



Three Ransomware Readiness Essentials for Healthcare Providers

The Healthcare Blueprint to Ransomware Data Protection

Table of Contents

Introduction: 2

The rapid evolution of ransomware: 3

The growing impact on healthcare: 4

Raising the threat level: 5

Three data protection essentials: 6

Managed security services from GM Sectec: 7

Introduction

Ransomware is an unwelcome reality in the digital universe, and a growing concern in highly regulated industries, such as healthcare. No individual or institution is immune, requiring providers to strategize on how to keep their valuable and sensitive data safe.

In fact, the healthcare industry has long been a focal point for cyberattack, as more than 1,500 healthcare organizations experienced successful ransomware attacks since 2016.¹ These attacks only intensified with the onslaught of the coronavirus pandemic. Bad actors opportunistically targeted overwhelmed providers who had become vulnerable to attack during their pandemic response efforts. In the first ten months of 2020,

fifty-nine (59) US health providers or systems were impacted by ransomware, affecting patient care in about 510 facilities.² And in September 2020, the first known fatality of ransomware was recorded in Duesseldorf, Germany when a cyberattack forced the transfer of critically ill patients to another city.³

While ransomware is here to stay, it's not all doom and gloom. With a proactive and multi-faceted approach to data protection, healthcare institutions can mitigate the risk of data loss and deliver a high-level of business continuity in the face of new and emerging threats.

The rapid evolution of ransomware

Many security experts compare protecting digital assets to securing a home. However, bad actors don't just walk through your front door; they use any means possible to gain access while going undetected.


Cyberattacks have become a very sophisticated form of digital organized crime and are no longer a lone wolf practice. Attackers understand the value of sensitive data and use it as leverage in their extortion. Ransomware, a type of malware attack, can use phishing spam and social engineering to access victims' resources. It takes over a part, or all of an IT environment, encrypting and denying access to critical data. Attackers then typically demand a ransom in exchange for decrypting the data and returning it to a usable format. But it doesn't stop there. Emerging technologies are breeding new and advanced forms of ransomware, as bad actors can more effectively mine for security loopholes and exploit them.

Without sufficient protection, ransomware victims have almost no maneuvering margin, often being forced to dispense high payouts or manage costly downtime for their business. For healthcare institutions, ransoms can cost providers tens of thousands of dollars to re-gain access to files and their network.⁴ Others have been less fortunate, as cybercriminals have demanded more than \$10m in ransom per healthcare facility.⁵ In some instances, paying a ransom isn't even enough, as some bad actors refuse to restore data even after payouts had been issued.



The growing impact on healthcare

The impact of ransomware-triggered shutdowns of healthcare facilities jeopardizes patient's records, personal data, and drastically impacts the ability to administer care. The effect is profound on the victim organizations, especially in the first year following the attack. The lasting adverse effects can drain revenue and extend far beyond just monetary loss, often resulting in a loss of patient confidence and trust, damaging harmful exposure and potential liabilities and lawsuits.



Accelerating cyberattacks. Healthcare providers must defend against an unbelievably high number of cyberattacks expected to reach an attack every 11 seconds.⁶ IT teams can no longer handle the incoming threats without automation and an AI-based cybersecurity posture as volume of attacks surge.

High payouts. It is not surprising that the more sensitive the data, the higher the price tag. It is estimated that ransomware payouts are expected to reach \$20B by the end of 2020.⁷ For regulated industries like healthcare, patient and operational data is not just valuable, it can jeopardize lives.

Costly downtimes. Healthcare disruptions of any kind are expensive and can impact organizations with stretched IT resources beyond their limits. Ransomware attacks shake the foundation of an organization and raise doubts about its ability to protect patients and their private data. Malicious attacks also expose healthcare providers to potentially costly liabilities and harmful exposure. It is estimated that the average cost of downtime doubled to \$283,000 in 2020.⁸

Failure to comply. As a regulated industry, many regulations govern the healthcare industry's operations and handling of patients' data, privacy protection, reporting and many more. A cyberattack could expose organizations to potential failure to meet regulatory compliance requirements, causing costly and lengthy distracting audits and reporting.

Reputation damage. In the aftermath of a ransomware attack, a provider's reputation can be irretrievably harmed, with patients losing trust and taking on a negative view of the provider's brand and causing loss of patient loyalty with a long-lasting adverse impact.

Raising the threat level

As in the case of many other traditional business sectors, the healthcare industry is ripe for disruption. Today's providers face new internal and external factors that further complicate safeguarding patient data from cyberattacks. Internal conditions, such as fragmented internal productivity tools, separate applications and support for different facilities and disparate data storage properties, increase the targets that attackers can seek. Combined with new, sophisticated ransomware tactics, this only further increase risk of data loss.

Threat #1

Data Sprawl and Silos

More data in more places introduce new vulnerabilities, especially with an increasingly remote workforce and rapid endpoint device expansion.

Threat #2

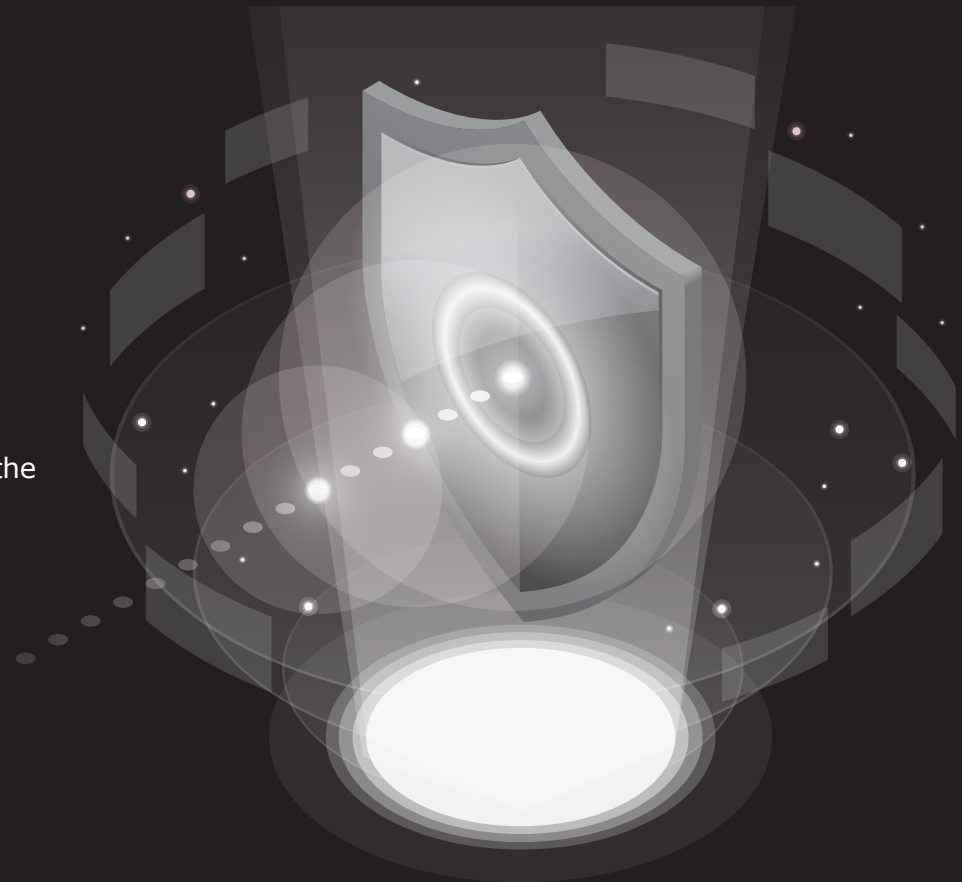
Cybercrime Activity

Ransomware attacks and other cybercrime is consistently growing to pace the expansion of technological advances and new tools.

Threat #3

Rapid Tech Advancements

New software applications and hardware platforms are being created and implemented faster than protective solutions.



An edge-to-cloud robust data protection strategy is essential for the efficient protection of valuable data.

Three data protection essentials

A robust security and data protection strategy falls within three main categories: denying unwarranted access to data, maintaining data integrity and enabling for rapid recovery after a malicious attack. These three elements are essential in ransomware readiness for healthcare providers. This multi-faceted approach not only proactively reduces the risk of attack, but also institutes best practices and controls to effectively recover data at scale.

Protection



Advanced security. A sound data protection strategy starts at its foundation. Hardened security and zero-trust access controls, including multifactor authentication, advanced data encryption and privacy locks, limit authorized access to data. They can also instill stringent security standards and privacy protocols (including HIPAA, ISO27001, GDPR and SOC 2).

Detection. AI-powered anomaly detection provides capabilities that spot suspicious activity before ransomware can successfully access data. By recognizing anomalous activities, users and administrators are notified of abnormal file pattern behavior and can proactively prevent a breach.

Backed by proven infrastructure. Cybersecurity experts should support trusted data protection solutions and adhere to global, regional, government and industry compliance. This approach establishes durability, scale, and performance as a critical component in the foundation of your backup solutions.

Preservation



Backup immutability. While malicious attacks can encrypt business data in production environments, separate and immutable backups maintain a protected data copy in an isolated location. This ensures backup copies of data can be preserved and are not subject to being altered or deleted in the event of a breach. Isolated backups not only protect patient and operational data, but can support potential compliance audits and defending against liability claims.

Air-gapped service. While isolated backups securely store copies of your data from bad actors, it is also imperative that your backup service (itself) remains air-gapped. This is a critical but often overlooked element, as both backup and restore operations should be separate and not susceptible to ransomware attacks that successfully penetrate customer environments.

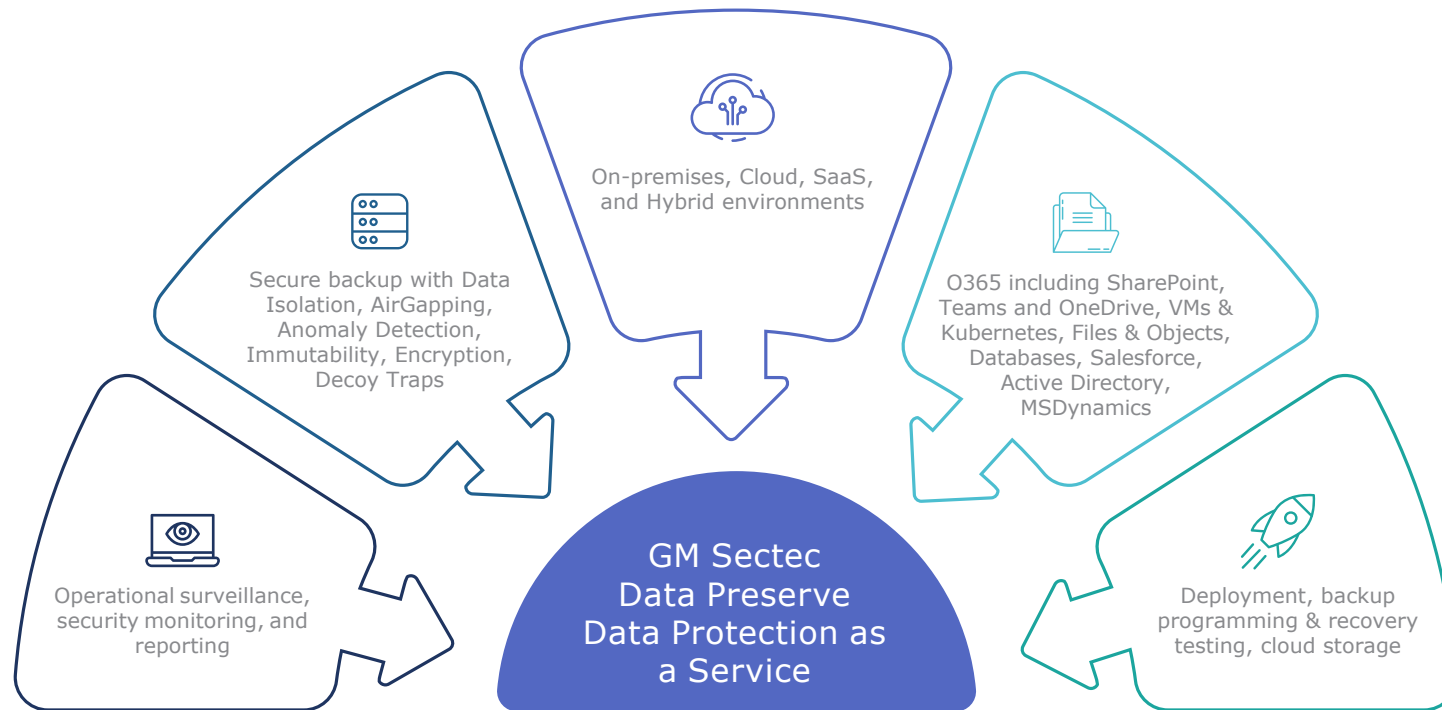
Recovery



High performance. Your solution should support the rapid recovery of data. Features such as built-in deduplication, compression and bandwidth optimization eliminate redundancies while ensuring data copies are highly available for quick and reliable restoration. The fast recovery reduces costly downtime and helps meet recovery SLAs. Rapid recovery is most critical for healthcare providers as disruptions impact operations and threaten the livelihood of patients and cause widespread loss of trust withing the patients and their communities.

Speed and precision. Granular search and flexible recovery options enable faster recovery with accuracy. A cloud-based control dashboard allows admins to restore their data even if they lose the production environment.

GM Sectec managed security services



Managed security services for ransomware readiness and prevention

Providing an essential combination of data monitoring and threat detection, response, and recovery, GM Sectec provides managed security services to safeguard your Healthcare organization's entire technology stack. With the simplicity of SaaS, GM Sectec DataPreserve powered by Metallic® provides multi-layered, zero-trust, air-gapped security to immutably protect your organization's entire technology stack across all environments. With a proven playbook to deploy enterprise-wide backup and recovery services and establish and test recovery objectives and priorities, GM Sectec provides the staff, knowledge, and facilities to deliver data protection resiliency with 24x7x365 operational surveillance and security monitoring and reporting. Leverage GM Sectec to meet HIPAA compliance requirements by standardizing a secure backup for EMR and ePHI data and files. Pair the leading data protection technology with the leading managed security services to securely backup critical workloads, identify and block ransomware threats, and rapidly restore data to avoid costly downtime and instill stronger business continuity.

Copyright 2022 Commvault Systems, Inc. All rights reserved. Metallic, Metallic and the "M Wave" logo, and the "M Wave" logo are the trademarks or registered trademarks of Commvault Systems, Inc. All third-party brands, product names, service names, trademarks or registered trademarks are the property of and used to identify the products or services of their respective owners.

Sources:

1. [Health IT Security](#) February 2020. "Ransomware attacks cost healthcare sector at least \$160m since 2016."
- 2, 3, 5: AP October 29, 2020. "FBI Warns ransomware assault threatens US health care system."
4. Center for Internet Security 2020. "Ransomware: In the Healthcare Sector."
6. EmsiSoft Malware Lab 2019. "State of Ransomware in the US, 2019 Report"
7. <https://www.Thesslstore.Com/blog/ransomware-statistics>
8. <https://purplesec.us/resources/cyber-security-statistics/ransomware/>