SOLUTION BRIEF

Five Steps to Combat Ransomware in Healthcare

Safeguard patients and your business with modern data protection from Pure Storage®.

Recent ransomware attacks have crippled several hospitals across the world. U.S. government agencies have alerted the healthcare industry to expect increased attacks in the coming months. It's predicted that a new organization will fall victim to ransomware every 11 seconds by the end of 2021, according to Cybersecurity Ventures. Although hospitals have insurance policies to cover a portion of the costs of unlocking or decrypting data, these policies don't offer a guarantee or complete safety net. Plus, payouts may further encourage cyber criminals. In response, the U.S. Department of the Treasury is planning to impose civil penalties against hospitals or their agents that pay ransomware demands.

Ransomware Recovery Time Impacts Patient Care

When a ransomware attack disables a hospital's electronic health record (EHR) solution, the disruption can be widespread. EHR downtime caused by ransomware attacks hinders clinical decisions, creates the potential for medical errors, and could even be a contributing cause to a patient death.

Ransomware attacks on healthcare organizations encrypt not only EHR production databases, but also the backups that you use to recover from attacks. As the sophistication of these attacks increase, healthcare organizations need to address ransomware mitigation and recovery with a modern cyber protection strategy.

Level-up Your Cyber Protection with a Five-Step Framework

Ransomware Recovery

Pure FlashBlade® with SafeMode™ Snapshots accelerates ransomware recovery by augmenting data protection strategies.

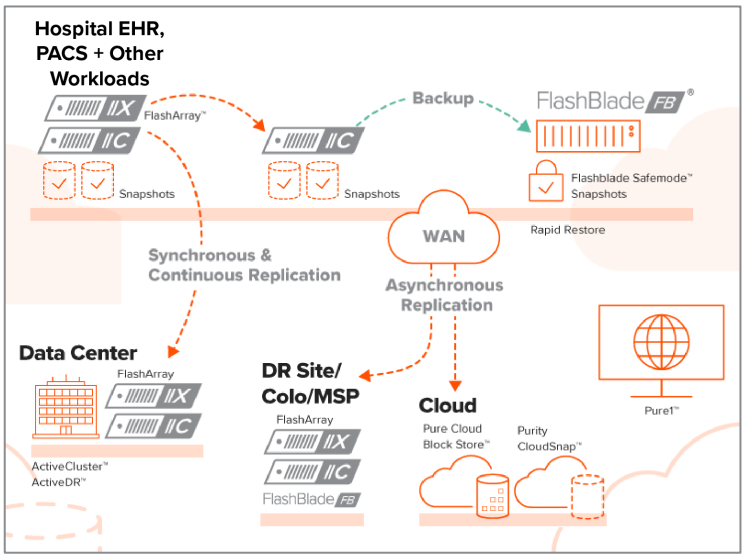
Data Protection

Introduce your organization to modern data protection and say goodbye to siloed legacy solutions.

Backup and Restore

Pure's modern architecture quickly backs up and restores data when it matters most.

Here are five steps you can take to safeguard your data against attack, and how Pure can help:



Step 1: Increase visibility. This step is all about knowing what equipment you have and why. That server that no one knows about sitting in your hospital basement just might be the most vulnerable link in your defense. Inventorying assets and points of entry are vital, as is monitoring events on each asset to find anomalies that might indicate intrusion.

- The Pure1 Meta® analytics platform synthesizes intelligence from thousands of devices.
- Combining Pure's FlashBlade® with Splunk or Elasticsearch creates a powerful data analytics and security platform.

Step 2: Ensure control. Put a virtual fence around your infrastructure to control access. The increase in distributed workforces and work-from-home policies require a new approach to cyber protection. Pure built FlashArray™ from the ground up to run VDI faster and with greater density than any other product on the market.

Step 3: Reduce exposure. This step isn't just about detection. It's also about building an environment that is consistently maintained and monitored, which requires collecting vast amounts of data for complex analytics. That's why it's important to have infrastructure that's architected to provide fast results.

- Take the assessment to see if your organization is prepared for the next ransomware attack.

Step 4: Increase the costs of attacks. Pure's SafeMode snapshots provide resiliency with immutable backups, making it impossible for an attacker or rogue insider to delete backups, even if administrator credentials have been compromised. Plus, SafeMode snapshots provide protection to your data if an attack occurs. Incorporating encryption makes it more difficult and costly for the attacker. At the 2019 RSA Conference, Pure Storage and Thales introduced Vormetric Transparent Encryption for Efficient Storage, the IT and security industries' first end-to-end data encryption framework that realizes storage array data reduction.

Step 5: Respond and evolve. Your ability to respond, recover, and evolve as quickly as possible following an attack is critical. Pure FlashRecover™, Powered by Cohesity®, the industry's first jointly architected all-flash modern data-protection solution delivers accelerated backup and rapid recovery at scale.

- Purity ActiveDR™ provides powerful data replication capabilities to ensure quick backups, and FlashBlade delivers rapid restore capabilities of up to 270TB/hour.
- For MEDITECH users, Pure has partnered with BridgeHead Software, Amazon Web Services (AWS), and Healthcare Triangle to deliver backup as-a-service (BaaS), which automates creation, storage, and replication of the MEDITECH backup to Pure Cloud Block Store™ in AWS.

PS1946-01 11/2020