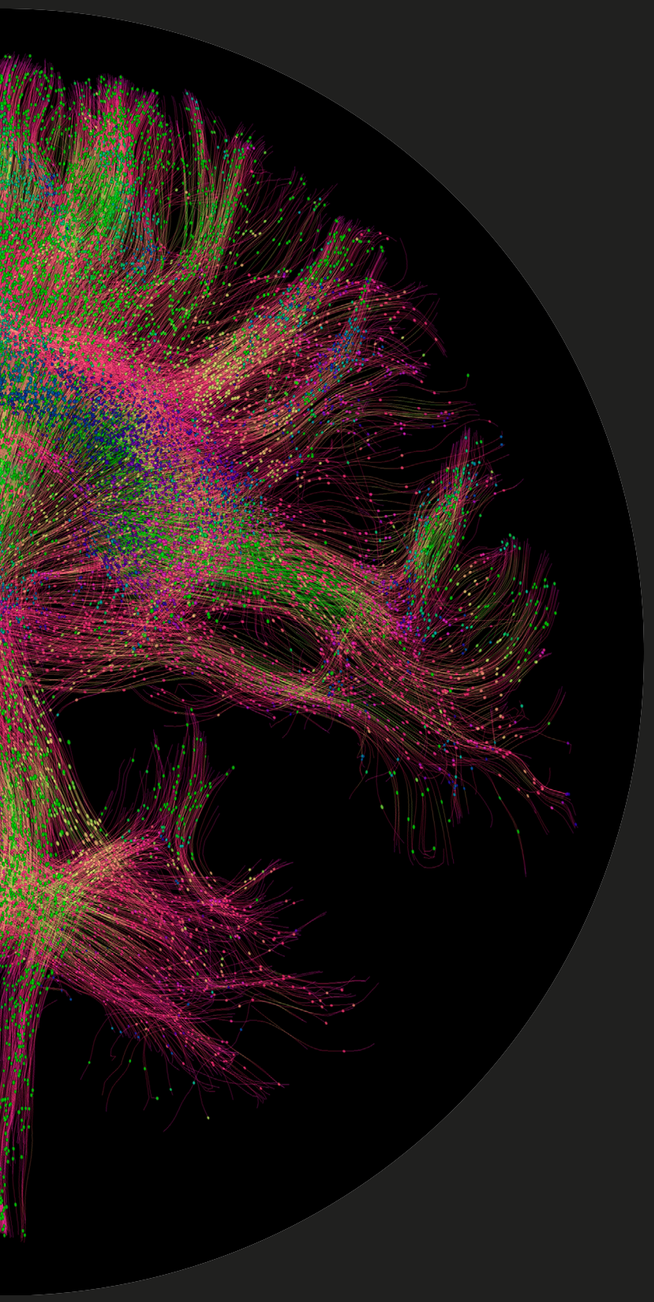


Merge

Stories of Imaging Resilience

Resilience breeds confidence: The key pillars of a resilient imaging environment.

merative

Introduction

Healthcare organizations strive to face their future with confidence – and do so with confidence in their technology partners.

A resilient imaging IT environment is key to creating and maintaining that confidence. An environment that minimizes security risks as much as possible. An environment with geo-resilience. An environment that is consistently reliable.

In this eBook, you'll read stories of organizations that have partnered with Merative and adopted our Merge imaging solutions to help improve patient outcomes, optimize care delivery, and create IT environments that are resilient against cyber risks, downtime, and the exasperation that comes with managing multiple services in-house.

Healthcare providers can't feel confident in the impact they make for their patients without feeling their IT environments are resilient and reliable. This eBook breaks down three essential ingredients of a resilient imaging IT environment –hybrid cloud, reliable uptime, and zero-trust security – and stories of how Merative, our partners, and our customers are working together to make resilient environments a reality for clinicians, IT teams, and patients.

Hybrid Cloud

Eliminating the hassle of managing multiple in-house services.

What's driving the move to cloud

Enterprises are getting tired of running infrastructure in their own data centers. Over the past decade, more and more organizations have begun outsourcing IT responsibilities like hosting servers, cybersecurity, and networking to colocation data centers (COLO), managed service providers (MSP), and, more recently, public clouds.

This strategy isn't about shifting responsibility for events like data breaches, but rather entrusting these matters to partners who are more specialized at managing these incidents and handling the necessary upkeep. In other words, buying into a better insurance policy.

"Lifting and shifting" current application architectures and workloads from on-premises to a COLO or public cloud may not save providers money. Instead, the net benefit is to reduce on-premise data center space and offload time spent managing the environment, while providing higher levels of availability, resilience, and security.

Cloud-native services such as Kubernetes and object storage can enable cost savings to a provider if the application is architected in a way to take advantage of the public cloud. The key is elasticity, with both the application compute and storage growing and shrinking with your workload, offering cost savings in the public cloud vs. depreciating infrastructure that is stagnant on-premise.

"System updates and security patches are a never-ending challenge in today's multi-server distributed environments. Managing these updates and tracking that every update has been made on every server requires ongoing meticulous attention straining in-house capacity. Outsourcing these services to vendors that specialize in this activity allows the enterprise to better manage the risk of missing an update or critical security patch; that responsibility falls to the provider now. Organizations want predictable upgrades, consistent, easy-to-track workflows, and an environment that is always up to date, without having to juggle the myriad required moving parts themselves."

James Boritz
Vice President of Development, Merge Imaging Solutions
Merative

The value hybrid cloud brings to the table

Every enterprise will migrate to the cloud at their own pace. Every situation is different, every enterprise has different needs, and these needs may change regularly. Some workloads will migrate completely to the cloud, others will need to remain partially or fully on-premise with business continuity in mind. A hybrid-cloud strategy accommodates all of those needs.

Hybrid cloud enables enterprises to control and adapt to their business needs, without fear of technical barriers, with geo-resilience and business continuity ensuring their ability to do their jobs and provide patient care. For example, a healthcare organization may choose to move its contingency applications to the cloud while running day-to-day production operations on-premise, getting the best of both worlds.

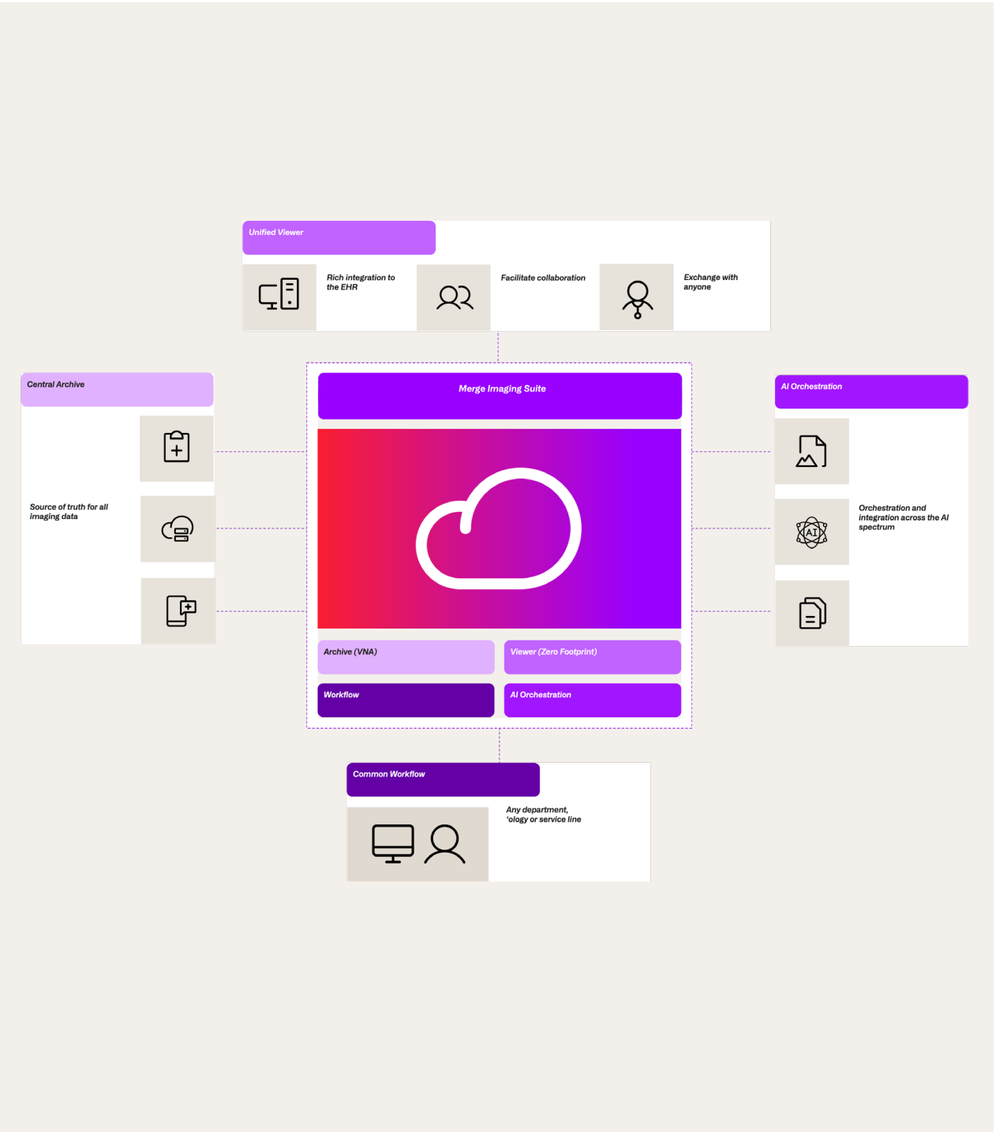
Taking cloud at your own pace with Merge Imaging Suite

Merge Imaging Suite empowers enterprises to migrate at their own pace, adopting a hybrid-cloud, modular approach with our Merge VNA, Merge Universal Viewer, Merge Workflow Orchestrator, and Merge AI Orchestrator.

Starting with Merge VNA – fully on-premise applications leveraging tier 2 cloud object storage, through all four modules in the cloud – we can start and progress your journey as it makes sense.

Merge Imaging Suite is cloud-native, leveraging Kubernetes and cloud-object storage to enable application and storage elasticity and provide our customers with a compelling ROI, all within the scale of our hybrid public cloud service.

Merge Imaging Suite charges on a per-study metric, where we take responsibility of the cloud-native environment. This includes all operations and security, while giving the provider control of the application administration, including when they would like to upgrade to a new version available.



McFarland Clinic and Uptime

Providing an antidote to the biggest source of imaging anxiety.

McFarland Clinic

The causes of downtime

The most common contributing factors to downtime usually originate in infrastructure (e.g., networks or servers), software and OS upgrades or misconfigurations; glitching interdependencies between different software; or interface engine stability or changes.

For McFarland Clinic, one recent episode of downtime occurred when an HL7 interface went down and consequently caused the downstream PACS to stop receiving order messages. Luckily, McFarland had several downtime procedures and contingencies to deploy – and in this particular case, the clinic's radiologists were able to switch over to a downtime worklist for studies that didn't have matching orders yet. This enabled the radiologists to continue working while IT addressed the orders interface. The ability to pre-cache images on these worklists allowed the radiologists to continue reading studies as if nothing had happened.

Downtime is impossible to predict, but it's also inevitable. You know it will happen eventually, just not when, so it's important to be proactive both with monitoring and building downtime procedures. Because McFarland Clinic had preconfigured and mapped out contingencies to quickly pivot systems and workflows, it was able to ensure little to no disruption to patient care during a downtime experience.

The impacts & ripple effects of downtime

On hospitals and patients

When the PACS goes down, that has a massive impact on ED and ICU clinicians. Hospitals begin considering diversion and ambulances are forced to bring patients and trauma victims to other hospitals that are still online, but further away. This places major stresses on these other hospitals – which are bringing on many more patients than they are fit to handle – but also robs patients of the choice to go to the hospital of their choosing.

On clinicians

When systems go down, image backlogs skyrocket. Clinicians are then forced to work longer hours – nights, weekends – for weeks just to catch up. This has ripple effects on home lives and family schedules, too; you can't be home in time for dinner or pick the kids up from practice if you are staying past 6pm every night catching up on week-old studies.

On the business

Downtime risks damaging a healthcare organization's reputation and erodes trust – it erodes the trust of hospitals and clinicians in the organization, which trickles down to an erosion of trust from patients.

A single organization's radiologists may read images for multiple hospitals. When that organization's PACS goes down, and providers and their patients withstand the worst of that downtime, it undermines trust in the radiologists' ability to deliver a timely diagnosis.

McFarland's experiences with downtime and Merge

For clinicians and IT, anxiety spikes when they experience downtime or see messages coming in from different sides of the business saying they're down. Imaging solutions without a good security infrastructure baked in are more liable to be at risk for ransomware, malware, and other cyberattacks that threaten even greater downtime.

What gives McFarland Clinic confidence in their systems staying up is Merge's proven track record in providing the proactive monitoring, maintenance, and architecture needed to ensure systems continually stay up with contingencies in place for when something happens.

McFarland has been working with Merge for over 10 years, with a lot of investment in understanding the ins and outs of solutions like Merge PACS, Merge Cardio, Merge Hemo, Merge Universal Viewer, and Merge VNA.

For all imaging organizations, the fears of downtime disrupting a clinician's workday and their home life pervade no matter where they practice. Clinicians are already burned out as is; unpredictability around downtime, and the actual downtime itself, further fuels that.

But taking this anxiety off the plate, thanks to solutions with built-in reliability and business continuity, can ease these pains and provide imaging organizations with more controllable, resilient environments – and consequently, more confidence.

"We work extremely well with Merge. We have confidence in the technology; replicating content management from the enterprise archive, with the PACS sitting on top and the virtual IP on the front end. If we ever do see issues with the PACS or our radiologists experience any slowdown, we can easily switch over to a Peer 2 PACS in a different data center within minutes, with minimal impact on the clinicians and support staff."

Eric Lehmkul
Director, IT, McFarland Clinic

RackTop and Security

A zero-trust approach to medical imaging.

Healthcare is a prime target for cyber attacks

Healthcare is one of the most ransomware-afflicted industries. As of 2021, it is the 7th highest targeted industry by ransomware groups, with an average remediation cost of $1.85m USD. These data breaches don't just hurt a hospital's bottom line; they can directly impact patient care. In fact, one out of four say mortality rates increase as a result of ransomware attacks.

80% of medical data is unstructured, and the vast majority of this data is for medical imaging. As a result, storage arrays are major targets for criminals stealing personal health information and holding it for ransoming.

Protecting data is critical to maintaining both clinicians' access to patient imaging data and patients' access to care. A zero-trust security model is critical for achieving that.

RACKTOP

Defining zero trust

What is zero-trust security? The framework for a zero-trust approach is comprised of five focus areas:

- **Identity:** Two-factor or multi-factor authentication (MFA) protocols used to verify a user's identity.
- **Device:** Antivirus software implemented on individual user devices.
- **Network or environment:** Firewalls deployed to protect entire organizational networks.
- **Application workload:** Securing workloads in a hybrid cloud.
- **Data:** For example, inspecting individual file transactions for compromised data.

Zero trust protects patient data by assuming no implicit trust for any user or application. Every transaction is inspected and either allowed, blocked, or flagged for individual review. Access to particular databases, apps, and environments is determined by an individual login basis; you are only able to access what you've been explicitly granted access to beforehand.

While most CISOs traditionally focus on network, device, and identity security – implementing measures like MFA – it's crucial to also protect the data itself.

How RackTop enables Merge solutions to adopt a zero-trust data-centric approach

An enterprise imaging strategy with zero-trust data security is a critical part of a comprehensive security plan, and the last line of defense against pernicious cyber threats like ransomware.

Merative's partnership with RackTop enables Merge imaging solutions to protect patient data and reduce cyber risk across healthcare. RackTop's BrickStor Security Platform follows a data-centric zero-trust model enabling organizations to actively defend unstructured data from ransomware, insider threats, and other cyberattacks. This protection is applied to Merge clients to help better safeguard high-value medical imaging files.

Here's how it works:

- **Proactive cybersecurity.** The RackTop platform actively defends and stops attacks in real time, reducing the threat window from months to minutes, to minimize the impact of a potential breach on both organization and patient.
- **Ensuring resilience during a breach.** Setting in place processes and continuity plans to continue providing patient care in the event of a breach. Utilizing technologies like immutable storage to ensure quick and safe recovery of affected data.
- **Identifying which data has been accessed.** Identifying who has unauthorized access to which data, when, and how. Both real-time and historical records enable IT teams to quickly recover affected data, while also informing the organization's leadership about what has been affected so that information about which data is at risk, and what has or hasn't been breached, can be transparently communicated to the public.

About Merative

Merative is a data, analytics and technology partner for the health industry, including providers, health plans, employers, life sciences companies and governments. With trusted technology and human expertise, Merative works with clients to drive real progress. Merative helps clients orient information and insights around the people they serve to improve decision-making and performance. Merative, formerly IBM Watson Health, became a new standalone company as part of Francisco Partners in 2022.
Learn more at www.merative.com

Produced in the United States of America
March, 2023

SM-1218 Rev 1.0