ABSTRACT

With cyberthreats becoming more sophisticated and damaging, healthcare organizations need to take extraordinary measures to protect their most vital patient, financial, and operational data. This white paper explains how the EMC Isolated Recovery Solution enhances your current cybersecurity capabilities as part of a layered data protection strategy. It also highlights best practice recommendations for planning, implementing, and validating a complete and secure solution. By following these guidelines, healthcare providers can mount a strong, effective defense against cybercriminals to ensure business continuity and deliver on their primary mission to provide quality patient care without disruption.

July, 2016
# TABLE OF CONTENTS

## EXECUTIVE SUMMARY

## INTRODUCTION

## THREE-LAYERED APPROACH TO DATA PROTECTION

The Foundational Layer

Extended hardening Creates Rock-Solid Security

Guarding against Destructive Attacks

## KEEP CRITICAL PATIENT DATA SAFE

Secure Vault for Your Most Critical Data

Flexible Approaches to Match your Data Protection Objectives

Protecting Enterprise Storage using Replication

Isolating Data Backups

Point-In-Time Recovery Strategy

## BOLSTER YOUR SUCCESS WITH AN EXPERT SERVICES PARTNER

## START HIGH ON THE LEARNING CURVE

## ADVANCED DATA PROTECTION BEST PRACTICES

Assess your Current Health IT Environment and Readiness

Develop a Detailed Plan for Isolated Recovery

Implement The Solution With Strict Governance

## CONCLUSION

## ADDITIONAL RESOURCES
EXECUTIVE SUMMARY

As healthcare organizations accelerate their use of technology to improve patient care delivery, they face critical challenges in keeping ePHI highly available, protected, and secure. Recently, healthcare providers have confronted a growing wave of destructive, malicious attacks from a new breed of cybercriminals who target clinical and financial data for its high value. Such attacks, such as fraud, identify theft, and ransomware, healthcare organizations can be completely locked out of their systems. These security breaches stem from a variety of sources including malicious insiders, phishing, ransomware, malware, advanced persistent threats, and denial of service.

A disruptive intrusion often can begin silently as it slips into your servers and databases and then encrypts critical data, holding this information “hostage” until the cybercriminal demands that your organization pay a ransom. Not only can these breaches disrupt clinical workflow for hours or even days, but they can negatively affect hospital revenue streams and organizational reputation, and even receive national media attention. At worst, patient lives can be at stake.

Two-thirds of healthcare respondents in the HIMSS Cybersecurity Survey reported a significant security incident in the recent past with 64 percent noting an incident had been conducted by an external actor such as an online scam artist or hacker, or through social engineering. In addition, the 2016 Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data by the Ponemon Institute estimated the average cost of data breaches for healthcare organizations over the last two years at more than $2.2 million per breach with criminal attacks as the leading cause.

With this current landscape in mind, healthcare IT leaders have ranked security and data protection as a top organizational priority. Meanwhile, an IDC report forecasts that healthcare data is expected to grow 48 percent per year through 2020 from a variety of information sources, including clinical applications, advanced medical imaging, Internet-enabled medical devices, next-generation sequencing, and remote patient monitoring.

This white paper presents an innovative approach with advanced tools to help minimize risks and vulnerabilities related to cyberattacks, as well as further strengthen organizational compliance with HIPAA, HITECH, and EU Data Protection Directives. The paper highlights deployment of a comprehensive and layered data protection strategy to further safeguard clinical and operational systems that combine traditional backup and replication approaches with additional hardening techniques and advanced data protection using the EMC Isolated Recovery Solution. It also details key features and capabilities of the solution, along with best practice recommendations for planning, implementing, and validating an effective and secure deployment.

The EMC Isolated Recovery Solution provides a stronghold for your most critical patient, financial, and operational data to further augment administrative, physical, and technical safeguards. The offering creates a secure vault to protect critical data with an isolated environment without any active network links or way for intruders to breach. Along with hidden point-in-time copies, the solution employs isolation or an “air gap” to enable data recovery as a last line of defense from malicious attacks. In addition, the EMC Isolated Recovery Solution provides healthcare organizations with plans and measures to undertake when combating active attacks.

By following guidelines outlined in this paper, healthcare providers can modernize and strengthen their data protection and security strategies to better prevent and manage potential cyberthreats that may impact the healthcare ecosystem. The EMC Isolated Recovery Solution provides vital assurance that clinical systems and medical information will be accessible and recoverable to ensure continuity of operations.

---

1Source: 2015 HIMSS Cybersecurity Survey, HIMSS, May 2016
2Source: Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute LLC, May 2016
3Source: The Digital Universe Driving Data Growth in Healthcare, IDC and EMC Corporation, 2014
4Source: EU data protection directives, European Union, June 2016
INTRODUCTION

As growing incidents of malware attacks become the “new normal,” healthcare providers need to reexamine their security and data protection strategies and plans beyond firewalls, end-point protection, and anti-virus and anti-malware software. The 2016 RSA Cybersecurity Poverty Index\(^5\) reported that just 27% of healthcare respondents rated themselves as having “developed or advantaged” cybersecurity maturity and practices, including incident response and risk identification. (Figure 1) These statistics highlight opportunities for improvement.

**Figure 1. RSA Cybersecurity Poverty Index**

In today’s evolving threat environment, cybercriminals have become highly sophisticated, advancing well beyond data theft and denial of service. Security incidents and ransomware is on the rise—with clever attacks that can encrypt your data, hold it hostage, or even aim all-out data destruction of files, database internals and complete systems.

According to the Ponemon Institute\(^6\) personally identifiable healthcare information makes an especially attractive target to hackers with an U.S. average cost per healthcare breach of $398 per exposed record and a worldwide per record cost of $363. Healthcare represented the highest per record cost across all of the industries, which is calculated at an average cost of $154 per record. This higher per healthcare record cost is due to the depth of information associated with identity and medical identity theft.

The lengths that cybercriminals will go to inflict damage on healthcare systems also have increased. No longer satisfied to breach only your production data, these attack points can reach deep into backup systems and archives, a physician’s smart phone, a patient’s mobile heart monitor, or any laptop, PC, server, and specialty device across the enterprise. One of the primary reasons healthcare organizations are so vulnerable to these types of attacks is the sheer number of interconnected devices used in the everyday care of patients with each device representing a potential port of entry.

The impact of these attacks also can be costly—both operationally and financially with potential interruptions to patient care delivery. As an example, imagine the impacts of an entire EHR database being taken over and rendered inoperable by ransomware—or worse, destroyed by a malicious cyberattack. Even if recovery from a backup was possible, clinical workflow, including patient diagnosis and treatment plans, would be severely hindered. Everything from office appointments to surgeries, allergies to certain medicines, and lab work would be slower until the recovery from backup was complete. If the backup database were to be compromised as well, patients may need to be sent to another facility. In the direst of circumstances, patients’ health would be impacted negatively.

\(^5\)Source: RSA Cybersecurity Poverty Index, RSA, 2016

With stringent requirements from HIPAA, HITECH, and the EU Data Protection Directives, healthcare providers need solutions that minimize risk; detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent identity theft, fraud, and cybercrime. And, to combat growing cyberthreats and preserve the integrity of the health IT infrastructure, CIOs and CISOs must take a comprehensive approach to security and establish plans to address as many scenarios as possible. EMC’s portfolio of trusted IT solutions for healthcare providers, including advanced security analytics, data protection, and continuous availability of applications and data, can help your organization focus on a layered data protection approach with a recovery plan for today’s digital environment.

The maturity of your trusted IT framework also must be considered including:

- What are the key business and clinical applications critical to patient workflow, such as biomed applications that run heart pumps, ventilators, nurse calling stations, and operating rooms?
- What about EMR, PACS, and other applications?
- What is the state of traditional data protection, such as backup and replication?
- Have you deployed extended hardening to include security policies and procedures, as well as encryption of data in flight and at rest?
- Where do you stand with extended protection, including security analytics and isolated recovery?

In particular, isolated recovery capabilities should become a vital part of your holistic security and data protection strategy. Isolated recovery provides methodologies and processes to limit penetration to strategic health system digital assets, keeping the most critical data separated from your active infrastructure—both production and backup systems. Using this approach, the solution physically and logically isolates protected information and systems from external cyberthreats. Simply put, cybercriminals cannot exploit what they cannot see. In many cases, an isolated recovery solution also can be built with existing infrastructure investments.

With the deployment of an isolated recovery solution, healthcare organizations can achieve dramatic improvements in business resiliency in the face of potentially devastating cyberattacks as your most critical data will be preserved even if production environments and backups are both destroyed. Isolated recovery represents your strongest defense against the most advanced cyberthreats and best assurance of preserving operations that are vital to patient care.

THREE-LAYERED APPROACH TO DATA PROTECTION

To ensure the most complete, effective protection of organizational healthcare data, EMC recommends deployment of a layered data protection strategy that spans traditional backup and recovery, incorporates additional hardening and security features, and provides advanced protection capabilities with isolated recovery. (Figure 2) EMC and its strategically aligned businesses offer a portfolio of solutions and technologies to help thwart cyberattacks, limit their impact and proliferation, and most important, enable rapid recovery following an intrusion to ensure continuity of clinical and business functions.

Figure 2. Layered Data Protection Strategy

For assured protection given today’s sophisticated and persistent cyberthreats, EMC advises healthcare organizations to incorporate the following solutions and best practices into their overall data protection strategy.
THE FOUNDATIONAL LAYER

As a foundational layer of protection, comprehensive backup and recovery for critical clinical and business applications, including virtualized environments and archived data, are essential. Replication across local and geographically dispersed data centers further ensure trusted disaster recovery and business continuity.

To advance this risk-reduction approach, continuous bidirectional synchronous and asynchronous replication needs to be included with multiple recovery points to restore critical applications to a specific point in time. In addition, every data protection strategy must include regularly scheduled testing of backup, replication, and recovery procedures. To learn more about the full suite of EMC data protection offerings and value they can provide to your organization, refer to EMC Data Protection Suite Family Overview video and EMC Data Protection Suite solution overview.

EXTENDED HARDENING CREATES ROCK-SOLID SECURITY

With regulatory requirements to secure and protect ePHI, healthcare organizations need to take more comprehensive measures to harden the overall data protection environment in their role as covered entities. EMC provides specific hardening guides for each of our data protection solutions by addressing passwords, certificates, unused ports, FTP, and unnecessary services.

In addition, hardening techniques need to be applied to your network. For example, ports need to be closed that are not absolutely needed and firewall policies set to block files from unknown or untrusted sources. In addition, network traffic must be segmented so users can only access data relevant to their job functions and multi-tier applications must be able to access compartmentalized databases.

It’s also important to embed security wherever possible by encrypting data in flight and at rest. In virtualized environments, solutions such as VMware NSX should be implemented, which makes security functionality an integral part of the hypervisor and enables micro-segmentation within the data center.

User education and policy enforcement also are essential to strengthening data protection across the healthcare ecosystem. Clinical and administrative staff need to be engaged in security best practices training, regular password reset procedures should be instituted, antivirus and security software must be continuously updated, and retention lock software that provides immutable file locking and data retention capabilities should be deployed.

Close controls over provisioning and de-provisioning of user accounts for network and data access are also paramount. Significant network intrusions often occur via stale and unused network accounts that still provide access to active network resources, such as file servers and applications.

GUARDING AGAINST DESTRUCTIVE ATTACKS

To guard against dire scenarios where cybercriminals attempt to destroy vital clinical records or maliciously encrypt critical data to render it useless, EMC recommends implementation of an Isolated Recovery Solution. This solution extends your data protection strategy focusing on three levels of control: prevention, detection, and recovery. It is applicable to systems and data that are absolutely essential to maintaining viable operations within healthcare delivery organizations.

When considering an Isolated Recovery Solution, it is best to begin by assessing the current state of your trusted IT infrastructure. This risk-based approach will help provide insight into which systems, clinical and business applications, and data are most critical to continuity of operations across the continuum of care. A thorough assessment also will help determine whether you have the necessary infrastructure components and what new capabilities may be needed to configure an Isolated Recovery Solution.

Based on this assessment, your team then can develop a detailed plan to fill technology gaps and address critical recovery requirements to meet your specific operational and clinical requirements. EMC offers pre-packaged, comprehensive professional services to assist with assessment, planning, implementation, testing, and validation of an Isolated Recovery Solution. Should your organization choose to handle solution planning and deployment internally, EMC recommends engaging our data protection and security experts to provide further subject matter expertise, objective testing, and validation of reliable and consistent data recovery.

7Source: Health Information Privacy, U.S. Department of Health & Human Services website
In addition, EMC recommends incorporating advanced security analytics, such as RSA Security Analytics, into your overall data protection strategy. This solution provides added assurance by helping security analysts detect and investigate potential cyberthreats that may be overlooked by other security tools.

**KEEP CRITICAL PATIENT DATA SAFE**

In battling the latest generation of advanced cyberthreats, your primary objective must be to ensure business continuity and access to patient information by authorized caregivers. Imagine a scenario where patient data is completely unrecoverable. In these cases, an affected institution may not recover from such a malicious event.

The EMC Isolated Recovery Solution is differentiated from other data protection strategies as it provides healthcare organizations with an extra level of confidence through a last line of defense that their most vital clinical systems and patient records will be protected from advanced intrusions.

Should your organization experience a cyberattack that has disabled or destroyed primary data sources, the solution provides an isolated, secured copy of designated data in an “off the grid” data vault. When necessary, this offline vault can be reconnected to your production network in minutes to recover data and resume business operations.

EMC’s air gap feature enables the Isolated Recovery Solution to intermittently connect and disconnect from your network. The air gap connects network ports momentarily, only to allow synchronization, and then immediately disengages connection to maintain isolation of the protected data. This process can be fully automated to minimize administration overhead.

The Isolated Recovery Solution offers easy integration with EMC and non-EMC technologies, becoming a critical component of a holistic data protection and security strategy across your entire healthcare organization. In many cases, you can build an Isolated Recovery Solution using infrastructure components already in your environment. This reduces upfront costs and streamlines implementation.

**SECURE VAULT FOR YOUR MOST CRITICAL DATA**

The Isolated Recovery Solution comprises an environment that is physically disconnected from production systems, applications, and data. This creates a secure vault where your most important data is kept invisible and inaccessible from the network and would-be attackers. (Figure 3)

**Figure 3. Isolated Recovery Solution Components**

![Diagram of Isolated Recovery Solution Components](image)

Data is periodically copied from production storage or backup systems to the isolated environment across the air gap. This dedicated connection opens only to allow synchronization and then closes immediately to maintain isolation. To provide additional security, EMC recommends zoned Fibre Channel or port-limited LAN connections to the vault.
Inside the vault, the Isolated Recovery Solution maintains "gold" copies of your protected data, including multiple restore points. It includes automated processes to update and validate these gold copies, managed by validation hosts. These hosts perform logical and physical integrity checks on data copies before creating gold (fail-safe) copies that are protected from access by cybercriminals and available for recovery if needed.

Management of the protection process always occurs from within the isolated environment. EMC recommends hardened security practices that permit only a few highly trusted personnel to oversee operation and management of the Isolated Recovery Solution. Access controls are implemented to prevent any external manipulation of components in the vault. EMC also recommends protection of data protection assets, such as the backup system, through network controls that only allow access from specific and restricted network segments to reduce the attack vector.

FLEXIBLE APPROACHES TO MATCH YOUR DATA PROTECTION OBJECTIVES

The Isolated Recovery Solution provides flexibility to enable protection based on your recovery objective, budget, and existing infrastructure. For example, fastest recovery is achieved when synchronizing enterprise storage between production systems and a target system in the vault. Alternatively, synchronizing backup systems may be more economical and still satisfy your business recovery requirements. There are many possibilities incorporating EMC or non-EMC systems. Here are a few examples:

PROTECTING ENTERPRISE STORAGE USING REPLICATION

Isolated recovery can be achieved between two VMAX enterprise storage systems using EMC SRDF replication. In this configuration, one VMAX array is in production and a second is located in the vault on an isolated network connected to the recovery, management, and validation hosts. EMC SnapVX copies are used as restore points. Generally, organizations will continue to maintain replication of the production VMAX array to an additional VMAX system in a separate site for disaster recovery.

The protection process follows a simple routine:

- Open the air gap to enable the link and invoke SRDF replication of critical data from the production VMAX system to the isolated VMAX system
- Close the air gap to disable the link between the production and isolated systems
- Perform an integrity check of replicated data in the vault, and move validated data to the gold copy

This process can be repeated multiple times over a 24-hour period based on your recovery point objectives. Should recovery be necessary, open the air gap and enable failback via the recovery hosts.

ISOLATING DATA BACKUPS

Similar to the VMAX storage scenario, data isolation also can be achieved across EMC Data Domain backup systems. (Figure 4) This approach can address protection requirements for critical data residing on either EMC or non-EMC storage. Restore times will be longer.

**Figure 4. Isolated Recovery Using Data Domain**
In this environment, Data Domain replication synchronizes data between production and isolated systems. The protection process is as follows:

- Create a data backup on Data Domain
- Open the air gap to enable the link and invoke Data Domain replication from the production backup to the isolated system
- Close the air gap to disable the link between the production and isolated systems

Healthcare organizations can use Data Domain Fast Copy to provide multiple copies and additional protection of data in the vault. Once these operations are complete, administrators should validate integrity of the most recent copies to ensure none of the data was corrupted during transfer.

To recover, open the air gap to re-establish the link with the production or disaster recovery network, and configure Data Domain for client access.

**POINT-IN-TIME RECOVERY STRATEGY**

Another approach is to use EMC RecoverPoint to create data isolation from VMAX, VNX, XtremIO, or VPLEX systems. In this case, RecoverPoint Appliances are deployed in the vault with a Fibre Channel link over the air gap to the production systems. (Figure 5)

**Figure 5. Isolated Recovery Using RecoverPoint**

This solution incorporates the following process:

- Open the air gap from within the vault through the RecoverPoint appliances
- Transfer the data using RecoverPoint and verify data integrity using the validation hosts
- Create and verify an array-based copy of the data
- Close the air gap through the RecoverPoint appliances

Standard failover procedures can be followed if a recovery copy of data is needed. This solution is best deployed when point-in-time recovery is required for multi-site environments needing remote replication, and when both local and remote replication is desired.

**BOLSTER YOUR SUCCESS WITH AN EXPERT SERVICES PARTNER**

While internal healthcare IT teams may be able to plan and implement an Isolated Recovery Solution, there are distinct advantages to working with a services partner that provides subject matter expertise in data protection. EMC offers broad industry knowledge that spans all aspects of data protection tools in a healthcare environment along with in-depth healthcare application experience. This valuable combination can help reduce the time to implement an effective Isolated Recovery Solution, avoid many common pitfalls, as well as aid in establishing or enhancing business continuity and technology plans.

EMC offers a proven methodology that follows industry best practices for delivering the Isolated Recovery Solution. It’s part of a comprehensive framework that includes advisory and implementation services. (Figure 6)
With this comprehensive service offering, EMC will fully assess your environment and work with your organization to identify all potential attack points across your health system. In addition, EMC will help you determine which applications and data require isolated protection and advise on your overall organizational readiness to defend against a cyberattack. We then will develop a detailed plan, including protection objectives, data classifications, recommended protection techniques, and recovery procedures.

EMC also will professionally manage the implementation of the Isolated Recovery Solution, ensuring that all technology components, processes, and controls are properly deployed. And, we will validate the solution, performing synchronization, verification, and recovery tests to ensure the solution meets your business continuity requirements. We also can engage with your risk management and compliance teams to ensure solutions meet corporate business needs and are properly integrated into continuity plans.

**START HIGH ON THE LEARNING CURVE**

Drawing on our experience designing and implementing advanced data protection solutions for thousands of healthcare providers around the world, EMC eliminates the steep learning curve that would be required by your internal IT staff. Instead, our data protection experts are productive on day one and equipped to move your project forward quickly and efficiently.

We also bring a significant body of healthcare industry knowledge of the full roster of clinical and administrative applications, including electronic medical records (EMRs), picture archiving and communication systems (PACS), patient accounting systems, lab, pharmacy, and numerous others. EMC consultants also are well versed in healthcare regulations for ePHI, including HIPAA, HITECH, and EU Data Protection Directives. With this broad subject matter expertise, our team can take a holistic view of your clinical operations and IT infrastructure to recommend the best approach to protect your most critical data and ensure compliance.

When you engage EMC’s seasoned services team, there's no guesswork. You can be confident the Isolated Recovery Solution was planned, configured, and implemented correctly. We provide documented validation, which means your organization can be confident that your most vital information is protected to endure the most aggressive cyberattacks. This assures your clinicians and administrative staff can continue to provide services with minimal impact on patient care.
ADVANCED DATA PROTECTION BEST PRACTICES

Based on our deep expertise in data protection strategies and solutions with healthcare organizations, EMC has developed a set of best practice recommendations to ensure a successful outcome. Organizations may choose to engage with EMC's Isolated Recovery Services team to ensure strict adherence to these best practices or follow guidelines independently.

ASSESS YOUR CURRENT HEALTH IT ENVIRONMENT AND READINESS

The first essential step is to ensure that you understand vulnerabilities across your healthcare organization within the current security landscape and that basic security hygiene has been applied. For example, LANs and vLANS should be segregated with no Internet access, all unused network ports should be turned off, and hardened policies and procedures should be put in place for everything from password management to administrative access.

A complete assessment will include defining requirements for compliance, application protection, and cybersecurity governance. This includes performing an in-depth analysis and prioritization of critical applications and data, determining where they reside in the infrastructure, and deciding if their location is optimal based on their criticality to the organization.

Next, you should identify the most critical business and clinical applications and data to be included in the Isolated Recovery Solution. This also should include determining the amount of data requiring isolated protection, along with checkpoints and deduplication expectations.

As an added level of security assurance, EMC recommends conducting a thorough production storage hardening audit, complete with HIPAA risk assessment and intrusion stress testing.

DEVELOP A DETAILED PLAN FOR ISOLATED RECOVERY

Planning for the Isolated Recovery Solution starts with establishing key metrics that go beyond traditional recovery time and recovery point objectives. Given the increasing sophistication of cyberthreats, EMC recommends also determining a Destruction Detection Objective (DDO) and Destruction Assessment Objective (DAO). The DDO specifies how much time may elapse before your organization is able to detect that data destruction has begun. The DAO is the amount of time allowed to identify the specific type of cyberattack and effective remediation.

Exceeding the DAO, for instance, would typically activate recovery procedures through the Isolated Recovery Solution. To plan for this scenario, you also should develop isolated recovery point and isolated recovery time objectives. Additional key metrics include the checkpoint interval and checkpoint count for the Isolated Recovery Solution—both critical to ensuring the integrity of protected data in the isolated vault.

An essential part of the planning process is classifying the data to be protected. Typically, this will include three categories of data: executables, transaction data, and read-only data (intellectual property and historical data).

The next step is to architect the Isolated Recovery Solution based on key metrics and protection requirements established for each class of data. In addition, EMC recommends choosing techniques to validate and verify protected data in the vault. Some common examples include running a transaction report against your database records to uncover any anomalies, or generating a report on sentinel records, which would uncover unauthorized changes to data values. Other techniques include performing checksums of executables, scanning data at rest for malware, or comparing daily backup image size against established norms.

Other important aspects of planning should include creating a detailed recovery plan, such as a capabilities matrix and recovery orchestration model, as well as performing a gap analysis to determine where additional capabilities are needed. In addition, EMC recommends developing a business case for the solution based on cost, revenue loss, insurance offset, and damage to reputation.

IMPLEMENT THE SOLUTION WITH STRICT GOVERNANCE

When implementing the Isolated Recovery Solution, EMC recommends establishing strict governance, access policies, vault operational guidelines, and recovery procedures. This should include training for IT staff.

A key component of the implementation process also requires creating a detailed architectural design, including network links, air gap, and vault systems (restore hosts, validation hosts, and management hosts). Technology deployment should include hardening and production storage remediation. You also will need to create Isolated Recovery solution runbooks based on the orchestration model, along with procedures for maintaining proper security hygiene and performing periodic health checks on the solution.
VALIDATE THE ISOLATED RECOVERY SOLUTION

Validation of the Isolated Recovery Solution should be an ongoing activity. EMC recommends running solution integration and isolated recovery tests periodically. To continually ensure data integrity, healthcare organizations also should institute daily monitoring of backups, data copies, gold copies, and restore points.

Given the widespread threat of cyberattacks, EMC also advises healthcare organizations to educate all clinical and administrative staff on security best practices. In addition, trusted staff overseeing the Isolated Recovery Solution should receive regular training on the latest threats, security hygiene recommendations, and data protection strategies.

CONCLUSION

With the volume of online patient data continuing to grow, cybersecurity is a top priority for today’s health IT leaders. Given the growing wave and sophistication of today’s cyberthreats, healthcare organizations must take extraordinary precautions to defend against attacks that could ultimately disable critical systems, destroy patient data, and disrupt and endanger patient care.

While traditional security approaches such as firewalls and anti-malware solutions are fundamentally important, healthcare organizations must embrace a comprehensive layered approach to data protection. This includes traditional backup and replication processes, as well as additional hardening techniques such as encrypting data in flight and at rest. Even so, persistent hackers can still break through these measures. As such, EMC recommends more advanced data protection strategies and tools, including isolated recovery.

The EMC Isolated Recovery Solution keeps your most critical and valued data out of reach from cybercriminals. By housing this data in a secure vault, disconnected from your network or the Internet, the Isolated Recovery Solution provides a fail-safe means to ensure business continuity even if both your production and backup systems have been breached. This comprehensive solution offers added insurance to protect your healthcare organization from the worst possible cyberattack scenarios—one that disrupts clinical workflow where patient care may be compromised.

Many of the underlying technologies required to build the Isolated Recovery Solution may already exist within your IT infrastructure, potentially reducing upfront investment. Successful implementation of an Isolated Recovery Solution requires knowing where vulnerabilities exist and creating a strategic plan to address them. This includes a technology configuration based on your organization’s unique recovery requirements, along with proper security hygiene across your network, storage and backup environments, as well as strict governance over data access and administration.

With thorough planning, the right technologies, and comprehensive security policies and procedures, healthcare organizations can further reduce their risk and vulnerability with the EMC Isolated Recovery Solution. As a result, you can demonstrate that your organization has the confidence and resilience to withstand advanced cyberattacks and ransomware, as well as ensure that clinicians and administrators have safe, reliable access to the systems and information required to deliver uninterrupted and quality patient care.

Finally, as with any security and data protection solution, it is vital that your organization can trust the partners that are delivering advanced technology services to the most sensitive and critical parts of your enterprise. EMC and our partners are committed to serving as trusted partners in the securing and protection of your most critical health system data.

ADDITIONAL RESOURCES

EMC Isolated Recovery Solution: http://www.emc.com/microsites/isolated-recovery-solution/index.htm

EMC Security: www.EMC.com/security
