% Windows-based, VMware, and a few Linux machines. In addition, they needed a solution that was easy to understand and wouldn't be too complicated for their IT staff to run or manage.

> “In the banking industry, everyone knows you have to offer a highly available system, and data backup and recovery is essential as well. We were able to have both a DR solution and a high quality data backup and recovery system for about the same cost of each. Also, the Proof of Concept was non-evasive.”
> - Banking Institution Representative

Data Protection Plan

The Banking Institution opted for a cloud based solution with a 15 minute failover guarantee that was both easy to use and manage. This solution offered rapid server replication to the cloud and included powerful failover and orchestration technologies. Most impressively, the solution allowed them to seamlessly move from proof of concept to implementation without any configuration changes, so it was ready to go right away.

The Banking Institution was able to secure protection from data loss and minimize downtime with the implementation of a DRaaS solution that combined the power of the cloud with an on-premise data protection appliance.

“"It's an easy-to-use solution that functions very well with minimal management from my end. Implementing this solution really frees up my time to work on other critical projects.
- Banking Institution Representative

Rooting out Ransomware:
DRaaS Keeps Dental Practice's Data Safe and Secure

Background

When a dental office owner and principle practitioner experienced a ransomware attack, he knew he needed to take action to prevent further attacks, downtime, and lost operational hours as soon as possible.

The busy office depended on its IT infrastructure to enable operations and keep private data secure, including imagery from X-rays, complete patient records, scheduling, and all other data maintained on their on-site servers.

The Pain of Downtime

Ransomware attacks against U.S. healthcare providers have led to more than $157 million in losses since 2016. Knowing the potential devastation another attack could inflict on the practice, it was critical to find an all-in-one solution for backup, recovery, and business continuity. Inability to access patient records is an extreme - and costly - inconvenience, as scheduling and treatment are impossible without accessible data.

> "Dental practices need more than just basic IT support. They have a unique infrastructure that requires experience in integrating their equipment, medical billing system, data storage, and more."
> -Practice Representative

A Repeat Attack Provides Rapid ROI

Less than one month after implementing their new, all-in-one DRaaS solution, The Practice was attacked again, with two servers infected with ransomware. The malware was detected right away and The Practice worked with their DRaaS team to take immediate steps to defend their systems. First, the team switched The Practice over to a virtualized, uninfected snapshot of their server that had been backed up to a secure cloud. Meanwhile, the team also deleted the infected files from the onsite server and restored it to full operation, all while continuing to back up ne files as patient visits moved forward on schedule.

""It's a changing world - there are a lot of vicious people trying to hack into doctors' offices. These attacks on small businesses don't make the headlines like they do when airports, school, or hospitals are targeted, but they hurt hardworking people."
-Practice Representative