



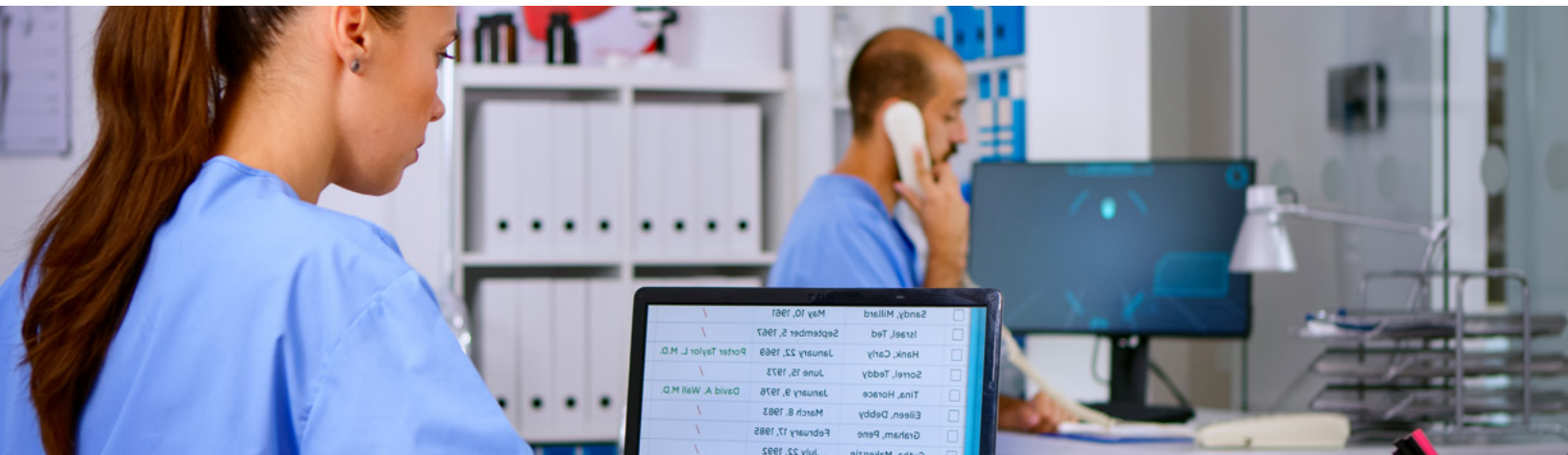
Large, Publicly-Traded National Healthcare Provider Solves Data Center Outages

Data Center Outages Cause Access Issues for Hospitals and Emergency Responders

In the healthcare industry, controlling access to sensitive patient data is crucial for compliance with [HIPAA's rules concerning privacy](#). However, data privacy isn't the only concern that healthcare facilities need to consider. Accessibility of information and systems is also crucial to hospital operations.

Being able to grant the correct hospital staff access to vital patient data, such as the patient chart, medical history, and other information is crucial for providing safe and effective healthcare in a timely fashion. When critical systems fail and hospital staff are unable to access systems and information needed for patient care, operations within the hospital can grind to a halt.

Worse yet, when systems go down, emergency response outside of the hospital can be negatively impacted. For example, when 911 dispatchers receive calls that require an ambulance or helicopter to be routed to the nearest hospital with available operating room capacity, a system outage at a hospital could leave the operator unable to assess if they have capacity. So, emergency cases where every second counts can end up being rerouted to hospitals that are much further away—putting lives at risk.



One large, publicly-traded national healthcare provider was encountering just this kind of issue. They had a mission-critical data center that was being used to house their on-premise software needed for hospital staff logins, inventory management, and task tracking.

This centralized resource hub suffered from periodic data center outages up to four times per year. While each outage was brief, hospital administration received complaints from staff about not being able to complete shift changes, gather data, or access necessary resources during their shift.

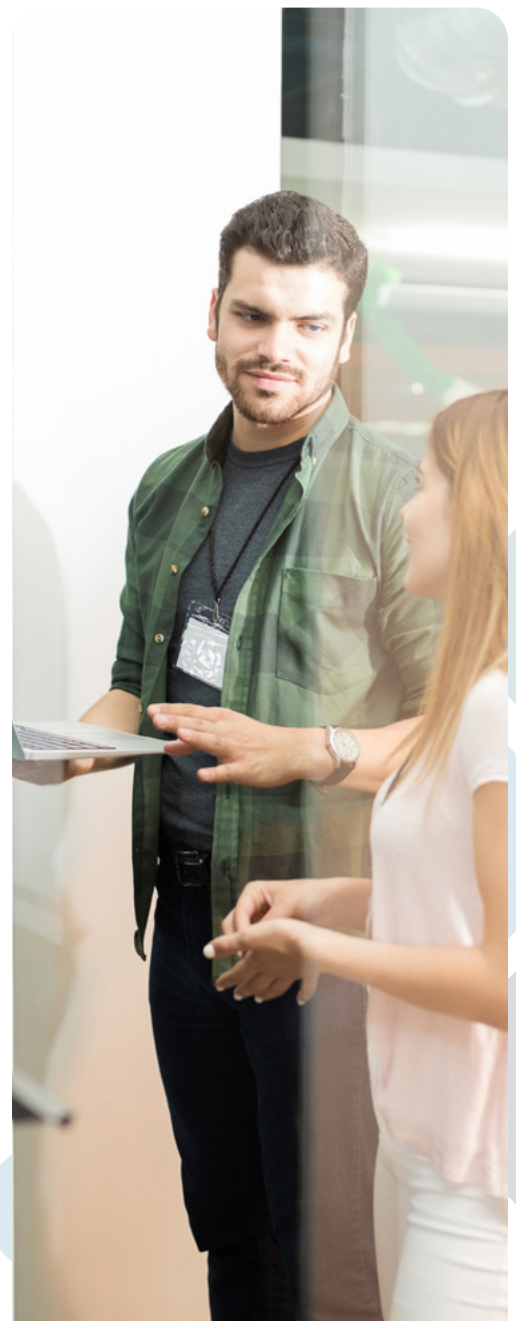
To avoid potential complications brought about by this data center outage issue, the hospital administration started investigating potential solutions. During this process, they consulted with each of their technology vendors and service providers, including GCA.

What Solutions Was the Hospital Using at the Time?

The client was, at the time, using an [identity management](#) (IDM) infrastructure provisioned in a NetIQ eDirectory alongside a mixture of PingOne and PingFederate as well as SaaS tenants and applications hosted in their data centers.

[PingFederate](#) is an on-premises solution while [PingOne](#) is a cloud-based identity as a service (IDaaS) solution for secure cloud single sign-on (SSO) and multifactor authentication (MFA). These solutions enable users of systems to have a single password and username for multiple resources—simplifying user access and security.

One major challenge in making this change was that the NetIQ eDirectory wasn't natively supported by Ping. To move the PingFederate instance to the cloud, the dependency on NetIQ eDirectory had to be removed.



Fixing the Problem

Step 1

Diagnosing the Problem

At the time the issue became known, the healthcare company was already a GCA client. They were trying to figure out why their access management system wasn't working and why key systems couldn't be reached. It was discovered that the issue wasn't with the IAM solution they were using, but with the data center that was hosting their on-premise solutions.

The data center was suffering intermittent outages. Because the [IAM solution](#) and other mission-critical apps depended on the data center to operate, it became the single point of failure in their network that brought operations to a halt.

There was another vendor involved in the mix that helped by putting together plans for a new system architecture that would, hopefully, resolve the data center outages. We reviewed these plans with a decision-maker from the healthcare organization and went over what would and wouldn't work—then proposed alternative solutions that would provide a more permanent and effective resolution to their issue.

Step 2

Moving to the Cloud

To keep operations from being impacted by random data center outages and other single points of failure, we recommended that the client set their PingFederate solution up in the cloud. Initially, they were going to host their NetIQ eDirectory instances in their own, private cloud to use with the new cloud-hosted version of the PingFederate solution, however, this would have introduced a host of other issues. After consulting with GCA, it was determined that a new directory would be needed for this cloud implementation.

[PingDirectory](#) does this for PingFederate, but for the then-current directory in the organization's data center, a connection was needed to keep it in sync while using PingDirectory for the cloud implementation.

In accordance with the recommendation from GCA, the architecture was modified to use the PingDirectory that is supported in the Ping Cloud alongside PingFederate instead of keeping part of the infrastructure in a separate cloud with maintenance and support costs associated with it. This made the overall solution much simpler, removed quite a few potential issues and shifted all support over to the cloud vendor at a significantly lower cost than had they maintained both technologies.

Fixing the Problem

Step 3

Integrating Cloud for IAM

Changes to accounts within the organization originate in specific authoritative sources, then are synchronized by the NetIQ infrastructure. The PingDirectory needed these near real-time updates to stay in sync but did not have a method to pull them at this rate. So, GCA suggested going the other direction: Using the existing IGA infrastructure from NetIQ to push the changes in close to real-time to PingDirectory as it does with the rest of the IGA-integrated systems.

To oversimplify things a bit: The client's SSO infrastructure would run on the cloud, across multiple datacenters—ensuring this critical infrastructure would be up and running despite any potential issues in the client's data center. The on-premise provisioning infrastructure would be leveraged to do synchronous provisioning as it is done with the on-premise version of the SSO infrastructure they had previously. The difference is, if there is an outage in the on-premise datacenter, the SSO infrastructure and any services, such as SaaS applications or applications not in the datacenter, will not be impacted.

To help with this, we recommended PingOne Advanced Services (P1AS), which allowed us to put the client's Ping infrastructure into Amazon Web Services (AWS) and enable Ping to manage it all for the client. This had the added benefit of providing 24/7 support with a 15-minute response time service level so that, if any issue did arise, the client could get a rapid response.

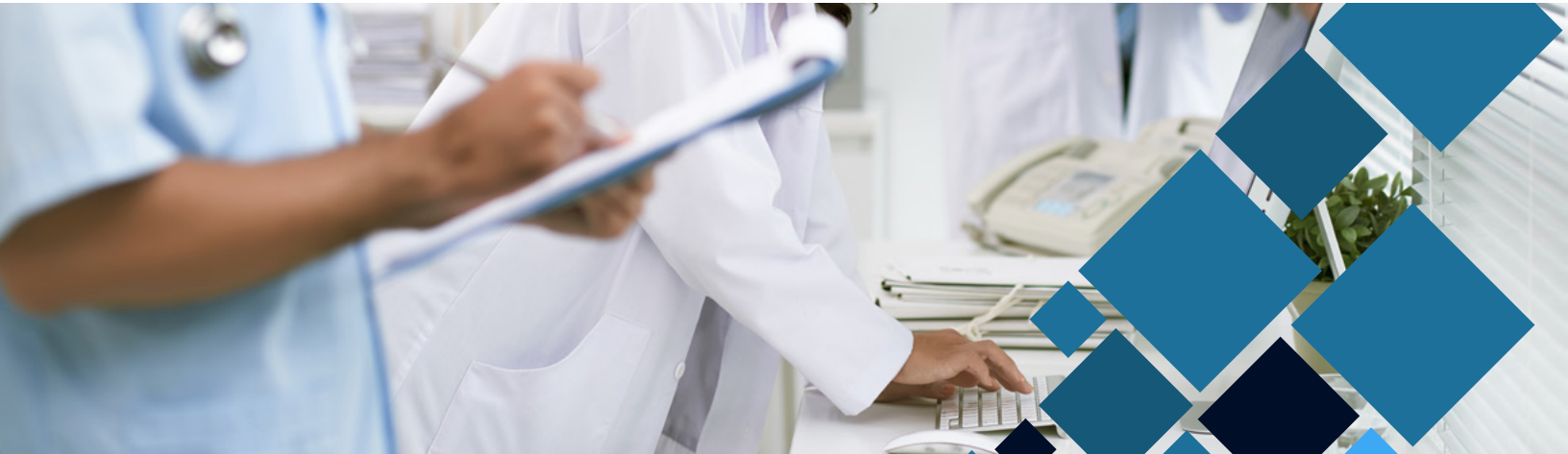
The GCA team changed the architecture to PingDirectory in the P1AS cloud and set it up to where the IDM infrastructure will provision that instead of NetIQ eDirectory in the data center. This, in essence, swapped the eDirectory with PingDirectory and provisioned Ping from the same IDM infrastructure. This provides several benefits:

- ✓ **Improved Business Continuity/App Uptime.** This setup allows the client's apps to continue running even in the face of data center outages.
- ✓ **Cost Savings.** By switching to PingDirectory on the cloud, the client has an opportunity to scale back on other costs—such as managing an internal data center.
- ✓ **Simplified IDM Solution Management.** With this change, there's no longer a need to use NetIQ eDirectory for the backend of Ping—which helps simplify solution management moving forward. Also, maintenance and operational tasks are now Ping's responsibility. So, there's less pressure on the client to manage IT solutions that aren't part of their core business focus.

Next Steps



The next step was to pick up the entirety of the client's on-prem data center infrastructure and clone/mirror it into the cloud. Then, we “flipped the switch” so that all SSO goes to the cloud instead of going to the data center. Of course, we did significant amounts of testing during this process and were able to set up a method to do pilot testing and seamlessly migrate over 60 applications all at once. The expertise allowed high levels of assurance there would be no interruption of service during this cutover and it was able to be completed quickly and as advertised.



Results

By moving their IAM solutions and their apps to the cloud, the client was able to improve accessibility, uptime, cost management, and risk management. Now, when both internal users and emergency dispatchers try to access any of the 60+ apps in use that are federated by Ping SSO, they can get in reliably and get the data they need (and only the data they're cleared for).

In a healthcare facility that takes in emergency cases, the speed and ease with which dispatchers can access vital information—like whether there is free operating room capacity or if the hospital has specific specialists available for an operation—may determine if a life is or isn't saved.

The GCA team is proud to have helped this healthcare client solve their data accessibility challenges.

Need Help with Your Identity and Access Management?

Call us at 1 (888) 422-9786

Contact Us