PROTECTED HARBOR

THE TOP 5 RISKS OF CLOUD MIGRATION

Many organizations fear migrating their applications to the cloud because it can be an extremely challenging and complex task. This process will require proper planning, effort, and time in order for it to be successful.

The security measures as well as practices that organizations have built for their on-premise infrastructure do not coincide with what they require in the cloud, where everything is deeply integrated.

Before streamlining your workflow with cloud computing, you must be aware of the most challenging security risks and how to avoid them. Let's explore how organizations should approach the security aspects of cloud migration, from API integration to access control and continuous monitoring.

This article will highlight some of the most common fears organizations have while moving from an on-premise infrastructure to a cloud environment.

WHY IS SECURITY IN THE CLOUD THE BIGGEST FEAR FOR ORGANIZATIONS?

The reason why security is the biggest challenge organizations face is because public clouds offer shared resources among different users and use virtualization. The ease of data sharing in the cloud creates serious security concerns regarding data leakage and loss.

The major risk in any infrastructure is neglecting security vulnerabilities due to a lack of expertise, resources, and visibility. Most cloud service providers contain various processing and cloud storage services. Therefore, it's easy for hackers to expose data via poorly configured access controls, data protection measures, and encryption.

MOST COMMON EXPOSURE POINTS FOR CLOUD-BASED APPLICATIONS

Overcoming cloud migration challenges before they arise can help any organization to migrate smoothly and save them from potential cyber threats. But first, we need to understand the weak links and exposure points that can put security at risk.

Let's discuss the weakest links that cause cloud application migration fears:

DATA THEFT CAUSES UNAUTHORIZED ACCESS

Providing administrative access to cloud vendors poses serious threats to the organization. Criminals are gaining access to programs like Office 365 through installations that give them administrative rights. In fact, very recently a phishing campaign leveraging a legitimate organization's Office 365 infrastructure for email management has surfaced on the cyber scam scene.

Hackers are always evolving their phishing tactics, and everything they do is seen as being smarter and more sophisticated.

If criminals get access to users' cloud credentials, they can access the CSP's (Cloud Solution Provider's) services for gaining additional resources. They could even leverage those cloud resources to target the company's administrative users and other organizations using the same service provider.

Basically, an intruder who obtains CSP admin cloud credentials can use them to access the organization's systems and data.

THIRD-PARTY PRODUCTS COMES WITH SECURITY RISKS

Organizations outsource information security management to third-party vendors. It reduces the internal cybersecurity burden but generates its own set of security risks. In other words, the cybersecurity burden shifts from an organization's internal operations onto its third-party vendors. However, leveraging third-party services or products may come with compliance risks, business continuity risks, mobile devices risks, and so on.

Last year, SolarWinds, a famous monitoring tool based on an open-source software had been compromise by the Russian Intelligence Service. They had created a backdoor within the coding and submitted it into the base product. Hackers used a regular software update in order to inject malicious coding into Orion's own software to use for cyberattacks.

Vulnerable applications are entry points for cybercriminals. They are always in search of weak spots to infiltrate the system. Applications are used in every industry for better workflow and management. However, there is a need to protect these applications by limiting their access and implementing available patches for better security. Frequent updating of applications and systems helps to protect your IT infrastructure from potential attacks.

HACKERS CAN COMPROMISE VULNERABLE VPN DEVICES

VPNs (Virtual Private Network's) provide an encrypted connection that hides your online data from attackers and allows businesses to protect their private cloud resources. Many cloud applications need a VPN to transfer data from on-premises infrastructures to the cloud. VPNs are configured to operate one way, but they are often bidirectional. This often opens your organization up to an attack occurring in the cloud service provider.

One such attack has been observed where cybercriminals exploit VPN servers' vulnerabilities to encrypt the network with a new ransomware variant. By exploiting unpatched VPN applications, hackers can remotely access critical information, such as usernames or passwords, and allows them to log in to the network manually.

Reconfiguring a VPN to access a newly relocated app in the cloud can be disruptive and complicated for its users. Most people don't use VPNs for cloud application migration because they don't trust them.

It's better to install on-site hardware, build VPNs' deployment on that hardware, migrate them into the on-site deployment, and then move the VMs (Virtual Machines) into a data center. This can be achieved by enabling transparent, unfiltered connectivity between environments. Enterprise cloud VPN can achieve this configuration between a cloud network and an on-premises network.

ACCIDENTAL EXPOSURE OF USER CREDENTIALS

Cybercriminals generally leverage cloud applications as a pretext in their phishing attacks. With the rapid use of cloud-based emails and document sharing services, employees have become habitual of receiving emails with links asking them to confirm their credentials before accessing a particular site or document.

This type of confirmation in particular makes it easy for intruders to get employees' credentials for their company's cloud services. Therefore, accidental exposure of credentials in the cloud is a major concern for organizations because it can potentially compromise the security and privacy of cloud-based data and resources

LACK OF SECURE API

Using API (Application User Interface) in the cloud allows organizations to implement better controls for their applications and systems. However, using insecure APIs can come with grave security risks. The vulnerabilities that exist within these APIs can provide an entry point for intruders to steal critical data, manipulate services, and do reputational harm.

Insecure APIs can cause security misconfigurations, broken authentications, exposed data, broken function-level authorization, and asset mismanagement. The most common example of an insecure API is the Facebook-Cambridge Analytical Scandal which allowed for Cambridge Analytica to access Facebook user data.

READY TO MIGRATE YOUR APPLICATIONS TO THE CLOUD?

Most organizations lack the experience and confidence to migrate to the cloud fearing the associated risks that come with it. The reason is that they don't have the right time and resources in place to facilitate the move.

Leveraging partners and service providers can help to overcome those fears and make the cloud application migration smoother for your organization. With Protected Harbor, discover a faster, more secure journey to cloud hosting services that is trusted by many organizations.

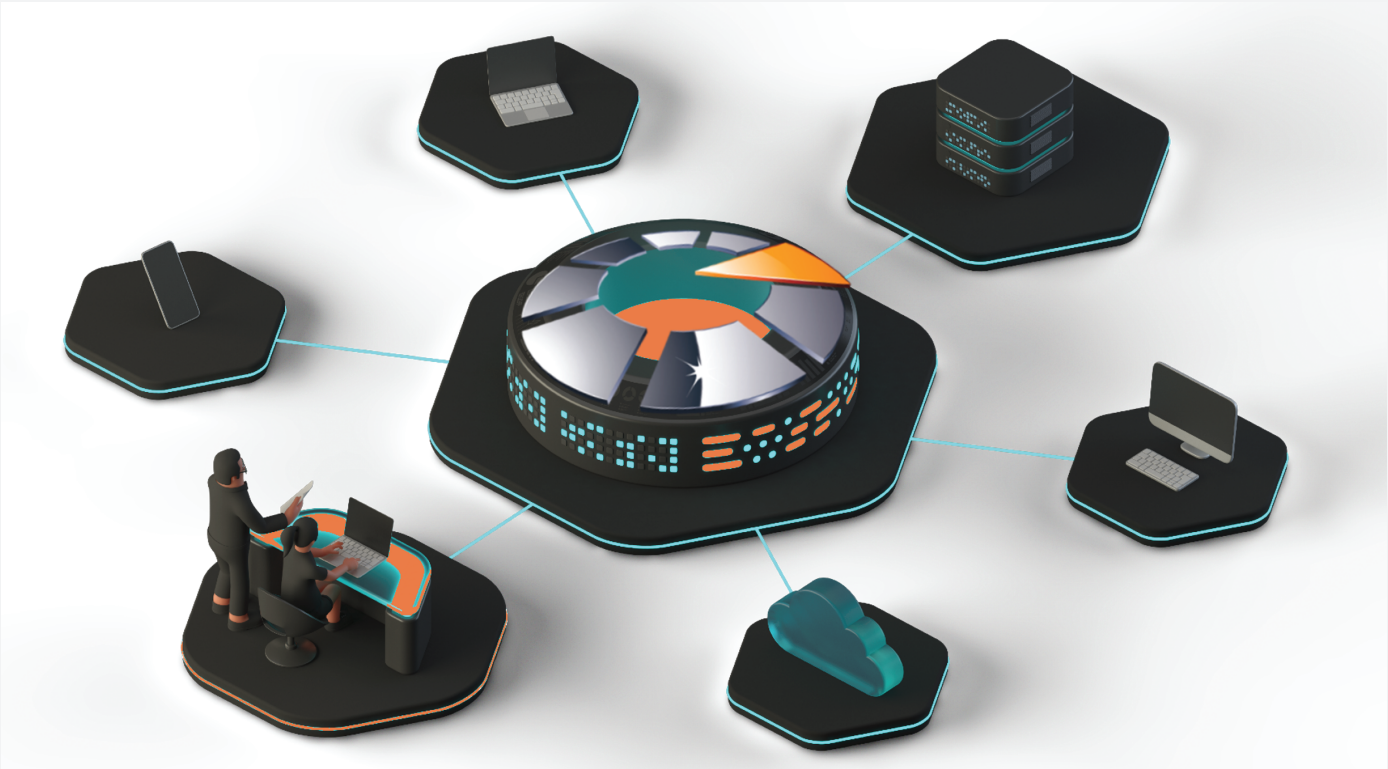
We provide deep industry expertise and a robust set of advanced tools. Experts at Protected Harbor migrate your applications to the cloud and help you to increase and optimize the productivity as well as flexibility of your workforce. Visit here to get more information about Protected Harbor's cloud services.

ABOUT PROTECTED HARBOR

Protected Harbor provides customized data center infrastructure management and appli-cation migration support to businesses looking to scale their technology and bottom line. With over 15 years of service and a 99.99% uptime record, our team is fully committed to creating, maintaining, and managing the high-est quality application operations environment experiences. Your uptime is our focus. Our 90+ Net Promoter Score, and 95% client retention rate back up that claim.

Our Protected Data Center is an integrated suite of managed services focused on the uptime of your application at the lowest possi-ble cost, regardless of location, and cloud pro-vider. From infrastructure design to network operations including security, storage, connec-tivity, remediation, monitoring, and more. Protected Data Center provides end-to-end support to secure deployments of complex enterprise applications to protect your tech-nology infrastructure investments.

Like everyone else, we o er Cybersecurity, Enterprise Networking, Infrastructure Design, Network Con guration, Monitoring, Customized Protected Cloud, Change Management, & Protection & Recovery.Unlike everyone else, we listen, learn, think, and do not blindly deploy. Focusing on durability and uptime, we design a custom architecture solution integrated with a seamless migration process. The entire time we keep your business up and running with our proprietary application outage avoidance methodology (AOA) providing redundancy and high availability.Protected Data Center features a global helpdesk with level 1, 2 & 3 support, 24/7 NOC, a Tier 3 Data Center, best-in-breed CMDB solutions, and years of experience & knowledge from working with leading technology companies.



How Modern Infrastructure Helped NYC's Most Vulnerable Get to the Doctors

AGAPE
TRANSPORTATION MANAGEMENT

INTRODUCTION

Agape Transportation Management focuses on Non-Emergency Medical Transportation (NEMT) services for individuals who are not currently experiencing an emergency but need a more specialized service than what a standard taxi is able to provide. They serve the New York community with essential curb-to-curb services to provide safe transportation for patients to their desired health care facilities.

With over 900 drivers and thousands of patient rides every day, the team needs to make sure their network and custom business software (app) for driver scheduling and communication is always up and running.

AT A GLANCE

- 5 TBs of email to be migrated
- Implementing High Availability
- Multi-phase migration
- Backup capacity increased from 0 to every 15 minutes
- 25% increase in application speed

THE PROBLEM

During the initial IT Audit, Protected Harbor found issues throughout the entire IT infrastructure, starting with incorrect application configuration that caused multiple server failures. The company was forced to revert the system back to a stable point and let Protected Harbor address their three main areas of concern: points of failure, security, and performance.

The previous IT company had a poor five-port switch set up where, in case of a hardware failure, it would bring everything down, including the firewall. Although at this point, the firewall was just a theory. Agape's last team had bought an indus- try-leading firewall for protection, but it was not set up properly and had not been renewed for over a year rendering it inactive. Additionally, the stack was not utilizing an uninterruptable power supply, negating the benefits of the client's expensive backup power setup. These single points of failure were enough to bring the whole system down and needed to be addressed.

There were other major security concerns, aside from the lack of a firewall. The client was vulnerable to an increased risk of attack, data leakage, and ransomware. A host of deactivated software was still installed on the network. There were IT management and monitoring tools that had access to the system with no control or oversight. Several virtual machines had no firmware or driver updates for the clients. One host had not been rebooted in 900 days. In a classic case of MSP over-reporting and under-performing, the previous service provider supplied updates to the infrastructure that the client could tangibly see. However, there were no updates on the backend servers.

Finally, the infrastructure was not optimized to provide the High Availability (HA) environment required. The vendor was still using servers with factory settings. There was nothing customized or set up to fully utilize the client's platform. Some of the software, such as SolarWinds, was not configured properly for the environment, creating an overuse of resources and inefficiency. Finally, the database for the mobile application the company relied on to schedule and communicate with drivers was heavier than the system could handle, creating latency and connectivity problems for the drivers.

PROTECTED HARBOR

THE SITUATION

Agape's systems were overburdened with software and tools that were either no longer needed or had expired, prompting both their replacements and much needed modification. Protected Harbor had to start with the basics. That meant first lowering the load, deciding what was necessary to keep, and then migrating the client to a new customized server setup with a focus on speed and availability.

The team started to intimately work with Limosys, Agape's critical software provider, to plan the migration. Protected Harbor replaced the Fortigates (firewall protection) with High Availability pfSenses. They then started the process of backing up hosts and configuring for monitoring the environment. Protected Harbor broke the project down into five stages.

THE SOLUTIONS

1. **Development and Testing:** During phase one Protected Harbor developed a process for testing the Limosys software. This was an unknown entity with no historical data to reference. Everything needed to be created from scratch. The team then followed through with completing the data migration. Once this was completed, Protected Harbor tested the app and checked with the end-users for suitability.

2. **Hardware High Availability:** Following the data migration, the terminal server was upgraded, which included the creation of new accounts and domains, as well as a high-end customization and setup of Agape's devices. All of the data was transferred from local workstations to the servers and then tested with users, again.

3. **Migrating Terminal Server:** Copies of virtual machines were created and saved at Protected Harbor's datacenter. As a result, the team was able to eliminate unnecessary hardware. Once migrated, Protected Habor changed out access points and reinstalled Windows on each device. The new High Availibility model ensured that the client had two SQL servers running in HA mode and that even if one of the servers failed, the client's databases remained operational.

"Thanks to Protected Harbor's data-driven, problem-solving, and result-oriented culture, Agape has quickly become one of the top companies in medical transportation."

Mario Sena
Founder, Agape

THE RESULT

The new network infrastructure created by Protected Harbor, which is driven by data loss prevention, aggressive backup, and synchronization, has resulted in a 25% increase in application speeds, a 50% reduction in response requests, and a 99.99% uptime for Agape, making it more effective while remaining efficient. Periodical SQL database back-ups are now performed every 15 minutes, and the backups can be restored directly into SQL using a custom solution. Furthermore, because the new network infrastructure has improved capacity, the firm has gained significant boosts in terms of new client acquisitions.