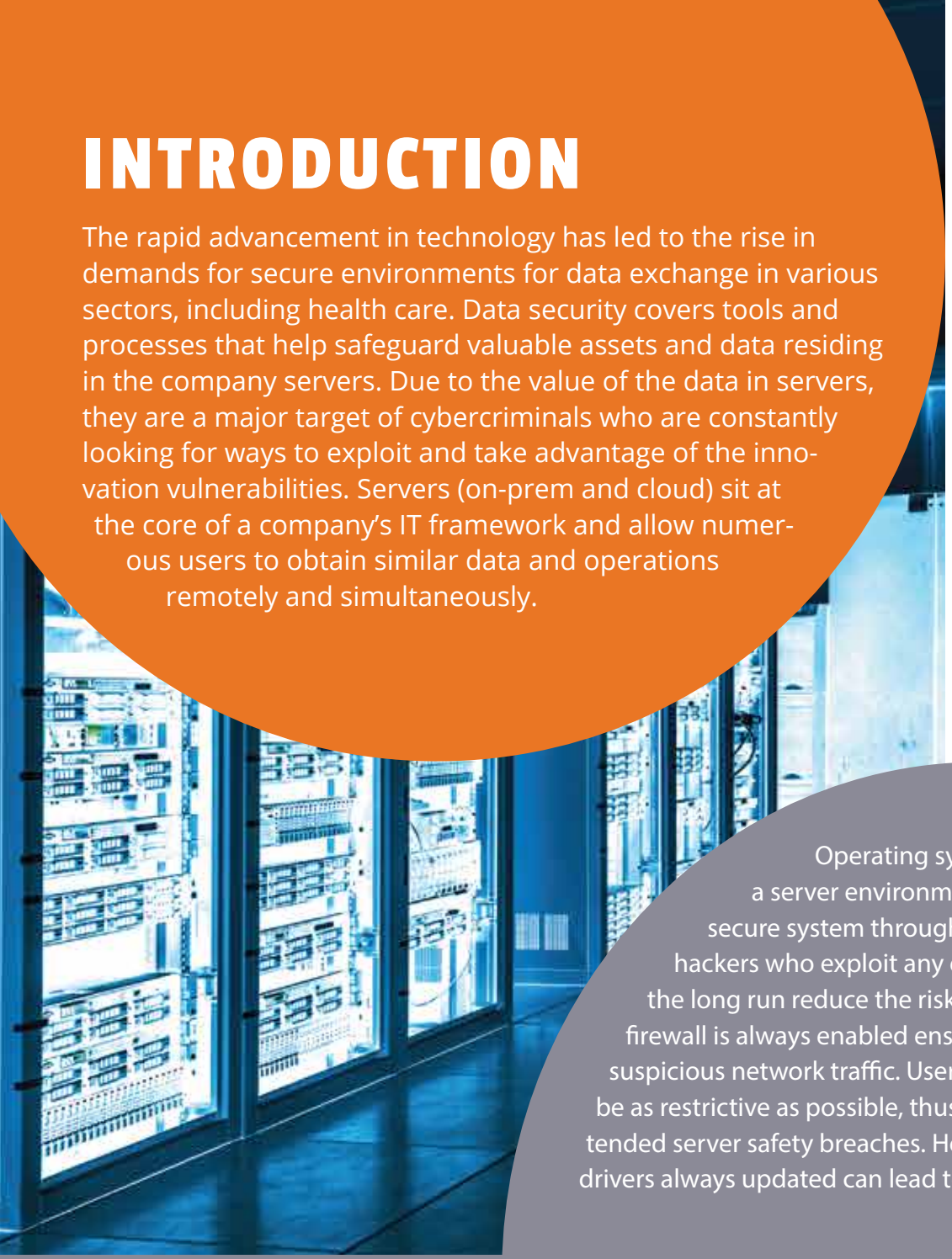
ProtectedHarbor

OPTIMIZING THE HEALTHCARE STACK FOR PERFORMANCE

INTRODUCTION

The rapid advancement in technology has led to the rise in demands for secure environments for data exchange in various sectors, including health care. Data security covers tools and processes that help safeguard valuable assets and data residing in the company servers. Due to the value of the data in servers, they are a major target of cybercriminals who are constantly looking for ways to exploit and take advantage of the innovation vulnerabilities. Servers (on-prem and cloud) sit at the core of a company's IT framework and allow numerous users to obtain similar data and operations remotely and simultaneously.



The increased application of e-health and telehealth has enabled health organizations to discover the need to place their data and workload records in private cloud networks due to their increased security. Achieving this requires IT specialists to develop sound designs and frameworks with appropriate network configurations to maximize the application of cloud-based resources. They should also ensure that system designs meet relevant privacy standards, such as HIPAA (the Health Insurance Portability and Accountability Act of 1996) or GRC (governance, risk, and compliance), and avoid violating predefined policies. Service Organization Control (SOC) 1 and SOC 2 certification will guarantee data security and integrity, thus increasing safety in business operations. Following these strategies means establishing a secure digital platform that integrates legacy technology focusing on speed, security, and uptime. IT personnel should also ensure that the system allows constant accessibility of the required data from any device without failure for the health professionals.

Operating system patching in a server environment helps establish a secure system through the prevention of malicious hackers who exploit any existing vulnerabilities that in the long run reduce the risks of an attack. Ensuring that a firewall is always enabled ensures optimum defense against suspicious network traffic. User access system access privileges should be as restrictive as possible, thus reducing both intentional and unintended server safety breaches. However, failure to keep the firmware and drivers always updated can lead to significant business losses.

UNDERSTANDING THE ARCHITECTURE

When designing servers, it is necessary to identify the primary users of the technology without assuming other issues such as security and ease of accessibility. Competent IT specialists must establish adequate security features in servers by integrating system control capabilities like authentication and backups that ensure data redundancy. Such practices give room for future growth and business continuity. Understanding the nature of the client workload is significant when establishing a secure performance environment. This means that it is imperative first to understand what the company does and how it wishes to utilize the server technology. Most people fail to consider this phenomenon, and, as a result, they end up causing increased server downtime and disrupted operations.

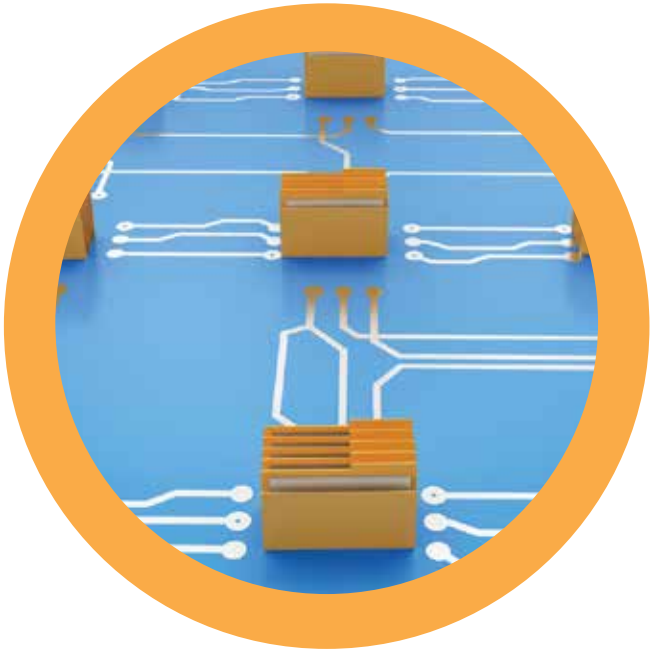
STORAGE

Data storage in the server environment helps in the information repository, access, protection, and management of digital records, files, and services. Finding the right choice of storage medium that meets the organization's needs requires proper considerations, including the purpose of information preservation, data usability frequency, and the number of details to preserve. Companies have a variety of categories of storage apparatus and some of them are directly attached storage appliances, network, and cloud data storage. Protected Harbor uses standard hard disk drives (HDDs), as they offer sufficient storage space for voluminous records. The firm also utilizes flash storage, a solid-state technology that employs flash memory chips to store and write documents. Solid-state disks (SSD) are advantageous as they have no moving parts like the HDDs, hence experiencing less latency. For heavier and higher storage workloads consider non-volatile memory express (NVMe) storage, which is faster than traditional SSD.

STORAGE

Knowing what a company does helps server architects determine what to integrate into their final product to meet the organizational needs. This knowledge can also be suitable for IT specialists to identify devices, hardware, and applications no longer in use and those that need replacement. As a result, architects can eliminate them to give room for advanced innovations that promote efficiency.

Assessment of legacy systems and applications helps determine a secure and efficient server atmosphere. IT professionals should conduct comprehensive auditing of programs to assess their value and understand whether they require any upgrade. Reviewing the framework assists in identifying whether the server delivers advanced results. Weighing the potential disruptions that the technology may have to the business and the associated impacts aids in the identification of the changes that IT experts can introduce in the technology. Designing, implementing, monitoring, and constantly making improvements on the server guarantees data safety at the workplace and eliminates data breach vulnerabilities.



Security at the endpoint devices requires the use of the zero-trust technique to improve security measures. Zero trust is a defense framework that requires users within or outside the company network to be authenticated for authorization into the network. It requires continuous validation for protective configuration before granting access to data and applications. Such strategies improve network security in such endpoint devices, as they are the main avenues through which successful breaches start. Failure to implement advanced endpoint administration practices increases company exposure to phishing attacks and information exfiltration. To achieve optimal security for endpoint devices, it is advisable to use techniques such as OS hardening, denial of server access, implementation of least privilege, and data encryption. Other essential practices entail the integration of threat detection, avoidance, and mitigation in the company systems.

ACCESS CONTROL

User management is a critical concern in any environment where the business needs to advance its system security. The administrator uses approaches like user authentication to control user access to servers, applications, and networks. Users within the same company can have varying responsibilities within the system but utilize a similar server access model. However, effectively managing users' access methods, including proper firewall configuration and following company security standards, is advantageous. Other practices to minimize threats entail authentication of people utilizing existing Active Directory and LDAP systems and use of guest accounts whenever sharing data. Improved administration of user roles helps in promoting compliance in the server environment.

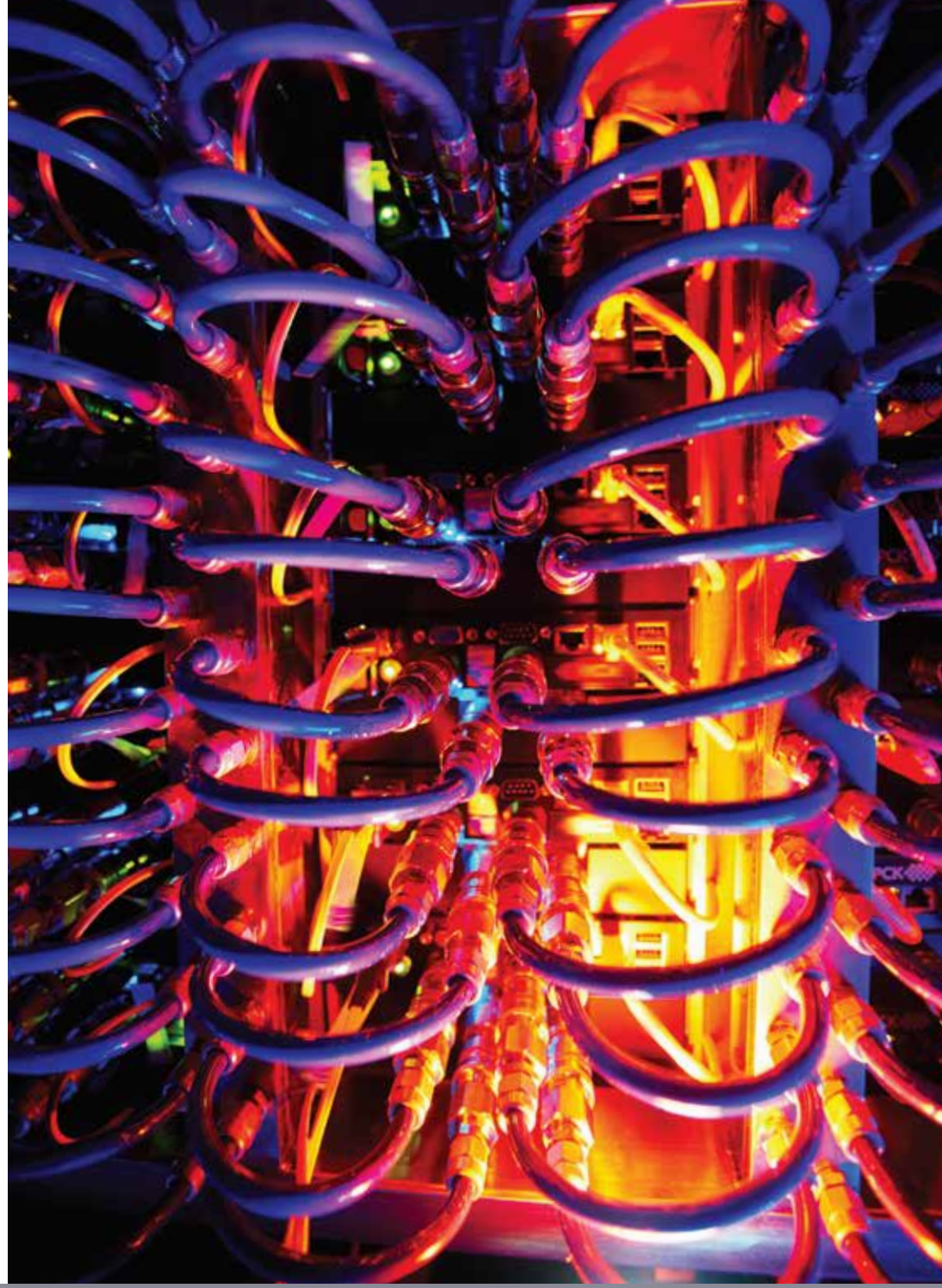
ELIMINATING VULNERABILITIES

A secure server environment requires proper strategies and approaches to ensure that data accessibility and transmission do not interfere with business operations. IT specialists should ensure that sensitive data does not get to unauthorized persons. System users should consistently implement data encryption whether data is at rest or in transit. Authentication and authorization are other factors that secure IT environments should accommodate. These steps require users to provide their security credentials, such as passwords and fingerprints and confirm that they have the right to access certain server resources or have permission to execute operations on the system such as delete, modify, copy, paste, and edit. A low privilege policy would allow users to have a minimal level of permission to perform activities on the system. Server and network segmentation are essential practices that contribute to improved system performance, better access control, and enhanced containment. The latter is necessary because if a problem arises within the IT infrastructure, containment increases efficiency. Recording of users' activities helps in monitoring user log activities such as open and close. This helps promote accountability and assists in the auditing process.

PROPER NETWORKING

Firewalls and switches have an essential role in enhancing security and efficient performance. For example, a primary firewall exists in the normal functioning mode and handles network traffic. The secondary firewall is always in a standby state and takes over whenever the primary firewall fails to work. Both firewalls enhance protection by blocking domain names, monitoring network traffic, promoting privacy, providing access control, and preventing hackers and malicious programs like Trojan. In our setup, firewalls utilize synchronized connections between the two components, and as a result, all modifications happening are mirrored.

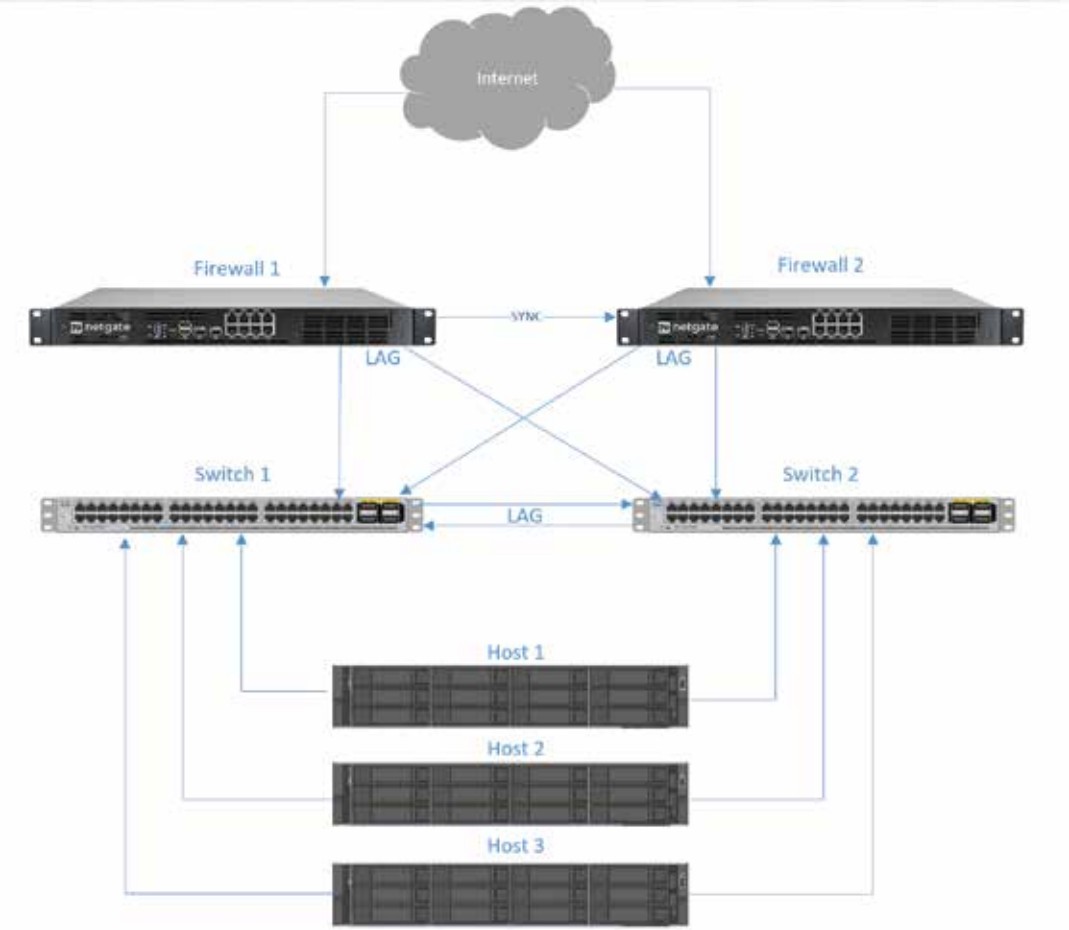
A Link Aggregation Group (LAG) lies between the switches that interconnect to the firewall. In the virtual private cloud (VPC) stack, the switches act as a single device, and as a result, no interference or failure occurs if one breaks down. In this scenario, every firewall has a single link to every switch, and from there redundant links into the stack. The use of LAGs promotes redundancy in the company, eliminating interferences in case of any single point of failure within the network.



PROPER NETWORKING

When comparing managed switches versus unmanaged ones, the most important difference is whether managed or non-managed switches are better for your needs. For most organizations, the former is more cost-effective and allows you to configure and troubleshoot your network remotely. Managed switches provide more granular control; however, unmanaged switches are less expensive. Managed switches are better for enterprise networks because prevent unauthorized access and deliberate attacks. In addition to providing greater security, managed switches are cheaper to operate and are less likely to suffer from network errors.

In the Protected Harbor Data Center, we use high-performance switches from Cisco. These switches are basically a server running an operating system. They are built to run nonstop, for years on end. They are the fabric of how everything in the network and stack talk to each other. We also use fiber ethernet cables and 40 SFP ports. Specifically, OM4 multi-mode fiber ethernet cables for simple server connectivity. OM4 fiber uses laser-optimized transmission to boost performance and achieve higher modal bandwidths. Perfect for building a stable environment.

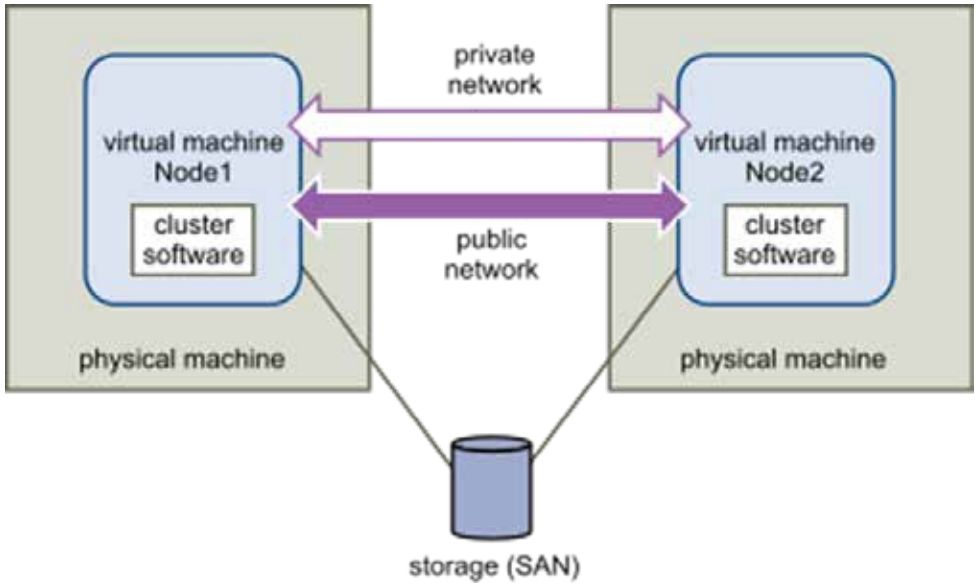


HOST

Protected Harbor's servers use Hyper-V, Microsoft software for virtualization products. Hyper-V allows IT specialists to establish and run a software version of a PC known as the virtual machine. To increase security for clients, the host network does not communicate with any VMs directly even though they run directly on the host. The system users cannot interact with the server directly. Data backups communicate to the host directly and do not interact with the VM.

Running several hosts in a cluster is beneficial as it introduces high availability for the running virtual machines. In the event of a host hardware failure, the VMs will be quickly rebooted on other hosts in the cluster, substantially reducing the disruption a hardware failure can cause to the business.

HOST



Any infrastructure can be designed—but always at a cost. How does Protected Harbor manage to develop such a fantastic framework and maintain optimal performance? We create advanced structures with high-security levels for our clients before deployment. We also train our clients on best practices, such as usage of new platforms and testing of the infrastructure. To safeguard our customers' operations, we mainly concentrate on six elements throughout the stack, uplink, firewall, switches, hosts, VMs configuration, and storage.

Protected Harbor ensures proper configuration at every point that contributes to improved security and high performance. This is made possible through our infrastructure, which is capable of accommodating sensitive data such as personal health information records. Our professionals have also managed to eliminate multiple challenges that interfere with most database environmental architecture, including the use of wrong relational database management systems and outdated databases, and storage not optimized for database workloads. Other areas where we excel are handling database scalability issues, increasing data volumes, growing database complexities, decentralization management, and poor data security. A well-defined system architecture makes it possible for the company to solve these hurdles and acts as the foundation for improved data quality, information governance, and data management. With the relevant business-scale capabilities, IT and engineering experts develop efficient stacks that handle important database issues such as those mentioned above.

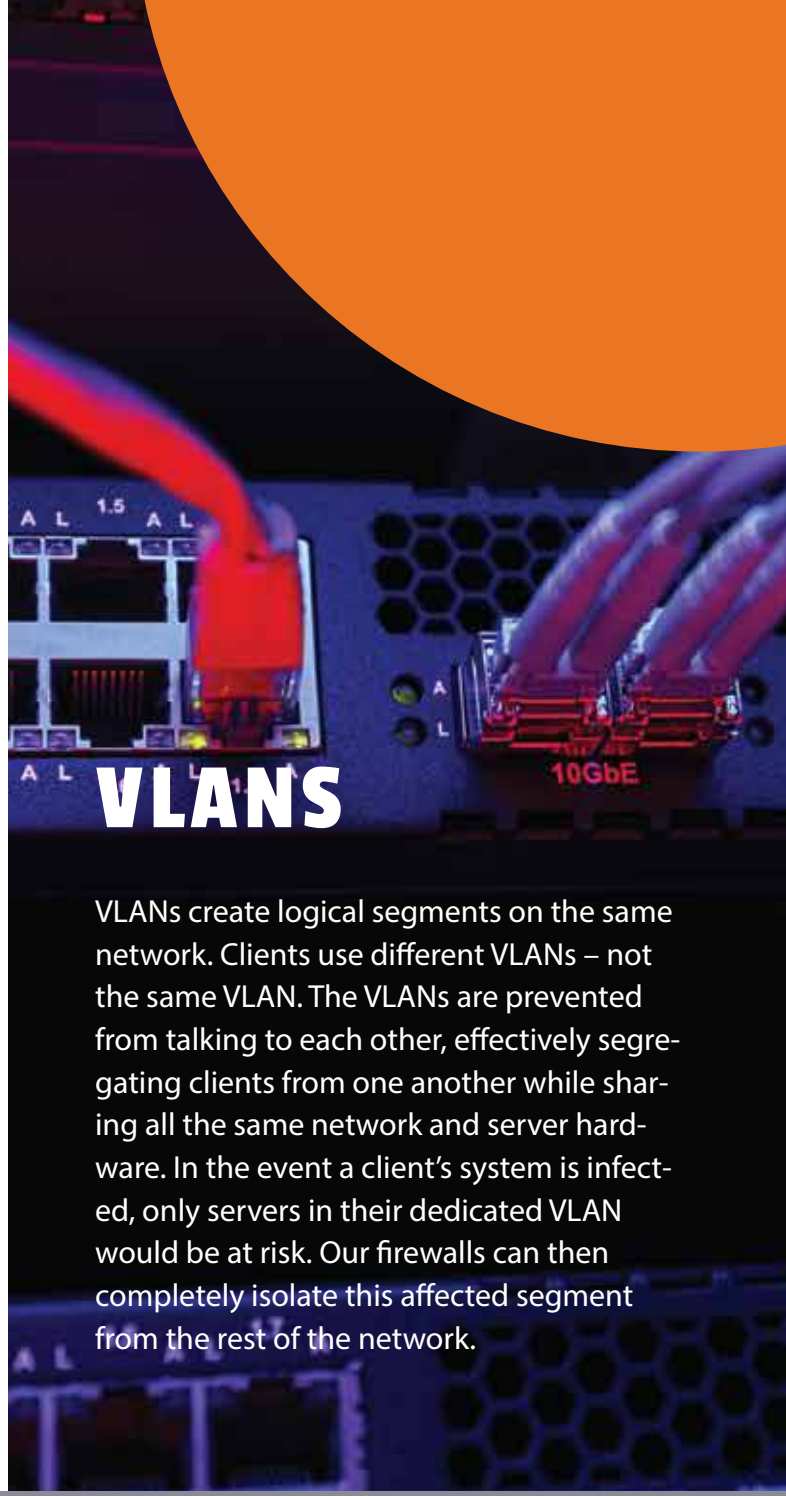
Understanding how a user operates is vital to realizing the kind of system model and securities to integrate. Configuration of devices requiring high availability demands that the involved IT professionals look at the framework from different perspectives, including load balancing layer, platform production space, routing layer, data layer, hosting console, and platform system console.

REDUNDANT SYSTEM DESIGN

Setting up a modular configuration helps ensure a secure system environment with optimal operational efficiency. This process allows for server scaling when the need arises and enhances easy maintenance since one can temporarily remove a faulty server and the system remains functional. It also allows for quick setup through the clustered server settings like a slow start, active connections, and failure timeouts. Most people ignore this initiative as they look at the cost of setting up the facility, and they end up experiencing severe threats such as security breaches and data accessibility by unauthorized persons.

UPLINK AND ISPS

Uplink and ISPs require redundant connections to prevent system breakdown in the working area. During uplink configuration, it is advisable to have a backup link to act as an access point if the primary uplink fails. The same case applies to ISP redundancy, which involves monitoring the ISP links and choosing the current and the best link for load sharing and primary or backup internet supply. To achieve adequate ISP redundancy, it is recommended that a company interconnects with different ISPs and have an entire block of IPs shared among internet service providers. This provides a constant internet supply since the breakdown of one ISP in the firm does not make it go offline. Its ISP switches to the next network since the IPs do not have to change to have a new configuration. However, this can be challenging because different ISPs have to collaborate.



VLANS

VLANs create logical segments on the same network. Clients use different VLANs – not the same VLAN. The VLANs are prevented from talking to each other, effectively segregating clients from one another while sharing all the same network and server hardware. In the event a client's system is infected, only servers in their dedicated VLAN would be at risk. Our firewalls can then completely isolate this affected segment from the rest of the network.

FIREWALL

Redundancy in firewall configurations involves setting rules that provide fault tolerance. If one firewall collapses, the other can pick up operations and handle the traffic while keeping the failure transparent to the system users.

At Protected Harbor, we use GEO-IP filtering, which allows our system administrator to block any connection originating or going to a geographical zone to resolve the public IP address of a particular country. This mode of sifting filters malicious links from a foreign state. GEO-IP filtering is used when blocking via a firewall where the access rules allow network administrators to control network traffic. Blanket blocking involves intercepting or allowing URLs for all users in specific institutions such as a school. We also utilize the reputation-based blocklist method to prevent any IPs on the blocklist from bypassing the firewall rules and stop destructive IPs from penetrating the system. We employ MaxMind, CI Army, and TOR List, just to mention a few, to combat foreign entities from penetrating our systems.

We prefer to use Elasticsearch machine learning in our servers to gather logs from devices with separate VMs that collect the records and verify and analyze them to identify whether the traffic going through them originates from malicious individuals. They also monitor clients' VLAN firewalls and switches within our networks. Other technologies that we use in our company include Elasticsearch, a distributed analytics and search engine effective for log analytics. Elasticsearch is also used at Amazon, Wikipedia, and the U.S. Department of Defense.

THE HOSTS

The host at Protected Harbor exists entirely as a separate entity from the virtual machines occurring in its network with no third-party software. Third-party software increases threat surfaces, which are the different points where unauthorized persons or cybercriminals can attempt to penetrate the system to cause harm or steal data. Such applications require constant checking and monitoring, which we avoid in our infrastructure. Regular update on hosts, which most organizations ignore, prevents data breach, enhance virus protection, increase efficiency, and introduce new security features in any given platform. A standing maintenance cycle helps improve safety through anomaly detection and reducing failure risks. Other vital steps to boost infrastructure defense include operating systems, drivers, and firmware patching. Most businesses do not practice firmware and driver updating due to configuration errors leading to execution disappointments. To avoid such issues, Protected Harbor uses the command-line utility from Dell, known as Dell System Update. We have also worked together with these tech giant experts to develop an appropriate update procedure that is user-friendly.

ACTIONABLE MONITORING

Effective and accurate monitoring is critical to uptime and performance. Paessler Router Traffic Grapher (PRTG software) is suitable for all types of businesses due to its application flexibility in website, network, ping, bandwidth, uptime, and SQL server monitoring. At Protected Harbor, the PRTG program communicates with all network devices such as servers, routers, switches, access points, and VMs. It logs historical monitoring data and facilitates the detection of malicious programs and intruders.

Other similar log monitoring programs are Nagios and Observium. Observium aids in monitoring the infrastructure with multiple supported devices such as networks using the Simple Network Management Protocol. Easy-to-use capabilities such as the user interface and statistical data display assist Observium users to utilize it. Another option is Datadog, which combines infrastructure surveillance, log management, and application performance tracking to ensure real-time notification and response of infrastructure failures. It aggregates different events and metrics and allows a customizable view to offer efficiency in the monitoring of the network functionalities.

FAILOVER CLUSTERING

Virtualization offers security benefits in the server environment because every VM has its unique privacy, such as separate authentication and authorization rules. Each also has distinct names, file, and process system spaces.
To enhance protection, there is no administrator access to the VM, and our monitoring systems are always alerted to identify any approaching intrusion.

(BREAK OUT) PRO TIP - Understanding the workload of the VM and putting it on appropriate storage for that workload is everything. Bad storage = bad virtual machine.

It is critical to understand that beyond security, virtualization also provides failover for data protection. In this setup, a VM can switch automatically and seamlessly to another node and lessen the impact on end-users. The host now becomes hardware independent and mobile. Failover clustering allows for disaster recovery to replicate the VM to another host in real-time. This is high availability technology because it can decrease or eliminate downtime.

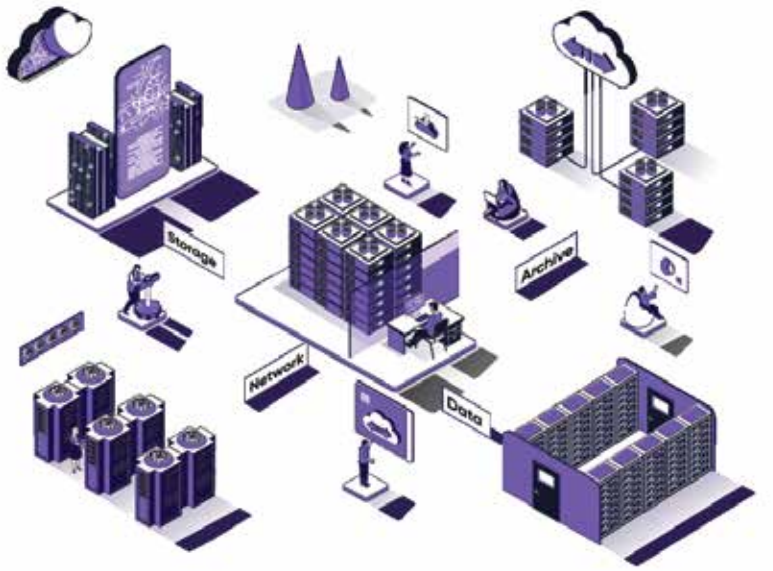
BACKUPS

System backups in the server environment are essential, as they lead to quick file access, promote operating system recovery, and safeguard an organization against failed network devices. Data obfuscation exists in backups and occurs through encryption and tokenization. Users also have no access to the backup data, which eliminates chances of data interferences. The backup server takes backup without the VM knowledge and stores it so that even the system administrator cannot obtain it. The container does not allow data sharing to avoid contacting virus-affected records.

CLOSING THOUGHTS

Firewalls and switches have an essential role in enhancing security and efficient performance. For example, a primary firewall exists in the normal functioning mode and handles network traffic. The secondary firewall is always in a standby state and takes over whenever the primary firewall fails to work. Both firewalls enhance protection by blocking domain names, monitoring network traffic, promoting Creating a secure server environment requires IT professionals to understand an organization's systems, workload, and potential threat surface.

Due to the increased application of technology, such as for e-health and telehealth, businesses should store their information in private cloud networks to advance security levels. System architects must comprehend the primary users of the infrastructure and ensure that they easily obtain resources. They should also accommodate future business growth and expansion by adopting modular system design. Proper data storage using devices such as HDDs and SSDs must incorporate the determination of accessibility issues, protection, management, and reduce user account compromises. , providing access control, and preventing hackers and malicious programs like Trojan. In our setup, firewalls utilize synchronized connections between the two components, and as a result, all modifications happening are mirrored.



Security at endpoint devices like smartphones, tablets, and laptops should be prioritized, as they are one of the most popular ways to target enterprise networks due to their vulnerability. User management in server environments is critical to protect such devices and control user access to server resources and data sharing and reduce the risk of account compromise. Too often guess users are left enabled long after their purpose has ended. Usually assigned simple passwords, like "Test123", "CompanyGuest", or "Password1$," attackers have an easier path to compromising the system.

Switches and firewalls are fundamental in promoting system performance. Proper configuration of any network components—such as uplinks, ISPs, VLANs, firewalls, hosts, VMs, and backups—boosts security and improves performance. System defense should be a considerable concern for any company due to increased cyberattacks.

ABOUT PROTECTED HARBOR

Protected Harbor provides customized data center infrastructure management and application 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 highest 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 possible cost, regardless of location, and cloud provider. From infrastructure design to network operations including security, storage, connectivity, remediation, monitoring, and more. Protected Data Center provides end-to-end support to secure deployments of complex enterprise applications to protect your technology infrastructure investments.

Like everyone else, we offer Cybersecurity, Enterprise Networking, Infrastructure Design, Network Configuration, 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.
Learn more at www.protecteddatacenter.com.