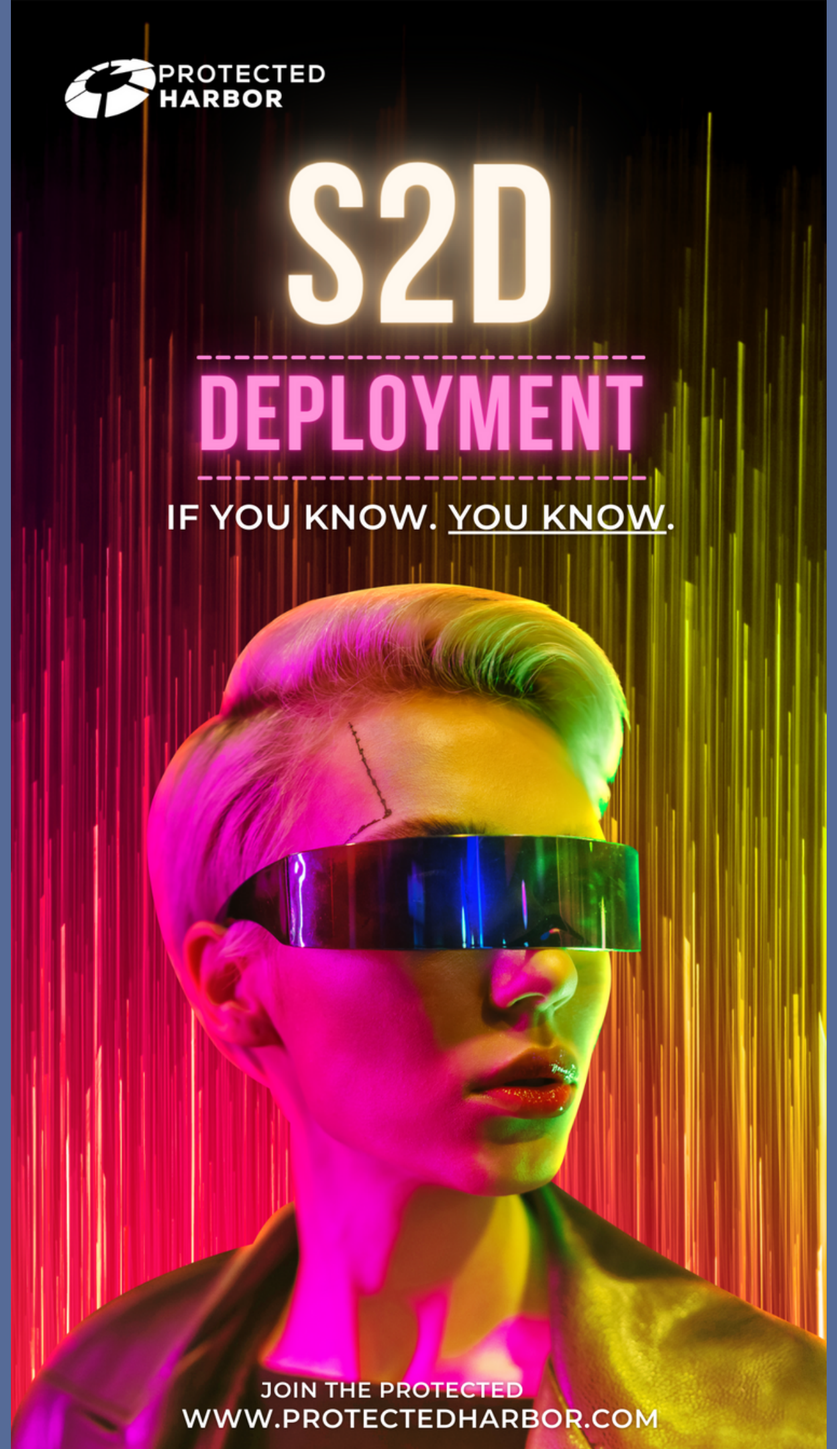
PROTECTED HARBOR

CYBERSECURITY RISKS OF 3RD PARTY CLOUD-APPS IN 2022

Stopping Healthcare Data Breaches via 3rd Party Platform Vulnerabilities



CONTENTS

INTRODUCTION

The healthcare cybersecurity market will be worth an estimated $26.1 billion by 2027, according to a study conducted by Meticulous Research. Large-scale cloud adoption paired with increasingly complex cyber threats, drives the demand for advanced cybersecurity risk protection in healthcare.

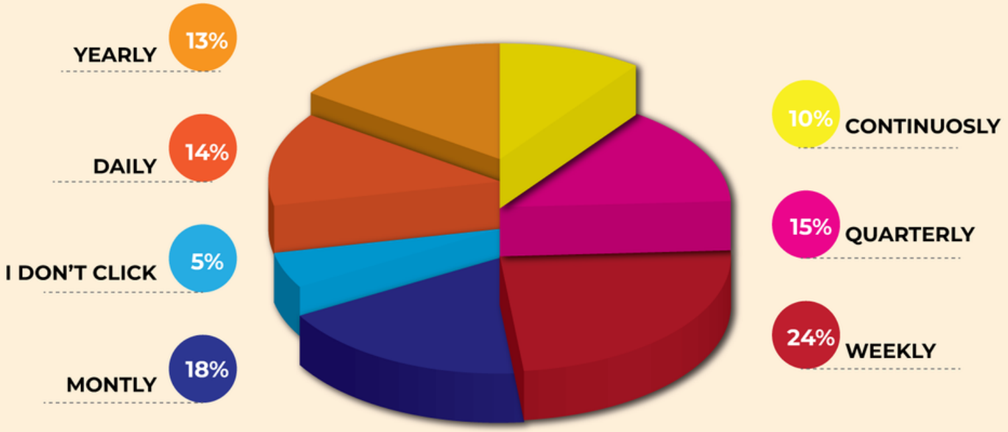
Due to the pressure of handling sensitive patient data; healthcare organizations must balance embracing cloud adoption to transform the delivery and accessibility of healthcare services against the legal and reputational ramifications of data hacks.

The Department of Health and Human Services' Office for Civil Rights' breach portal shows over 240 healthcare data breaches of 500 or more records in 2022. 15% of those have come through third-party business associates. However, many cloud and third-party apps are not classified as business associates under HIPAA (Health Insurance Portability and Insurance Act) nor are they required to adhere to HIPAA security standards.

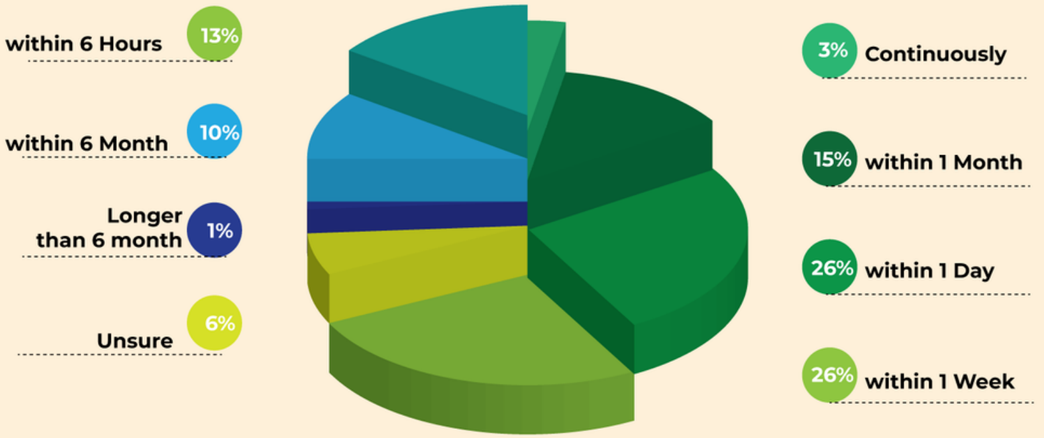
In September of 2021, the Federal Trade Commission (FTC) issued a policy statement affirming that health apps and connected devices that collect or use consumers' health information must comply with the Health Breach Notification Rule. Yet, there are still too few privacy protections for these apps.

Health organizations, large and small, are prime targets for cybercrime. With the growing number of healthcare-related cyberattacks, smaller healthcare providers are falling victim to cybercriminals at an increasing rate.

Frequency of SaaS sequrity configration checks*



Length of time to fix SaaS misconfigrations*



01.

TOP 3 CYBERSECURITY THREATS

As the frequency of cyber-attacks increase, it becomes essential to stay protected. Ransomware is one of the biggest concerns as it can shut down critical systems, disrupt business, and steal valuable data. Phishing emails as well as unauthorized access are among other ways to lose data and fall victim to identity theft.

MALICIOUS NETWORK TRAFFIC

Privilege misuse, web applications, and miscellaneous errors account for 81% of cybersecurity incidents in healthcare, according to a 2019 report by Verizon. Although this type of malicious network traffic might not be as coordinated as an all-out ransomware attack, its prevalence in the industry should put healthcare providers on high alert.

Unauthorized downloads, apps, and websites allow malicious actors to move laterally within a provider's network, leading to costly breaches and service interruptions.

Many healthcare organizations are adopting cloud-based services to improve patient care and collaboration. However, these cloud-based apps can also show vulnerability to malicious network traffic.

RANSOMWARE ATTACKS

Ransomware is a type of malware attack in which the attacker locks and encrypts a victim's data and critical files, then demands a payment to unlock and decrypt them. This leaves the victims at the mercy of the attacker once the *ransom* is paid.

In late October 2020, CISA (Cybersecurity and Infrastructure Security Agency), HHS (United States Department of Health and Human Services), and the FBI (Federal Bureau of Investigation) released a joint report detailing how ransomware becomes increasingly intricate when deployed in healthcare settings. For example, malware loaders such as TrickBot and BazaarLoader deploy popular ransomware like Ryuk and Conti via phishing emails and drive-by downloads.

PHISHING SCAMS

Phishing refers to correspondence that appears to be from a trusted source, like a mortgage company or government portal, asking for sensitive information. This usually includes a personal identity number, login credentials, as well as payment details.

Medical school can’t prepare you for everything. From doctors and nurses to patients, recent data shows that all parties within the healthcare system are susceptible to dangerous phishing scams. Emails, social media, or even phone attempts to deploy harmful files are often the precursor to widespread ransomware attacks.

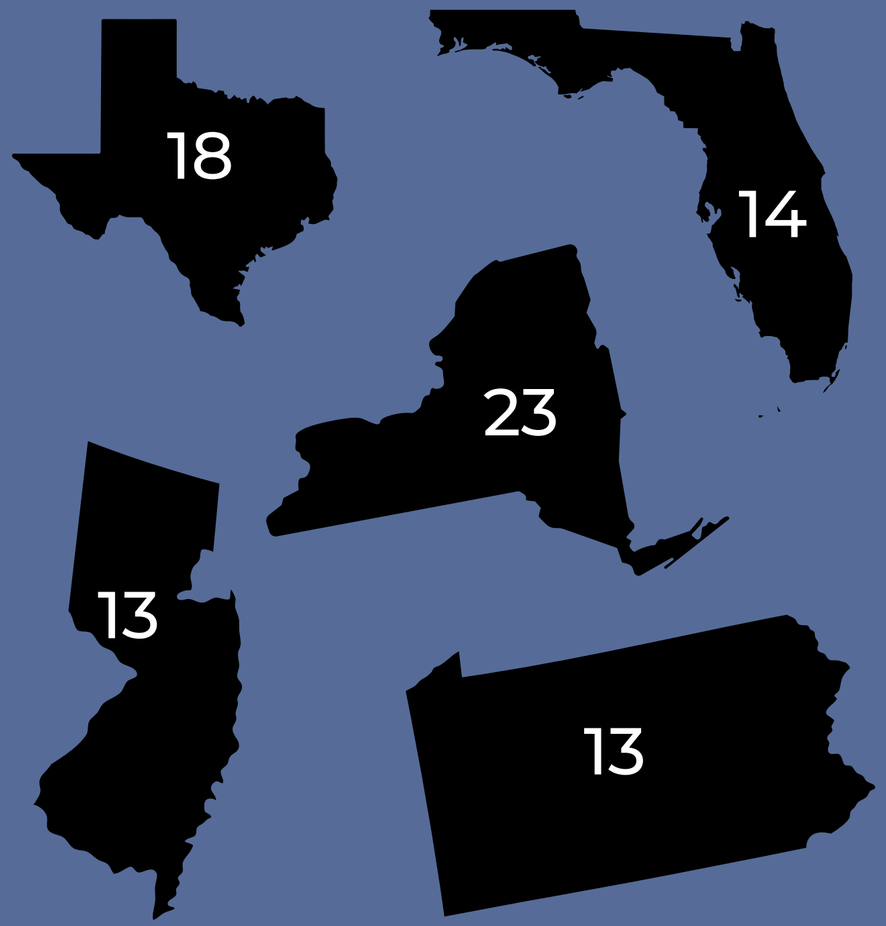
02.

Q1-Q2 2022 DATA BREACH TRENDS

So far in 2022, there were over 240 healthcare data breaches and over more than 500 records, reported to the HHS. That resulted in 10,783,906 individual health records being compromised within a six-month period between January-June 2022. An overwhelming 71% of breaches have been via hacking incidents.

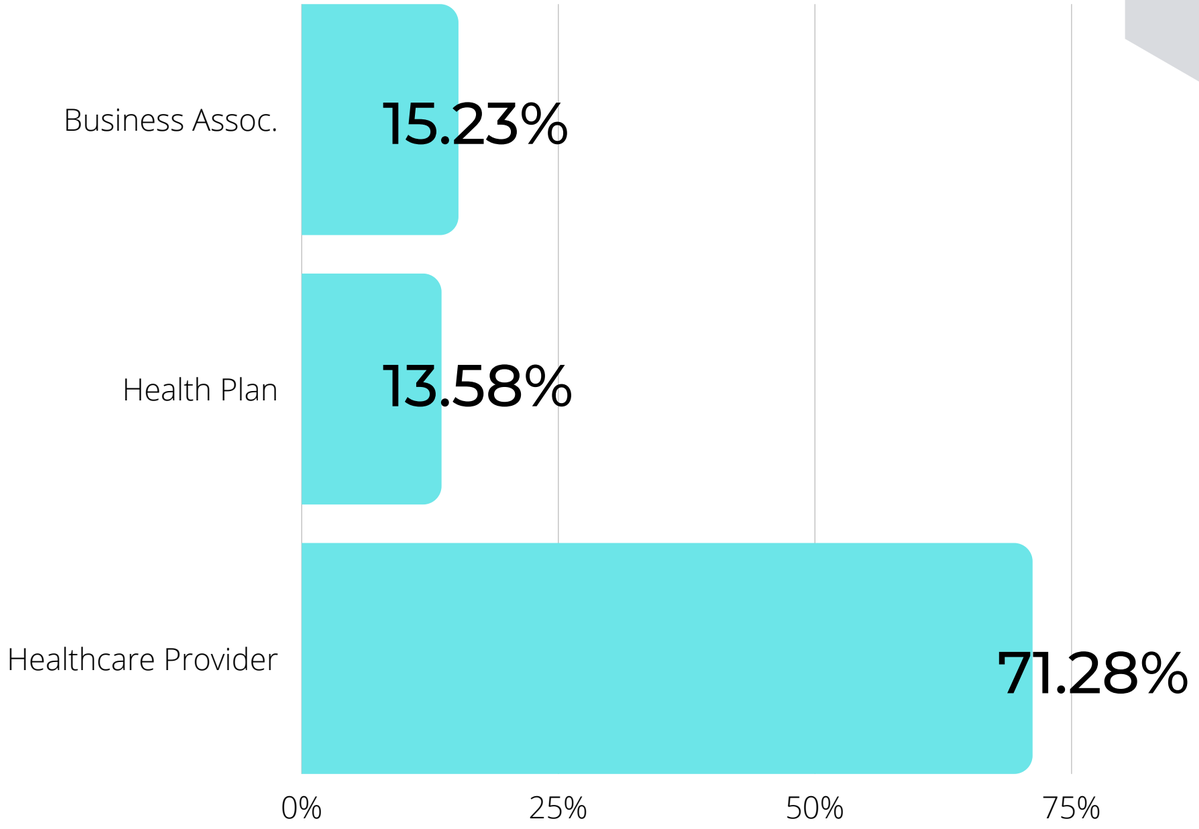
But a growing 17% have been due to unauthorized access incidents which is the most common breach type regarding data loss via third-party apps. One example is when the Boston-based medical billing company Medical Healthcare Solutions (MHS) hack affected the Beth Israel Deaconess Medical Center. The same happened to the Colorado Department of Human Services (CDHS) when third-party vendor Sound Generations had encrypted information hacked, causing CDHS to send a breach notification to over 6,000 individuals. It wasn't MHS or CDHS that caused the breach, however, they were still considered responsible for it.

WHERE ARE THE ATTACKS HAPPENING?



OF ATTACKS PER STATE IN Q1&2 2022

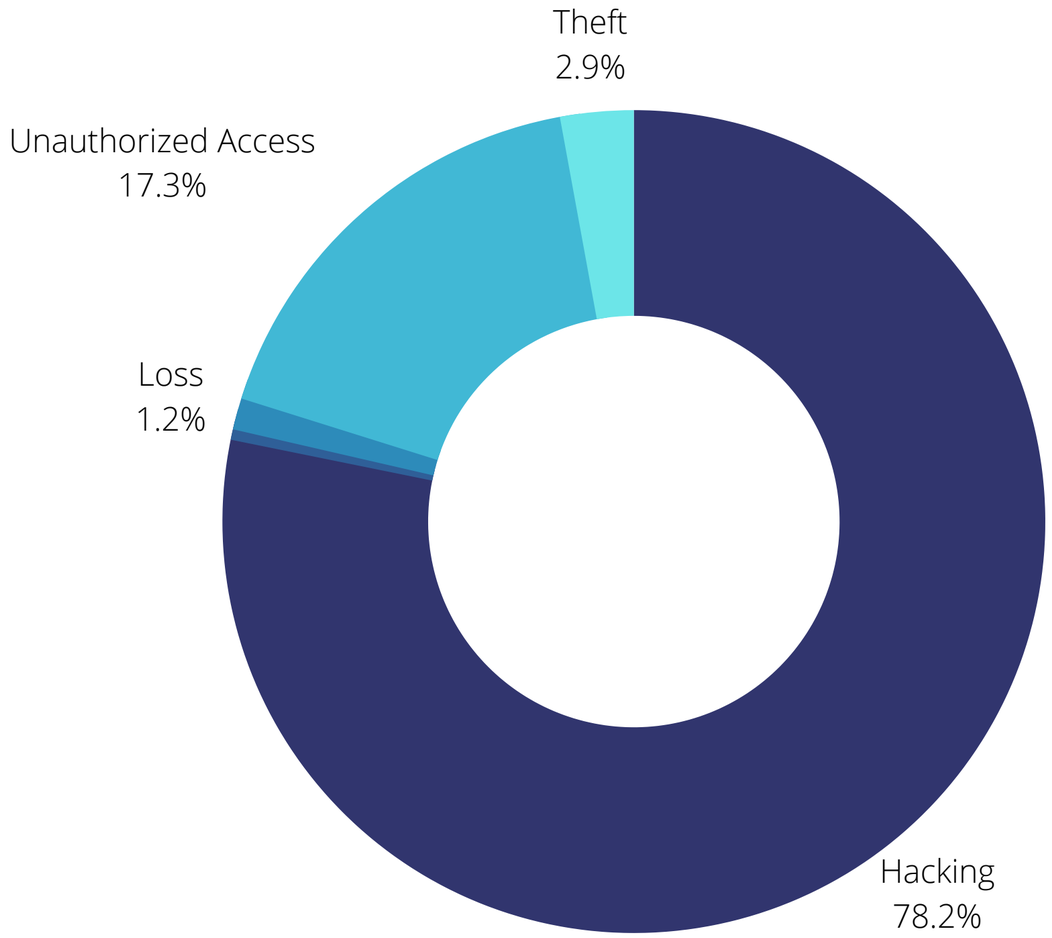
WHO IS GETTING ATTACKED?



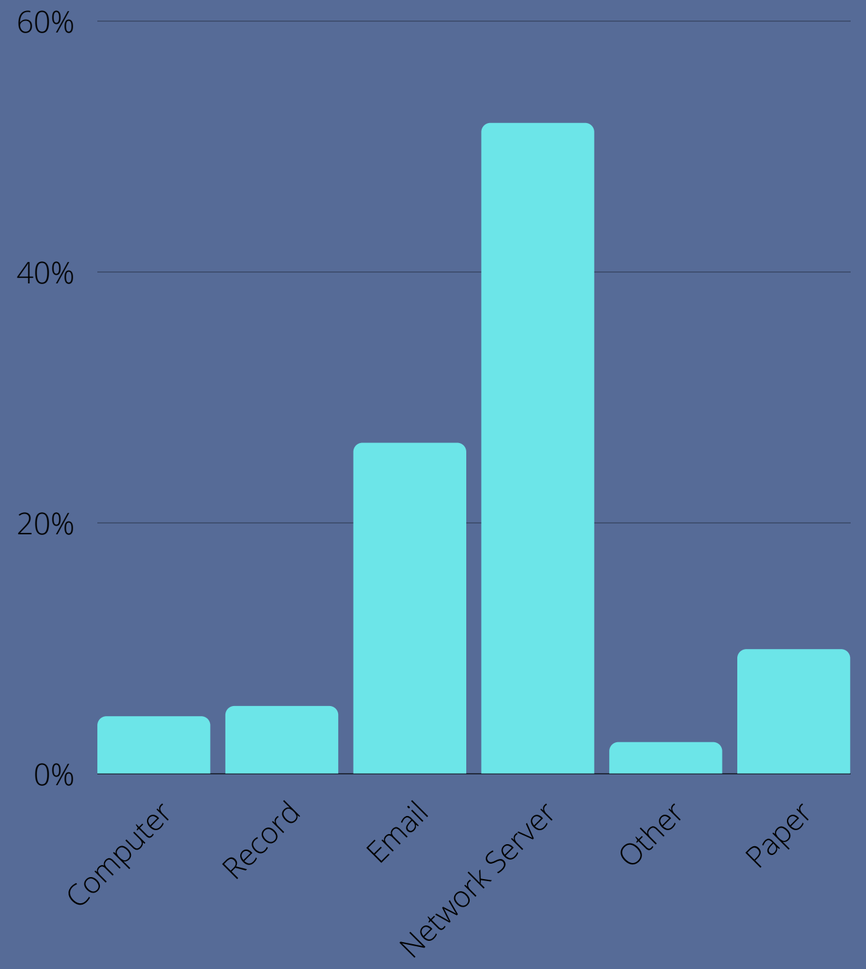
OVER 1.1M INDIVIDUALS WERE AFFECTED BY THIRD PARTY BUSINESS ASSOCIATES DATA BREACHES.

71% OF BREACHES IN OHIO ARE DUE TO UNAUTHORIZED ACCESS

WHAT IS THE BREACH DUE TO?



HOW ARE THEY ATTACKING?



31% OF HACKING/IT INCIDENTS GET THROUGH VIA EMAIL

TOP 10 LARGEST HEALTHCARE DATA BREACHES OF Q1 2022

NORTH BROWARD HOSPITAL DISTRICT

Location: Florida
Entity Type: Healthcare Provider
Affected: 1,351,431
Type/Breach: Hacking
Breach Location: Network Server

Unspecified hacking and data theft incident

MEDICAL REVIEW INSTITUTE /AMERICA

Location: Utah
Entity Type: Business Associate
Affected: 134,571
Type/Breach: Hacking
Breach Location: Network Server

Ransomware attack

MEDICAL HEALTHCARE SOLUTIONS

Location: Massachusetts
Entity Type: Business Associate
Affected: 133,997
Type/Breach: Hacking
Breach Location: Network Server

Ransomware attack

RAVKOO

Location: Florida
Entity Type: Healthcare Provider
Affected: 105,000
Type/Breach: Hacking
Breach Location: Other

Cyberattack on cloud prescription portal

TTEC HEALTHCARE

Location: Colorado
Entity Type: Business Associate
Affected: 86,305
Type/Breach: Hacking
Breach Location: Network Server

Ransomware attack

TOP 10 LARGEST HEALTHCARE DATA BREACHES OF Q1 2022 CONT.

ADVOCATES, INC.

Location: Massachusetts
Entity Type: Healthcare Provider
Affected: 68,236
Type/Breach: Hacking
Breach Location: Network Server

Unspecified hacking and data theft incident

IRISE FLORIDA SPINE AND JOINT INSTITUTE

Location: Florida
Entity Type: Healthcare Provider
Affected: 61,595
Type/Breach: Hacking
Breach Location: Email

Email accounts accessed by unauthorized individuals

SUNCOAST SKIN SOLUTIONS

Location: Florida
Entity Type: Healthcare Provider
Affected: 57,730
Type/Breach: Hacking
Breach Location: Network Server

Ransomware attack

HOSPITAL AUTHORITY OF VALDOSTA

Location: Georgia
Entity Type: Healthcare Provider
Affected: 41,692
Type/Breach: Hacking
Breach Location: Desktop Computer

Unauthorized access and PHI theft by a former employee

FAMILY CHRISTIAN HEALTH CENTER

Location: Illinois
Entity Type: Healthcare Provider
Affected: 31,000
Type/Breach: Hacking
Breach Location: Network Server

Ransomware attack

03.

SAAS SECURITY THREATS IN HEALTHCARE

Healthcare organizations adopt SaaS (Software as a Service) like never before due to the convenience, ease of use, and cost savings associated with these applications. However, there are certain risks related to third-party apps that every healthcare organization should be aware of.

Bad actors are now attacking third parties directly to have a broader impact and attack more victims at once. These hackers can cause more damage by targeting third party software or billing providers since they have access to many customers and their impact is more significant.

A few of the top SAAS security threats these apps pose to healthcare providers are more effective regulation, data access control, and limited security infrastructure

MAN-IN-THE-MIDDLE VULNERABILITIES

Data doesn't travel between an app and the hospital backend directly. There is a communication route which sends the data back and forth between the two. Every stop on their route allows bad actors to intercept the data and potentially damage the backend.

Those designing or engineering third-party apps are not always thinking about security. Their focus is on how the app operates and how it works for the user, not how it interacts with the network nor how data is transferred.

More than half (53%) of the mobile apps tested had hardcoded API (Application Programming Interface) keys and tokens that would enable hackers to attack the APIs. Token-spoofing, MAC address spoofing, and IP address spoofing are just a few ways hackers can intercept data.

It is up to the healthcare organizations to focus on third-party security to ensure that they are well protected against. such sophisticated attacks.

LIMITED CLOUD INFRASTRUCTURE

The cybersecurity vulnerabilities inherent to cloud storage are nothing new. Many companies were still in the process of improving their cloud security when the pandemic hit and were forced to accelerate their plans. Two years later, and essential cloud infrastructure of many telehealth and mHealth apps have not been improved.

Unfortunately, many APIs still have security vulnerabilities, often giving cloud storage providers undue access to your data. Many of these startups are unaware of how to safeguard their applications, leading to vulnerabilities in deployment. This is done without carefully thinking through access policies or future configuration needs in many cases.

Traditional security tools and strategies are often not adequate enough to protect a cloud-based infrastructure effectively because it is so different from an on-premises data center. But if the building blocks of your third-party app are not set up right, nothing you can do will make it safe.

LACK OF REGULATION

The way third-party apps choose to use their health data is mainly up to individual companies rather than predetermined regulations. Under HIPAA, cloud service providers aren’t considered business associates and therefore are not subject to HIPAA. Instead, most third-party apps fall under the FTC jurisdiction and the protections provided by the FTC Act.

The FTC Act, among other things, prohibits deceptive acts. For example, an app that says it won't share your personal information but then does would violate the FTC Act. About 88% of healthcare apps are built with the ability to collect and share user data, according to a study published in the BMJ. Therefore, it is critical to understand how your health information will be used once you decide to share it with an app.

DATA CONTROL ISSUES

Along with concerns that the SaaS provider’s servers could shut down for good during an outage, there are risks and worries that your data is not really under your control. Should something happen, and your information is lost, you will have to contact the service provider, wait for their answer—however long that may take—and only then will they explain what might have happened.

The SaaS provider is responsible for data storage. That may be a relief, but it’s also a loss of control that opens users to panic and, in some cases, costs them much time waiting for answers when faced with issues. You have no clue where your data is located, how secure or hardened the facility is, or who works there.

As HIPAA does not cover some SaaS companies, they work data access language into their licensing agreements. That means the cloud provider can access and use the information stored on their platform.

According to a 2019 study published in the National Library of Medicine (NLM), 79% of healthcare apps resell or share data. There is no regulation requiring patient approval of this downstream use which can cause potential privacy regulation issues.

HOW IS YOUR DATA SECURED?

During the pandemic, a study by HealthGlobal suggested that 80% of all Covid-tracking apps were found to leak data. In contrast, around 70% of tested medical apps included at least one high-level security vulnerability. Moreover, a study published in BMC Medicine toward the end of last year showed that 66% of apps sending identifying information over the Internet did not use encryption.

These third-party apps claim to use the Fast Healthcare Interoperability Resources (FHIR) standard. This, however, does not necessarily mean it's secure. An Approov's 2021 report found leaks within 25,000 apps, where the vulnerabilities lay within the implementation of apps and by third-party FHIR aggregators. Not the HL7 (Health Level Seven) FHIR standard itself.

HOW IS YOUR DATA SECURED?

This still leaves systematic gaps in compliance with data protection principles in accredited health apps. According to the Open Web Application Security Project (OWASP), many security vulnerabilities are due to weak server-side control, insecure data storage, insufficient transport layer protection, insecure encryption algorithms, and a lack of binary protections.

Cloud computing enables rapid data movements between the cloud provider and the company. However, more often than not, data stored in a public cloud is not sanitized to DoD (Department of Defense) levels. There is the risk of data exposure due to data deletion from the platform since it exists within either their archives or backup volumes.

For example, suppose a subscriber deleted a portion of their data. The cloud provider previously backed up that data every night to tapes and archive tapes for six months. That data will still exist well past the point that the subscriber has deleted it, and the subscriber cannot do anything to change this.

Even if the data may be safe now, it might not be in a year or two when protocols have changed, policies have been updated, and risks are heightened. As mentioned above, most providers insist on long-term investment within their SaaS software.

04.

HOW HEALTHCARE CAN RESPOND TO CLOUD APP SECURITY ISSUES

The cloud has improved patient experience by optimizing healthcare infrastructures with real-time data exchange and access. As healthcare application workloads become more prevalent, they pose unique next-generation security and compliance issues for healthcare IT security professionals.

Healthcare organizations as well as regulators who handle and oversee this sensitive data must give equal attention to their third-party security enforcements as they do their network protection. Yet, most providers have not fully tackled vendor or access risks within the healthcare or pharma environments.

There needs to be regulation for third-party apps and the security of patient health information. But until then, there are several steps hospitals and doctors' offices can take to mitigate the risk of cloud apps for themselves.

REDUCE THE RISK OF RANSOMWARE ATTACKS

Prevention is the best way to mitigate threats. Organizations often start by working with their internet service provider (ISP). These cybersecurity practices are the best way to decrease vulnerabilities within your healthcare organization:

- Prioritize Patch Management: Cybercriminals typically find an entry by known software vulnerabilities. This highlights the importance of needing to keep applications, software, and operating systems patched.
- Harden your Systems: Attackers search for exposed areas, so decrease soft surfaces by closing ports and shutting off unused services. Leverage firewalls where possible.
- Apply “Least Access Privilege” Policies: Only give workers access to what is necessary for their job position and duties.
- Use Multi-factor Authentication: Deter hackers by requiring more than one system authentication layer.
- Employ Email Gateway Filters: These help to identify malware indicators in subject lines and other areas while a firewall blocks suspicious IP addresses.
- Filter Traffic by IP Ports and Addresses: Use threat-based and geographic blocking to filter outbound and inbound traffic.
- Require Remote Staff to use a Virtual Private Network (VPN): A VPN adds a layer of protection for employees accessing systems and data.
- Perform Network Segmentation: Use multiple servers to separate sensitive data from email.
- White-Listing: Create a list of approved processes and applications as well as prevent the use of non-approved sources.
- Implement File Integrity Monitoring (FIM): This process reviews your system for changes, port activity, and unusual activities, like unauthorized access.

CHECK-IN WITH HEALTHCARE THIRD-PARTY VENDORS

In our interconnected world, it's vital to ensure your health technology partners prioritize cybersecurity. For example, more than 20 healthcare systems experienced threats after hackers attacked a cloud-based scheduling application.

Consider:

- Reviewing your vendors' security policies and procedures for detecting malware.
- Adjusting your process for third-party remote access by disabling any access until needed.
- Examining vendor compliance with regulations requiring a service level agreement such as SOC1 (System and Organization Controls 1), SOC2, or PCL (Protocol Composition Logic).
- Does your vendor offer a Service Level Agreement?
- Going through all vendor accounts and updating passwords.

CYBER HYGIENE AND EMPLOYEE TRAINING

Employee education and user awareness are primary ways to prevent ransomware infections, especially in organizations with varying staffing flows. Medical and administrative staff must understand techniques used by cybercriminals and what these may look like in day-to-day operations.

Training should include:

- **Email Security**: Teach staff how to identify problems with email links or attachments, including tips on avoiding them.
- **Current Trends**: Highlight emerging risks, like phishing schemes that target staff through an organization's email.
- **Support Policies:** Explain the process and importance of reporting suspicious emails or stolen devices.
- **Remote Management**: Clarify how off-site staff can access health systems, including rules for devices and methods for updating antivirus and malware software.
- **Practice Scenarios**: Devise malware outbreak drills to ensure each person understands their role and learns from feedback.

DEPLOY TECHNOLOGY TO PROTECT HEALTHCARE INFRASTRUCTURE

Along with segmenting your networks to reduce ransomware spread, healthcare organizations should rely on various technologies to prevent and respond to cyber threats. Security solutions may use artificial intelligence (AI) and threat intelligence software with centralized monitoring systems.

Signature and behavioral-based tools continually scan for malicious activities and can isolate remote browsers. All network security tools must be appropriately configured and kept up to date.

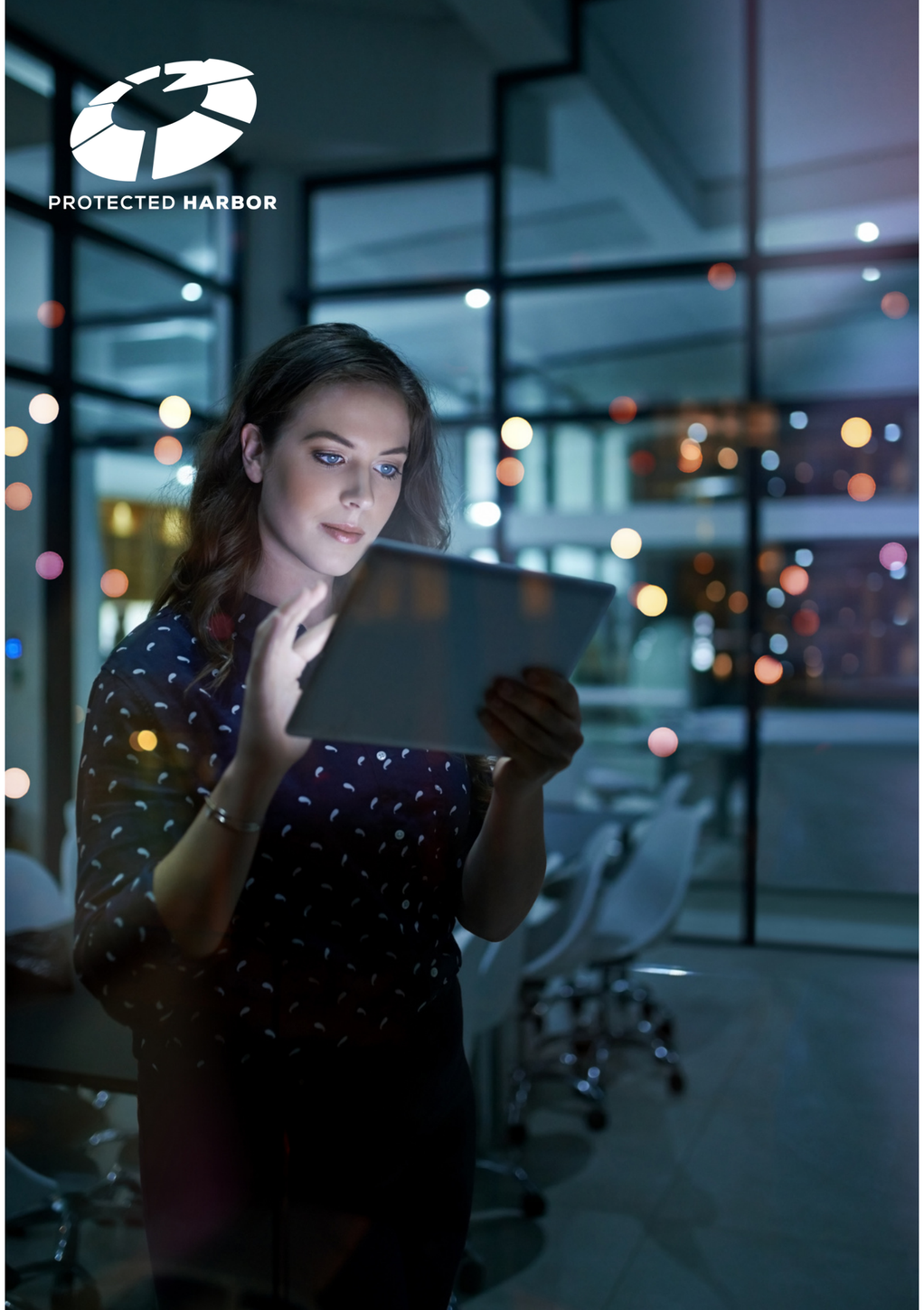
BREACH PREPAREDNESS

The average downtime after a ransomware attack is 15 days. Being without necessary digital records during that time is detrimental to all involved. Healthcare organizations must assume a breach is always imminent with so much at stake.

Along with assessing risks, create a proactive and preventive incident response plan. It should explain how you identify incidents, isolate the breach, repair damage, and continue normal operations.

BEST CYBERSECURITY TECH TO PROTECT AGAINST 3RD PARTIES VULNERABILITIES:

ENDPOINT PROTECTION SOFTWARE
ANTIVIRUS AND ANTIMALWARE PROGRAMS
INTRUSION DETECTION SYSTEM (IDS)
EMAIL FILTERING SOLUTION
FIREWALLS
INTRUSION PREVENTION SYSTEM (IPS)



DATA PROTECTION AND RECOVERY PLANNING

Cybercriminals will look for network backups. If they can gain access, hackers will either corrupt or destroy these backups. Reduce the impact on your healthcare organization with a multi-level backup program.

Start by exploring significant assets and assuring these components are regularly backed up and kept offline from your hospital network. This data may include telehealth infrastructure, remote work foundations, patient database servers, and medical records. Best practices take a 3-2-1 approach:

- Three copies of data
- Two different media formats
- One off-site backup.

You should also create and save several backup versions. Variants account for the possibility of infected or encrypted files. Experts tend to recommend off-site and offline backups (typically known as isolated backups) as an extra preventive measure. However, hard copy backups won't contain your latest data, causing disruptions to patient care.

Additionally, third-party cloud-based Disaster Recovery as a Service solutions (DRaaS) can alleviate backup issues by performing data backups and real-time system surveillance.

Finally, regular testing of your retained data's integrity and accessibility is crucial to ensuring optimal business continuity.

INCIDENT RECOVERY STRATEGIES

Ransomware and malware attacks aren't the only threats your organization faces. Disk hardware can malfunction, power failures occur, or weather-related disasters may harm onsite hardware. Having a backup is only one step of your resiliency plan.

To reduce downtime, you need a recovery strategy—a comprehensive plan, describing the estimated recovery times, goals, and process for the recovery of critical systems, infrastructure, and data.

Your document may include:

- Offline documentation processes for Electronic Health Records (EHR) downtime.
- Graphics showing where your sensitive data resides.
- An environmental, architectural diagram of critical systems, hardware, databases, and more.
- Data flow documentation showing your data lifecycle.
- Communication response and notification methods.

GET CYBERSECURITY SUPPORT

There are several ways healthcare organizations can get ongoing assistance from vendor partnerships and information-sharing programs.

First, it's essential to work with a third party to complete a security risk assessment yearly. This evaluation should meet or exceed the HIPAA requirements. Many healthcare organizations have installed firewalls, spam filters, and anti-virus software to close vulnerabilities created by third-party apps. However, bringing in an experienced team to help with the rise in threats can provide a level of service beyond what firms currently have and at a lower cost.

Companies like Protected Harbor provide various benefits, including cost-saving, superior protection and IT performance, plus advanced technology for organizations. In addition, they will ensure that your organization is protected from outside threats with well-tested, proven, and integrated technology.

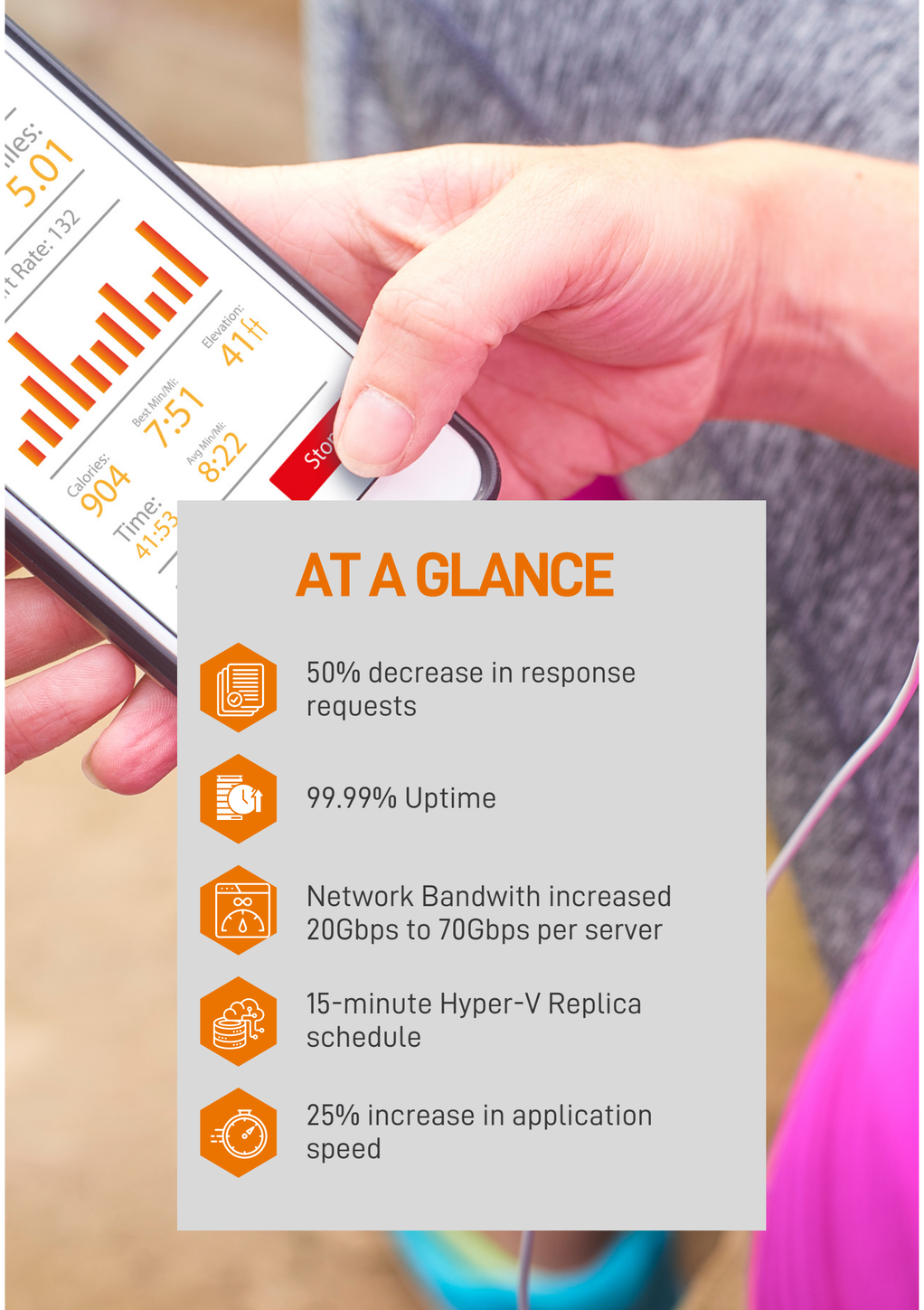
Protected Harbor has helped support healthcare network security and compliance management programs for the past decade. From implementing required security controls and automating the data collection needed for compliance reporting to assisting with audits and reports to regulatory authorities. Outside teams like Protected Harbor bring years of actionable experience to strengthen any healthcare IT team.

Protected Harbor concentrates on six elements throughout the stack which include uplink, firewall, switches, hosts, VMs configuration, and storage to safeguard our customers' operations.

05.

CASE STUDY

AGAPE



AT A GLANCE

- 50% decrease in response requests
- 99.99% Uptime
- Network Bandwith increased 20Gbps to 70Gbps per server
- 15-minute Hyper-V Replica schedule
- 25% increase in application speed

WHEN A MISCONFIGURED THIRD-PARTY APPLICATION PUTS THE BREAKS ON YOUR OPERATIONS

OVERVIEW

With over 900 drivers, Agape Transportation Management provides transportation options for thousands of passengers each day who need assistance getting to doctor's appointments as well as other medical treatments or necessities.

Agape used another software vendor, LimoSys, for a custom multifaceted system that included internal dispatch software, driver, and passenger apps. However, the software solution was not configured perfectly within the network hardware ecosystem Agape had in place. This resulted in various issues and negatively affected the company's business operations and performance.

Hence, Agape required that the Protected Harbor team come in, troubleshoot the problem, resolve it, and increase the network capabilities of the company by migrating the current system to Protected Harbor's data centers; all this without any significant downtime.

THE CHALLENGES & STRATEGY

PHASE 1

All of Agape's users were working from their local desktops. The company was also facing abysmal performance issues because many hosts were incorrectly set up and even had the wrong disk configuration for SQL data. Therefore, the team installed several on-site hosts temporarily to facilitate the stabilization of data and instill a favorable environment for data center migration.

Next, the team presented an action plan to the client regarding the migration, which was immediately accepted. The team began the move by stabilizing and protecting the Limosys app before aligning users with the terminal servers and moving the data from their local desktops to the terminal server by creating a remote environment. The team also made sure that the users were familiar with the new environment so work would continue on their systems hassle-free.

Moreover, the team replicated the client's on-site environment at the data center. While working on the virtual machines, they rebuilt them from the ground up without migrating the client's faulty configuration. However, after a changeover, the application was facing further problems to the point where the software vendor was at a loss even after carrying out software troubleshooting efforts.

PHASE 2

Even though the configuration was the same, as the team used a one-to-one replication approach, shutting the virtual machines off-site and turning them back on in the data center resulted in issues with the application. After taking a swift approach, the team quickly moved it back to on-site and started to troubleshoot what went wrong. The team found out that the application did not turn back on correctly because when switched back on, the application was sending requests to servers that did not exist. Secondly, the software vendor did not know how to measure the application's performance; thus, the team developed a synthetic load to measure performance on-site and then measure again in the data center. Furthermore, the team now had a copy of the client's user configuration in the data center due to the failed changeover initially; thus, they could work on it and replicate the exact issues without disrupting their current operations. Hence, by using the synthetic load, the team tested both environments for comparison, finding out that the data center was reacting slower than the on-site systems.

PHASE 3

As a result, the team made hardware changes, created new servers, and increased the local network bandwidth per server from 20Gbps to 70Gbps. Protected Harbor also went into SQL (Structured Query Language) and found out that the software vendor knew how to install the application but did not understand the complexities of SQL. Hence, the team decided to fine-tune SQL regarding all complexities that could occur and re-ran our numbers. As expected, the numbers were now satisfactory at the Data Center. Using the Hyper-V Replica approach, the team decided to give the changeover another try, which was a success. Now, the team knew how to restart the application and measure its performance. Thus, all the performance issues were gone and the performance at the data center was twice as fast compared to the on-site version.

THE SOLUTION

1. DATA LOSS PREVENTION - The new HA Model made sure that the client had two SQL servers running in HA, and if one of the servers went down, their databases still stayed up.
2. INCREASED CAPACITY - The number of app servers that supported the driver app was expanded which increased the number of requests, meaning that they could cater to more customers.
3. AGGRESSIVE SQL BACKUP & SYNC - Now, periodical backups for SQL databases happen every 15 minutes, and the backups can be restored directly into SQL using a custom solution.
4. REDESIGNED NETWORK - The team troubleshot, completely redesigned, and optimized the client's on-site network configuration, thus increasing their overall functional performance.

THE RESULTS

The new network infrastructure, driven by data loss prevention, and aggressive backup & synchronization, has resulted in an overall 25% faster application speed, 50% decrease in response requests, and 99.99% uptime for Agape, thus making it more effective yet efficient. Moreover, this has provided added benefits for the company in terms of new customer acquisitions, as the new network infrastructure has an increased capacity. Lastly, Agape has become one of the flagship customers of our company in a very short time due to the data-driven, problem-solving, and result-oriented culture at Protected Harbor.

05.

ABOUT US

Protected Harbor is an IT service provider with a focus on Data Center Infrastructure Management (DCIM) and application durability solutions for healthcare providers looking to scale their technology.

PROTECTED DATA CENTER

Protected Data Center (PDC) is a suite of integrated application reliability and DCIM services that protects your technology infrastructure investments. We help design, secure, manage and optimize the infrastructure that runs your critical busi ness applications. Whether building infrastructure from scratch or upgrading legacy systems, Protected Data Center can implement IT solutions to support your operations. From Microsoft Storage Spaces Direct to multi-clustered environments, we have the capabilities and *know-how* to scale your technology to meet your business' growing demand. Our hybrid IT and multi-clus tered roadmaps promise to keep your tech online and moving quickly, so you can work faster and safer.

WHY US

Like everyone else, we offer Cybersecurity, Enterprise Networking, Infrastructure Design, Network Configuration, Monitoring, Customized Protected Cloud, Change Management, and Protection & Recovery. Unlike everyone else, we listen, learn, think, and do not blindly deploy. We care about your business.

Seriously.

We do.

Our customer satisfaction rating and client retention rate speaks for itself. PDC becomes a trusted part of your company. If you're ready to join the winning team and get a good night's rest, we are here to work with you.

THE PROBLEMS

This perfect storm of infrastructure interconnection and network hypergrowth leads to more problems for the industry, such as:

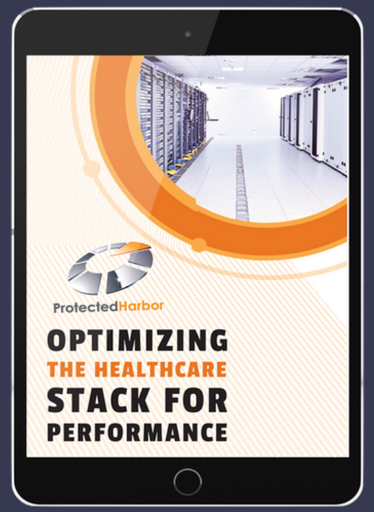
- Dependency on poorly configured third-party apps causing cascade failures.
- Billing systems were based on small file (HL7, etc.) processing in the thousands. They were never designed for billions of larger file processing, resulting in crashes.
- File transfers dependency on antiquated FTP technology resulting in delays, outages, and attach access points.
- System monitoring of several intertwined legacies and state-of-the-art systems that were not designed to be interconnected becomes impossible.

OUR SOLUTIONS

This type of problem is only solved by evaluating the entire environment & identifying the sources that cause the greatest systematic interruptions. Part of our Technology Improvement Plan (TIP) that addresses healthcare applications durability & reliability include:

- Understanding the client workload before establishing a secure performance environment.
- Making sure the right storage for the right workload is placed with the right servers.
- Setting up a modular configuration for a stable environment with optimal scaling and efficiency.
- Installing redundant links in switches and firewalls to avoid a single point of failure.
- Utilizing a multi-layer load balancing & guest clustering approach to achieve high availability.

CHECK OUT OUR OTHER HEALTHCARE IT EBOOKS & RESOURCES



OPTIMIZING THE HEALTHCARE STACK FOR PERFORMANCE

Infrastructure strategies for establishing a secure digital platform that focuses on speed, security, and uptime.

READ NOW

THE HEALTHCARE DATA BREACH TREND REPORT

A look at the biggest data breaches of 2021, what the security trends are for 2022, and how you can protect your data now.

READ NOW

Thank You

For more information and help with healthcare cloud app security, you can reach us at:

201.957.1616

support@protectedharbor.com

www.protectedharbor.com

PROTECTED HARBOR