From Ransomware to Resilience: Strengthening Security with IRE

Legacy Systems and Processes Can't Handle Ever-evolving Cyber Threats

As care moves from legacy systems to the cloud, finding and remediating security gaps is more important than ever. When an attack occurs, everyone is impacted—from doctors and staff to patients. The volume of personally identifiable information (PII) and other sensitive information in the healthcare sector has made it a valuable target for threat actors, especially ransomware attacks. Research from the Cyber Threat Intelligence Integration Center of the USA reports that from 2022 to 2023, ransomware attacks in the US against healthcare increased by 128%.[1] These attacks are costly, with healthcare organizations paying an average of $2.57 million in recovery costs in 2024.[2] With patients' lives at stake, healthcare organizations can't afford downtime.

The current cybersecurity landscape is rife with threats born out of malicious intent and exploitable vulnerabilities arising from disjointed systems, legacy technology, and outdated processes. Threat actors are no longer solely focused on compromising data but are disrupting systems relied on for recovery, increasing the pressure on healthcare organizations to comply with ransom demands. Legacy systems make this easier for threats, with outdated technology that is easy to exploit. Compounding this is the number of devices used in daily care, including computers, tablets, cell phones, and medical devices like heart monitors and MRI machines. As more logins are required and more devices are added, the result is security fatigue—poor security hygiene, such as reused passwords. This adds up to a perfect storm for threat actors.

Build Security in the Cloud With IRE

While you can't eliminate cyber threats, you can equip your organization with tools to increase prevention and minimize the impact of attacks, starting with a secure cloud environment on Amazon Web Services (AWS). If your organization is in the early phases of its cloud journey, you can ease the transition to the cloud by establishing an Isolated Recovery Environment (IRE). This provides a low-risk way to create an initial footprint in the cloud and allows your organization to develop cloud familiarity.

This new environment creates a mirrored replica of your production operational database, which can be utilized read-only or read-write. End users can access this environment using a browser or mobile application. This solution supports your overall resiliency to keep operations running smoothly, giving your IT team space to assess and disable the threat. With IRE, the entire healthcare organization can continue with business as usual without impact on patient care.

What Makes an IRE Low-risk?

Since IRE uses a designated network separate from any other environment, cloud servers supporting the environment are not joined to your main network. The only connection to your IRE is the production mirror duplicating EHR data between your on-premises and AWS IRE environments (figure 1). The goal is to ensure that data in your IRE location remains clean and uncompromised, allowing for a safe restoration or failover.

[1] Cyber Threat Intelligence Integration Center, Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double, Feb 2024.
[2] The HIPAA Journal, Healthcare Ransomware Attacks Continue to Increase in Number and Severity, Sept 2024

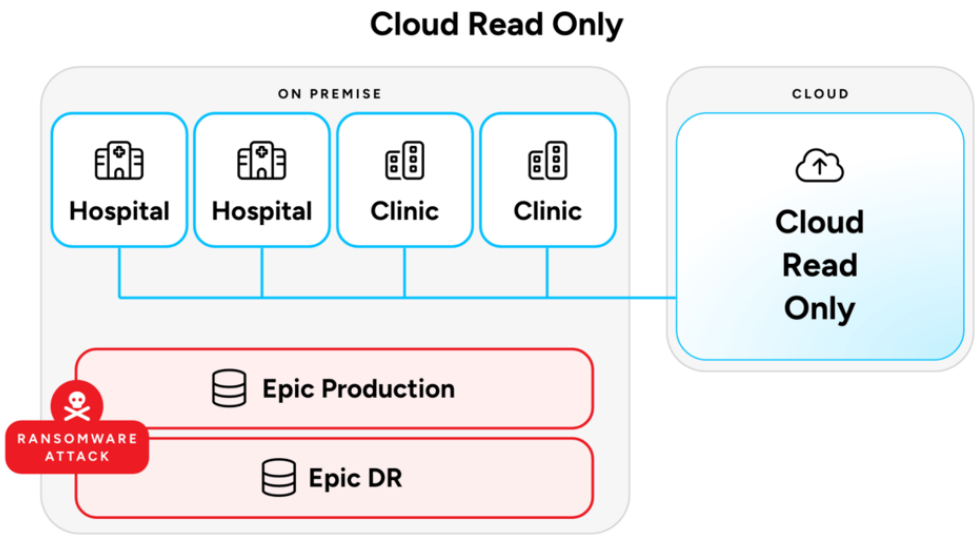

Figure 1

Increase Security While Moving Towards a Modern Cloud Environment

With an IRE in place, you can feel confident that you can recover from malicious attacks without sacrificing care or impacting staff. The IRE increases your security posture with an immutable, air-gapped version of your Epic® database. Your IT team benefits from an easier-to-manage, update, and scale environment that also serves as a "playground" for them to increase cloud confidence. The cloud helps keep IT budgets low, with no hardware to purchase, scalability to meet changing needs, and access to the latest cloud innovations and hardware.

Why Work with Sapphire Health and AWS For IRE?

Sapphire Health is well-versed in EHR migrations and AWS infrastructure, bringing the best of both worlds to every engagement. As part of their specialized expertise in migrating Epic® workloads to the cloud, Sapphire Health has proven experience and in-depth knowledge of the technical nuances that create a smooth journey from legacy data centers to the AWS Cloud.

Paired with their expertise in using powerful migration tools like the Landing Zone Accelerator (LZA) for Healthcare on AWS, Sapphire Health accelerates the implementation of an IRE. By reducing the heavy lifting of establishing a regulated cloud environment, Sapphire Health reduces the implement time of an IRE from months to weeks and can help organizations achieve an IRE activation time of minutes.

Sapphire Health speeds cloud adoption while creating a plan that works for your unique needs, resulting in an optimized and secure environment. With an AWS environment in place, you can successfully migrate additional workloads when ready and take advantage of AWS infrastructure's scalability, reliability, performance, flexibility, and compliance.

When you work with Sapphire Health, their implementation team covers all services from initial account creation to final test activation. Upon deployment, Sapphire Health fully manages regular updates, upgrades, and system maintenance, lessening the burden on your IT team. Should you need it, IRE read-only activation can happen in as little as 5 minutes. Once the decision is made to activate full read-write functionality, this additional step can also occur in 5 minutes.

Trust Sapphire Health with Your IRE Project

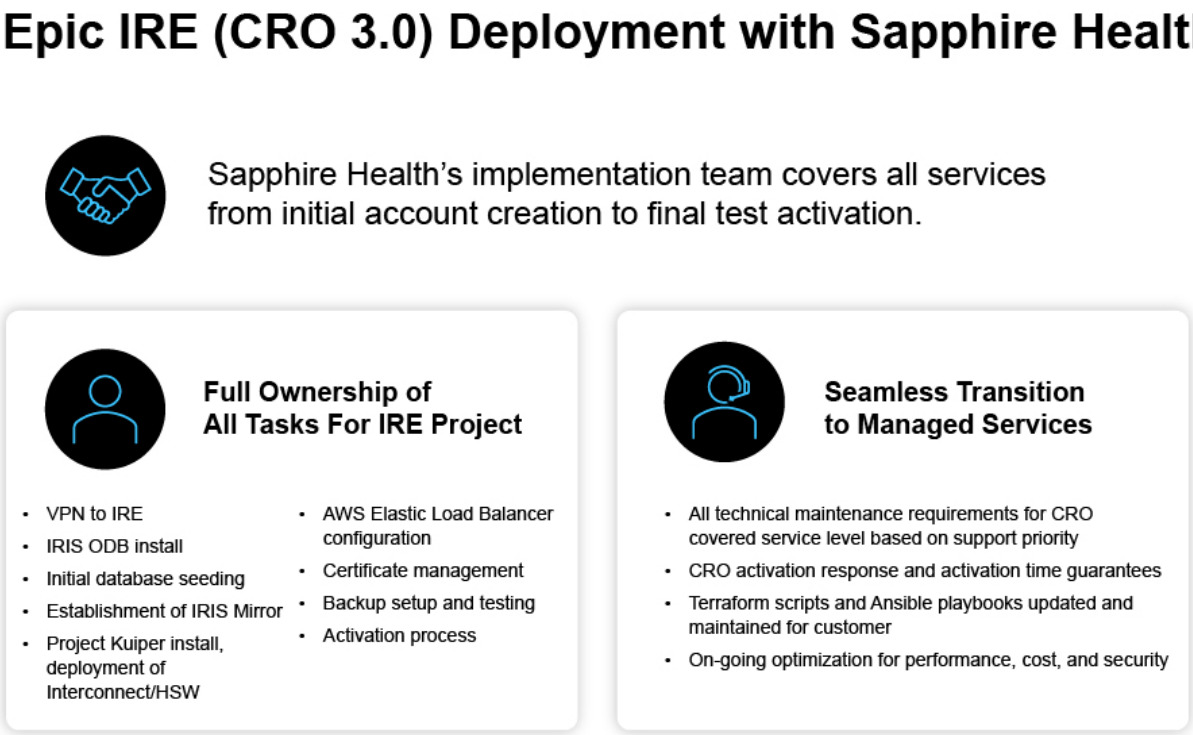

Figure 2: Sapphire Health manages your IRE deployment on AWS end-to-end and can offer further managed services to support your investment.

Cybersecurity is an every day, every hour, every minute consideration for running a healthcare organization. By equipping IRE, you can be confident that you can keep operations running during an attack. With Sapphire Health and AWS, you have partners that help you increase security, scalability, and compliance while taking the first steps to complete cloud migration.

Read the next blog to learn how to maximize your Epic® investment in the cloud.
To read the first blog in this series, please visit here.