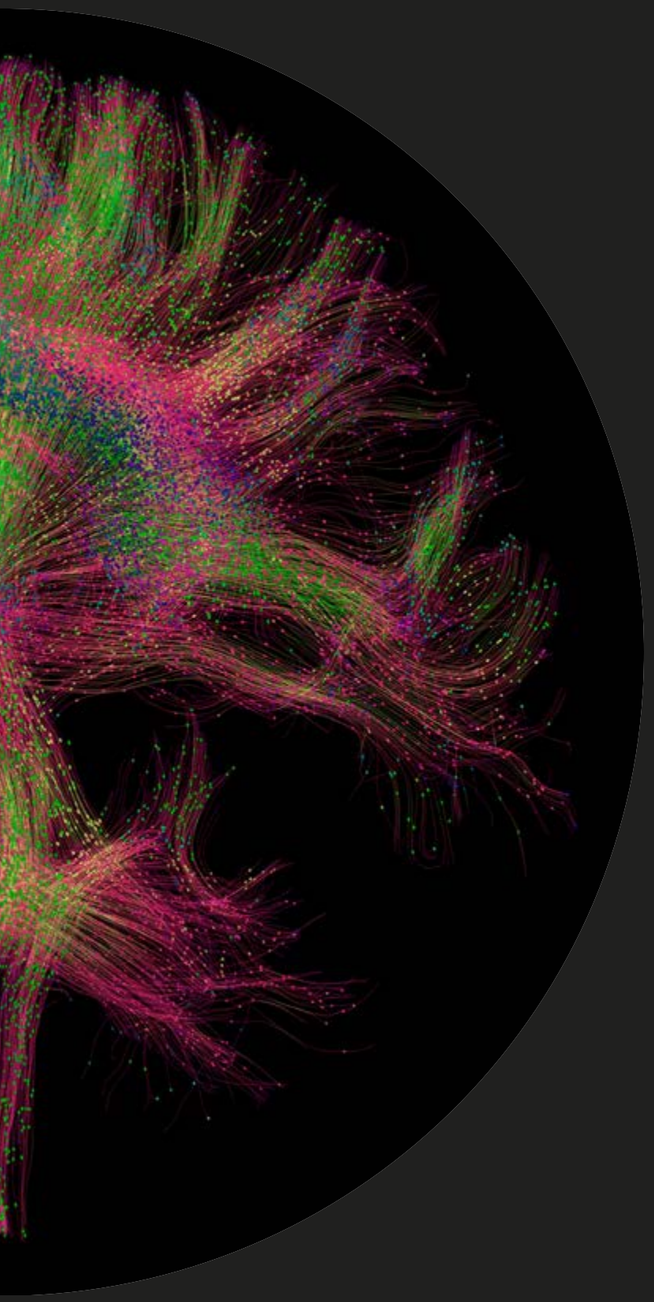

Merge

RackTop and cybersecurity

A zero-trust approach to medical imaging

merative

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.

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 provides data, analytics, and software for healthcare and government social services. With focused innovation and deep expertise, Merative works with providers, employers, health plans, governments, and life sciences companies to drive real progress. Merative helps clients orient information and insights around the people they serve to improve decision-making and performance.
Learn more at www.merative.com

About Merge

Merge medical imaging solutions, offered by Merative, combine intelligent, scalable imaging workflow tools with deep and broad expertise to help healthcare organizations improve their confidence in patient outcomes and optimize care delivery.
Learn more at merative.com/merge-imaging.

Produced in the United States of America
March 2024

Merge imaging solutions are manufactured by Merge Healthcare Incorporated, an affiliate of Merative US, LP
900 Walnut Ridge Drive, Hartland, WI USA 53029

SM-1456 Rev 1.0