PURESTORAGE®

Strengthening healthcare cyber resilience with an assume-breach approach

A primer on how healthcare data storage decisions help combat cyber attacks

Executive summary

Organizations fall victim to ransomware attacks every 14 seconds[1], and healthcare is a top target. Attackers recognize that system uptime is critical for providers, making them prime targets for extortion. Healthcare is rife with high-value data and intellectual property that can be sold on the dark web, creating a powerful incentive to end the attack. Paying the ransom might get back control of the system, but it doesn't end the pain. Long-term issues including reputational damage, lost revenue, lawsuits, and potentially regulatory penalties can extend the damage for years after an attack.

Healthcare organizations often rely on a defensive strategy to combat the growing threat of ransomware. A strong security defense works—until it doesn't. That's why it's critical for healthcare organizations to take an "assume breach" approach and prepare for what happens after the inevitable attack.

In this dossier, we will discuss the most common types of attacks affecting healthcare today, the short- and long-term ramifications of an attack, and why healthcare organizations need to embrace a proactive approach. We'll also address how Pure Storage can help organizations plan and prepare.

Healthcare is a prime target for ransomware attacks

Healthcare organizations generate large volumes of regulated data, a favorite target for attackers. There are two primary threat types being wielded against the healthcare industry today:

Encryption-based ransomware

Malware is triggered in the system, locking up access to critical information such as electronic health records (EHR) and imaging data, effectively freezing operations.

Data exfiltration

Attackers download sensitive data and/or intellectual property with the intent of extorting the organization and/or selling it on the dark web.

There are countless stories about organizations that have had their systems compromised or data breached. What those stories don't discuss are the broader ramifications of an attack. Without access to the to the Electronic Health Record (EHR) or Picture Archiving and Communications System (PACS), patient care is likely to slow or cease. This downtime can effectively freeze operations.

Once the system is back online, the organization will need to pay a third-party to conduct a forensic investigation and cleanse data and systems, which involves yet more downtime. Then there's the extended impact of the breach: reputational damage, lost revenue, and potential lawsuits and/or regulatory fines. Taken together, the long-term damage can reach billions of dollars. It's important to stand firm, however. Organizations that succumb to ransom demands not only reward attackers but also make themselves a stronger target for future attacks. In the next section, we'll discuss how to prepare for a breach—without preparing to pay the ransom.

Ransomware attacks are rising at alarming rates worldwide and show no signs of subsiding.

- Companies paid more than **$1.1B** for ransoms in 2023[2]
- Cyberattacks increased **30%** worldwide in 2025[1]
- The healthcare industry averages **1,999** attacks per week[1]

The case for cyber resilience

While healthcare providers may believe they are prepared to recover from a disaster, that's just partially true. Traditional disaster recovery (DR) systems create an up-to-date, exact copy of the organization's real-time data. In the event a server fails, or a data center goes down, IT can failover to the replicated systems to resume operations.

With a ransomware attack, IT has additional challenges to deal with beyond failing over to another data center: They must eliminate the threat, find and restore clean data, and perform forensics to determine how the attack happened and what data was accessed and potentially stolen.

Traditional disaster recovery systems were designed to keep the DR copy of the data as closely updated to production as possible. This is not ideal for dealing with an encryption event, however, as the DR copy will almost immediately become encrypted and is useless for recovery. Additionally, these systems do not typically have any mechanisms to prevent a privileged user from destroying the data, again rendering the DR system useless for recovery.

A cyber resilient solution maintains safe copies of an organization's data, ensuring data is available for restoration efforts. Start by developing a plan and ensuring the right infrastructure is in place to minimize the potential damage of an attack—and update plans regularly, as attack trends are constantly evolving.

Key challenges for the cyber resilient enterprise

Data resilience:

- Threat actors will seek to destroy backup data
- Data is susceptible to privileged access attacks

Security performance:

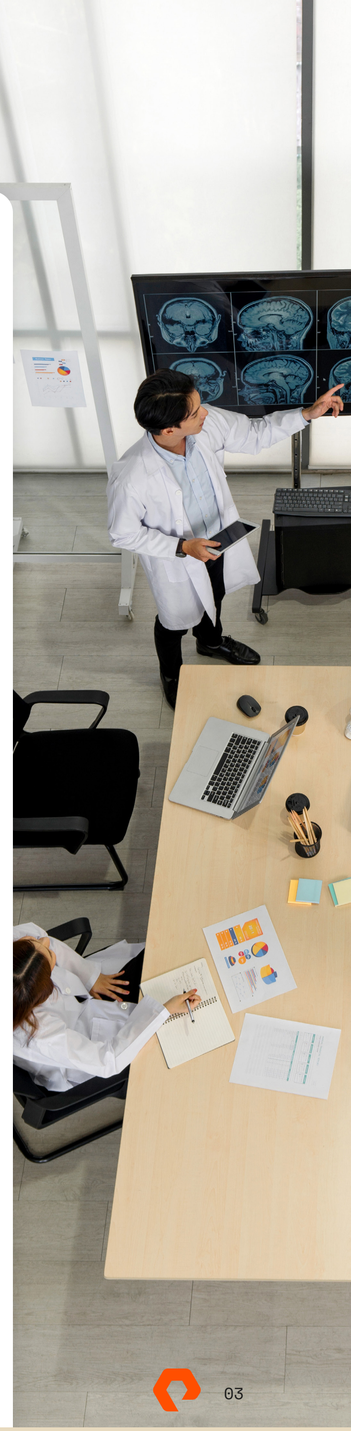
- Attack detection (SIEM, UEBA) cannot keep up with volume
- SIEM, UEBA need visibility for all critical storage

Recovery layering:

- Primary data centers could be compromised or unavailable
- Data RTO and RPOs vary significantly

Recovery performance:

- Multi-step cyber recovery requires ultra-fast data movement
- Recovery may require moving extremely large data sets



Preparing to recover from attack

A posture of cyber resilience helps ensure healthcare providers can withstand and recover from attacks. A resilient approach incorporates robust data protection mechanisms, incident response planning, and adaptive technologies to recover from attacks minimizing downtime and reducing the impact of the attack. Internal education may also help employees understand the difference between disaster recovery, cybersecurity, and cyber resilience.

The right solution:

Provides fast access to critical patient data:

Expedite access to patient data for faster diagnosis, treatment, and data recovery for EHR applications.

Improves cyber resilience:

Reduce cyber vulnerabilities and help ensure data availability and integrity for patient data and records.

Reduces storage costs:

Drive operational and cost efficiencies across your business to reduce TCO.

Facilitates compliance:

Reduce potential risk exposure with data monitoring and manage compliance requirements with encryption at-rest and in-flight.

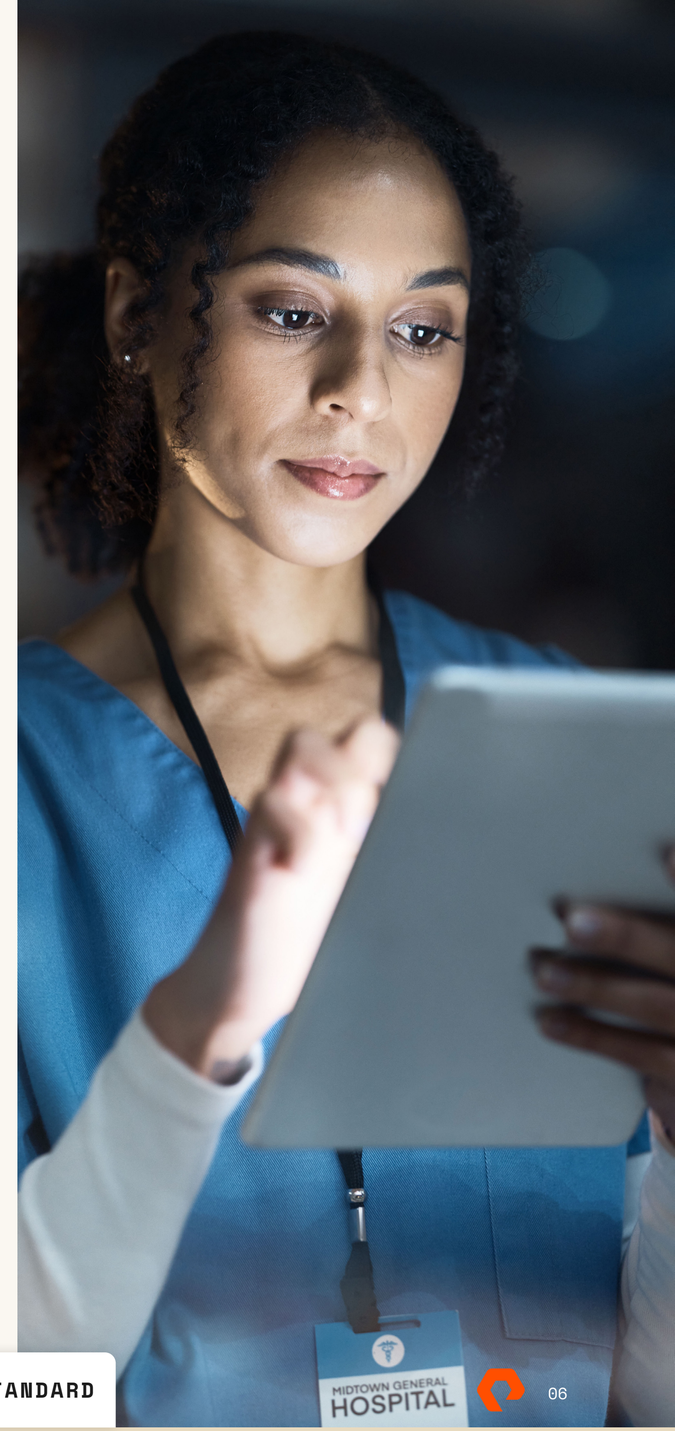
What happens next/what to watch for

It’s important that everyone in your organization understands cyber resilience, why it matters, and how it differs from disaster recovery.

CISO	IT Operations Manager	Compliance Officer	Data Scientist / Analytics Team Lead	Biomedical / Imaging Systems Administrator
If an attacker encrypted your EHR data today, how quickly could you restore operations without reinfecting your environment?	When was the last time you tested your recovery plan—and did it include a real cyberattack scenario?	Could you prove to regulators that patient data integrity was maintained after an attack?	What would happen to ongoing AI or research workloads if your data was corrupted or unavailable for weeks?	If your PACS or imaging servers were encrypted, how quickly could radiologists access historical images again?
Pure Storage provides immutable and indelible, verifiable recovery points and isolated recovery zones so that restoration happens quickly and safely without repeating infection cycles.	**Pure Storage enables regular, automated validation of recovery plans, so systems can be restored from clean copies under real-world conditions.**	**Pure Storage helps ensure recoverability that meets privacy and compliance mandates.**	**Pure Storage resilient solutions provide fast, reliable data restoration and version integrity across environments.**	**Pure Storage enables rapid restoration of imaging archives and associated metadata, reducing clinical downtime and diagnostic delays.**

The difference between what you have vs. what you actually need

Data resilience:	Reality	Pure Storage
We have backups; we can just restore if needed.	Your backup may contain the malware that started this (opportunity for repeat attack). Recovery can take days or weeks.	**Pure Storage SafeMode™ Snapshots are immutable and indelible, providing data integrity and fast access for incident responders.** **Multiple versions can be instantly cloned for forensic validation and recovery.**
Backups are stored safely in the cloud	Cloud repositories can be accessed through compromised credentials, allowing attackers to delete or encrypt remote data copies just as easily as on-premises copies. Bringing data back on-premises from the cloud dramatically increases restore time.	**Pure's SafeMode and Object Lock features protect cloud and on-premises data from modification or deletion, even by administrators.**
Cyber insurance will cover our financial losses	Insurance may not cover regulatory fines, lost patients, or long-term share price decline. Premiums rise sharply after a breach.	**Pure's Cyber Resilience solutions reduce downtime and reputational risk, helping demonstrate proactive controls that lower insurance exposure.**



Where to go from here

Healthcare organizations must assume breach and prepare to recover from an attack with a cyber resilience solution that maintains safe copies of data to recover systems quickly so providers can return to their primary function of patient care.

To learn more about how Pure Storage can help your organization safeguard patient data, visit https://www.purestorage.com/solutions/cyber-resilience.html.

purestorage.com

800.379.PURE

PURESTORAGE®

1. 83 Cybersecurity Statistics 2025 (Worldwide Data & Trends), Demandsage, July 24, 2025
2. Ransomware Payments Hit a Record $1.1 Billion in 2023, Wired, February 7, 2024