ENPM 686 (0101) INFORMATION ASSURANCE

FINAL PROJECT PAPER ON

**SECURING HORIZON INC, A COMPUTER MANUFACTURING COMPANY**

AAKASH RAMAN (UID: 119211663)

DHANASHRI DHANE (UID: 119396315)

# Index

## Introduction:

The main objective of this project paper is to assess, identify, mitigate, and improve the Security Posture of Horizon Inc, a small-scale Computer Manufacturing company. As a recently established company, Horizon Inc has been the victim of multiple Cyber attacks and does not have proper policies, procedures, and technical controls in place to stop these attacks. This paper outlines the current issues of Horizon Inc with a brief overview of its threat landscape considering assets being impacted. Furthermore, it provides the main objectives along with how some of its critical assets were affected. It also details how the Proposed Plan helps to counter the current/future problems faced by Horizon Inc. We are concluding this paper with a cost estimation and a secured architectural diagram of Horizon Inc in comparison to the current architecture as well.

## Assets of Horizon Inc to be Secured:

1) **Intellectual Property**: Proprietary products, design plans, product information, serial numbers, Copyrights, legal paperwork, and Trade Secrets of device developments. (*Security Label: Top Secret*)
2) **Hardware Modules**: 2 Primary MySQL Production Database Servers, 2 MySQL Secondary Databases, 2 Cisco C921-4P Routers, 10 Linux Hosts, 20 Windows Hosts, and 10 Work From Home Laptops and electronic components used in making the products of Horizon Inc. (*Security Label: Top Secret*)
3) **Software Modules**: 3 Apache Virtual Production Web Servers, “Beyond Horizon” Web Application. (*Security Label: Secret*)
4) **Physical Facilities**: An On-Premises facility, Storage warehouses. (*Security Label: Confidential*)

5) **Human Resources**: All Horizon Inc's employees.
6) **Customer Data**: Customer/client payment plan, Credit Card information, and Personally Identifiable Information (PII) like Names, Addresses, Occupations, Payroll details, Phone Numbers, Email Addresses, and Social Security Numbers. (*Security Label: Top Secret*)
7) **Supply Chain Data**: Electronic components manufactured by different vendors, and third-party product suppliers' information with their delivery schedules and inventory levels. (*Security Label: Secret*)

## Current Problems:

Horizon Inc is facing multiple vulnerabilities across its Network, Web Application, Endpoints, Operating Systems, and Employee front. There is only a budget of **$600K** and of any 5 systems that have been compromised with the "**NotPetya**" Ransomware, 3 of those systems were not recoverable. Multiple Spear Phishing campaigns were launched on most of its 200 employees along with periodic DDoS attacks on its "**Beyond Horizon**" Web Application login portal. Furthermore, Horizon Inc's single Web Server is locally hosted and hence has limited scalability. There is a separate network segment for Linux and Windows environments that are used for scientific and administrative tasks without any built-in security. Also, some employees have been assigned remote devices for work but there is no planning/procedures in place for employee login authentication monitoring and data security. The only Security Device owned by the company is a Layer 2 Firewall that only detects Layer 2 attacks and as customers use Credit Cards to buy products, there is a requirement to enforce PCI-DSS Compliance which is currently lacking.

## Threat Landscape of Horizon Inc:

### Internal Threats:

Internal Threats may come in the form of disgruntled/unsatisfied employees that can compromise the Proprietary information of the company. For Horizon Inc, the assets subject to insider threats are current business goals for the next fiscal year, Intellectual property and customers PII, etc.

### External Threats:

External Threats come from outside and aim to cause a significant business impact on the company's assets. For Horizon Inc, the external threat is the "**NotPetya**" Ransomware. Sometimes, attackers that attack the Supply-Chain or other third parties can also be a threat.

### Natural Disasters:

This is a form of an environmental threat such as Floods, Hurricanes, and Tornadoes. These natural calamities can destroy Data Centers, Homes, Offices, etc. Currently, no such loss is experienced by Horizon Inc under this threat.

## Goals/Objectives of the Proposed Solution:

The Proposed Solution for securing Horizon Inc must have the following goals/objectives:

### Ransomware Mitigation:

The first priority is to mitigate Ransomware as 3 out of 5 devices' data were lost. Assets of Horizon Inc like Proprietary products, design plans, product information, serial numbers, copyrights, legal paperwork, Customer/client payment details, Names, Addresses, Payroll details, Phone Numbers, Email Addresses, and Social Security Numbers must be protected first to prevent competitors from buying it from the Dark Web/ Hacker Forums. This is crucial to protect the "Confidentiality" & "Integrity" of Horizon Inc's information.

**DDoS Mitigation:**

The second priority is to cater to the DDoS attacks that are attacking the "**Beyond Horizon**" client login page. This security measure ensures the "Availability" of Horizon Inc's Web Application and also the continuity of their business operations.

**PCI-DSS Compliance:**

The third priority is to ensure PCI-DSS Compliance as it is a regulation across the globe. As Horizon Inc processes Credit Cards, there need to be best practices in place to maintain Compliance and periodic auditing which is crucial for various legal activities.

**Hosting & Securing Horizon Inc's Web Server:**

The fourth priority is to improve the Scalability and Security of Horizon Inc, by load-balancing its Web Servers to make them accessible from all across the globe and prevent them from acting as a Single Point of Failure.

**Lack of Security between Internal Linux & Windows Environments:**

The fifth priority is regarding the protection of the Linux & Windows environments. Network & Endpoint Security is lacking in these environments and stronger Endpoint Detection and Response (EDR) should be built in.

**Reducing Spear Phishing:**

The sixth priority is to ensure Horizon Inc's employees are properly trained to be able to identify, detect and respond/report to Social Engineering attacks such as Phishing.

**Work From Home Setup Security:**

The seventh priority is to plan and protect the extended business continuity initiative; Work From Home mode of operation for Horizon Inc's employees from any unknowing physical or cyber-attacks.

## Proposed Plan Details:

### Ransomware & Spear Phishing Mitigation:

**Assets Impacted:** Horizon Inc was a victim of the "NotPetya" Ransomware which impacted crucial assets like Intellectual Property including new computer designs/software code, supply chain vendors' contact details, and product delivery schedules. Any 3 of the 5 machines which were encrypted by the attacker through Spear Phishing by sending Phishing E-Mails to Horizon Inc's HR Department, the attacker also has the employee's Name, Email address, Date of Birth, and employee IDs. This mainly caused a **loss in productivity** as one of the employees from the HR Department got his credentials compromised which was then temporarily suspended to prevent data theft by the attacker, and so the pipelined work was severely impacted.

**Solutions:** The best solution to a Ransomware attack is to perform regular **Incremental Data Backups** roughly every 7 - 14 days to secure the 2 MySQL Primary Production Databases with asset inventory and manufacturing data, Customer PII, employee, and vendor details. Every week an Incremental Backup of all the Linux Production Web Server and Windows Active Directory Servers would be necessary. These backups can then be utilized to spin up the infrastructure if any data is stolen in such an attack and legal proceedings can be taken against Ransomware. To incorporate Disaster Recovery, an **additional 2 Secondary Production Database Servers** will also be added, and data would be replicated into them periodically in 2-3 days as a proactive plan to maintain the "**Availability**" of the Databases.

These generally cost around **$1000** per month via Cloud providers like AWS and these Backups can be stored in Warm Storage sites (Storage locations that are designed to store Data Backups) that cost around **$0.05** per GB of data for an AWS Simple Storage Service (S3) Bucket. Conducting

regular **Patch Management** will ensure the systems are updated with recent security patches and enforcing **Multi-Factor Authentication** adds an extra security layer.

**Spear Phishing** can be mitigated by ensuring all employees at Horizon Inc follow proper policies and procedures and have adequate security awareness knowledge. To educate the employees, regular Phishing campaigns must be enforced by the security team to identify, detect, and respond to any Phishing/Smishing attempts. A video course module with quizzes can be set up for around **$1850**. Alternatively, Anti-Phishing Software like **Cofense** can be used for advanced Spam Filtering and Malicious URL /File Detection which costs **$10** per user per year.

**Proposed Plan for DDoS Mitigation:**

**Assets Impacted:** Horizon Inc's most crucial asset, a Web Application named "***Beyond Horizon***" is the victim of DDoS (Distributed Denial of Service) attacks where multiple botnets continuously bombard the Web Application to flood it and disrupt the business-critical operations. Also, a single locally hosted Web Server is overwhelmed with multiple DDoS requests. This **disruptive availability** impacted the **sales, profit,** and **marketing efforts** of Horizon Inc which was degraded by **26%** in the last fiscal year as per their report.

**Solutions:** Horizon Inc can utilize Cloud Providers like AWS that offer DDoS protection through their **AWS WAF** and **Shield** services. These services follow a Pay-as-you-Go model the AWS Shield Advanced subscription costs roughly **$3000** per month. AWS Shield Advanced offers protection against more sophisticated DDoS attacks that target applications. It also includes features like 24/7 access to DDoS Response Team, DDoS cost protection, blacklisting known malicious IPs, and advanced real-time metrics and reporting by which "Beyond Horizon" will be always "Available to its customers service to buy/return/report the products. Additionally, we are

suggesting Horizon Inc use AWS Route 53, a DNS service to host www.horizon.com globally (later in this paper), hence, a Cloud Security Architect should be hired to set up AWS WAF+Shield and AWS Route 53 hosted zones. His/her salary would be **$157,376** annually.

Alternatively, companies like **Cloudflare** offer DDoS Protection services with a **$2400** annual subscription. In case any attackers are still in the system, they can also create a **Honeynet**, of another supposedly present Database Server which has "confidential customer information" to analyze the attacker's tactics, techniques, and procedures and use that knowledge to build their defenses. To set up a Honeynet and maintain it, it will cost roughly **$2500** annually.

**Proposed Plan for Web Server Hosting & Security:**

**Assets Impacted:** A locally hosted production Web Server of Horizon Inc is single-handedly providing customer support and advertising products for sale. This not only **affects the scalability** of the environment but also **limits Horizon Inc's reach** to a wider customer network to increase revenue.

**Solutions:** To mitigate this impact on critical assets and to load-balance the Web Server functionalities, Horizon Inc should utilize a cost-effective Cloud Computing solution. One such technique is hosting the production Web Server workload on **AWS Route 53**, an AWS-based Domain Name Service that uses a combination of Load Balancers and Apache Virtual Web Servers that can improve the scalability along with Horizon Inc's service reach globally. This way, multiple Web Servers can handle advertising and customer support queries flexibly. To secure the Web Application, **AWS Web Application Firewall (WAF)** can be integrated with Route 53 to deter all the common Web Application Attacks (OWASP 10) like **SQL Injections**, **Cross-Site-Scripting (XSS)**, **Cross-Site Request Forgery (XSRF)**, etc. AWS WAF uses a **WebACL** (Web

Access Control List) uses a combination of WAF rules to monitor incoming HTTP and HTTPS requests. WAF rules can be AWS managed or custom created by the Cloud Security Administrator of Horizon Inc to monitor, block or allow network traffic based on HTTP/HTTPS headers, URIs, and IP addresses. Let us assume that Horizon Inc has 1 hosted zone called, "www.horizon.com", which receives 1 Million DNS Queries, then the cost is:

*Hosted Zone: $0.50, Queries: $0.40x1 = $0.40 Hence, $0.50+$0.40 =* ***$0.90 Monthly***

The cost to set up AWS WAF depends on the type of Web Requests and the rules built into the WAF. Generally, Web Requests are processed at **$0.60** per Million requests and the rules deployed are **$5** per rule per month. For future scope, Horizon Inc can utilize CloudFront which is a Content Delivery Network service from AWS and easy to integrate with AWS Route 53 to provide low latency and faster data transfer speed around the globe.

**Proposed Plan for PCI-DSS Compliance:**

**Assets Impacted:** The main asset affected is the **payment card details** of Horizon Inc's customers/clients along with their bank account information, and payment/subscription plans. Additionally, Hardware and Networking devices such as routers, and 2 main Production Databases must be highly secured as the cardholders' data is stored in the on-premises/virtual Database servers and this security implementation is currently not in place.

**Solutions:** PCI-DSS Compliance is a form of Security standard that ensures that all companies that store, process, accept or transmit credit card information at rest or during transmission do so in a secure environment. Horizon Inc can adhere to PCI-DSS Compliance by following its best practices and conducting regular Security Audits across the entire company infrastructure by a **Qualified Security Assessor (QSA)**.

Following are the PCI-DSS Requirements that must be met immediately by Horizon Inc:

- ***Detect and Report Security Control Failures****:* This is required to detect/prevent any Indicators of Compromise (IOCs) and can be satisfied using NIPS/NIDS & HIPS/HIDS.
- ***Install critical security patches on all system components and software****:* This is done by regular Patch Management of Horizon Inc's production environment's Web Server, Load Balancers Database Servers, and also employee workstations on-site and remote.
- ***Enforce 90-day password change for user passwords and passphrases****:* This is done by enforcing good password policies for all admin, user, guest, and service accounts too.
- ***Provide security awareness training for all personnel annually and upon hire****:* This is achieved by mitigating Spear Phishing and providing Phishing awareness training.
- ***Perform external and internal network, application, and Segmentation Penetration Testing****:* Once the proposed plan is set up by around 75%, Horizon Inc can invest in an External Penetration Testing firm as a proactive approach to secure networks.
- ***Review and test the Incident Response Plan****:* Additionally, Horizon Inc's security team can invest time in Risk Management and Incident Response planning to adopt a Defense-in-Depth approach.

The cost to set up PCI-DSS costs roughly around **$20,000** annually and conducting a Security Audit costs **$10,000** annually. Horizon Inc can also use the Splunk SIEM, which has built-in Compliance checks for Compliance Management.

**Proposed Plan for Linux Host & Network Security:**

**Assets Impacted:** From the 10 Linux hosts utilized for scientific research purposes, 2 were the victim of a **"Dirty Copy-On-Write (COW)" vulnerability** where the Linux kernel's read-only

memory mapping was exploited by an attacker to gain privileged access. Hence, the impacted assets include these 2 servers, Trademarks, Product Designs, and futuristic business models.

**Solutions:** Regularly scheduled **Patch Management** is crucial for Horizon Inc to keep all its endpoints up-to-date. We are suggesting a **NIDS/NIPS** (Network Intrusion Detection/Prevention System) to detect/prevent any Network attack, and also the configuration of a **SIEM** (Security Incident and Event Management) solution connected to ingest logs from all network and user actions. A popular SIEM is **Splunk**, which has Log Management, Threat Intelligence, and Incident Response to detect investigate, and solve security incidents. Horizon Inc can use Open-Source IDS/IPS systems like **Suricata**/**Snort** or even commercially available IDS/IPS solutions like **Cisco's NGIPS**. To set up a commercial IDS/IPS solution, it will roughly cost **$4500,** and maintaining it will cost around **$1000**. Strong Network Security algorithms like **AES-512, ECC/RSA** should be used for encryption and **SHA-512** should be used for hashing. Host Based Firewalls with IDS/IPS functionalities like **Trend Micro Deep Security** should also be used for additional security checks between Host connections. They cost around **$3000** and maintenance charges are around **$1000** per month. Lastly, EDR (Endpoint Detection and Response) tool like **CrowdStrike's Falcon Insight XDR** offers continuous detection and response for all hosts in real-time. It incorporates **Threat-Intelligence** along with **AI-Driven** Insights with a price starting at **$299.95** annually.

**Secure Boot** or **UEFI Secure Boot** should also be enabled to ensure no Boot Time attacks on 10 Linux Hosts. Good administrative controls ensure that **Root/Admin** logins are monitored and **Multi-Factor Authentication** (MFA) should also be enabled if any host is performing an elevated access operation. **Application Whitelisting** can also be used to ensure each Host has only approved applications by Horizon Inc. Horizon Inc can also add complex **Password Policies** and

**RBAC** (**Role Based Access Control**) to enforce the **Principle of Least Privileges**. By this, employees will have strong passwords to prevent Credential Stuffing/Brute Force/Dictionary attacks and utilize access to the infrastructure according to their job role.

Finally, **Vulnerability Scanning** of the internal assets that is Linux, and Windows Hosts network, Production Database, and Web Server every 3 days a week to reduce the number of **False Positives** and also identify any vulnerabilities as a proactive approach.

**Proposed Plan for Windows Host & Network Security:**

**Assets Impacted:** Of the 20 Windows Endpoints being used for Administrative tasks that were used for administrative tasks, 5 of them fell victim to the **EternalBlue exploit**, which allows any attacker to perform Remote Code Execution by crafting special packets over the SMB protocol. This affects all Windows systems that communicate over the **SMBv1** protocol. Hence, once an attacker gets access to one Windows host, it is very easy to access the entire Windows network.

**Solutions:** Similar to the Linux section, regular **Patch Management,** using a **NIPS/NIDS,** a **SIEM** solution for logging and monitoring, using strong cryptographic algorithms, and using Open-Source/ Commercial IDS/IPS Systems along with security for Container applications all help provide strong Network Security for Windows environments. Some security best practices for Windows Systems include using **RDP** and **SMBv3** for Remote Connections to combat the main problem in our current environment. The **Active Directory** hierarchy contains the Domain Controller that is responsible for managing all the other Windows systems of an enterprise. This Domain Controller can have access to all the other Windows systems which contain Horizon Inc's Asset Inventory, computer orders placed, vendor details, and customer details. Some best practices for monitoring and securing Active Directory can be followed by Microsoft.

Windows Host Security is also similar to Linux Host Security but with an extra addition of enabling **Device Gaurd**, **Windows Defender Application Control,** and **Credential Gaurd** which are Microsoft's in-built Security controls. Using EDR, HIPS/HIDS, and MFA are all strong technical recommendations for Endpoint Security. Administrative Controls such as **Application Whitelisting,** monitoring **Root/Admin** logins, and maintaining complex **password policies** and **RBAC** ensure that all employees are provided strong credentials and are granted privileges only for the actions they are provided to perform.

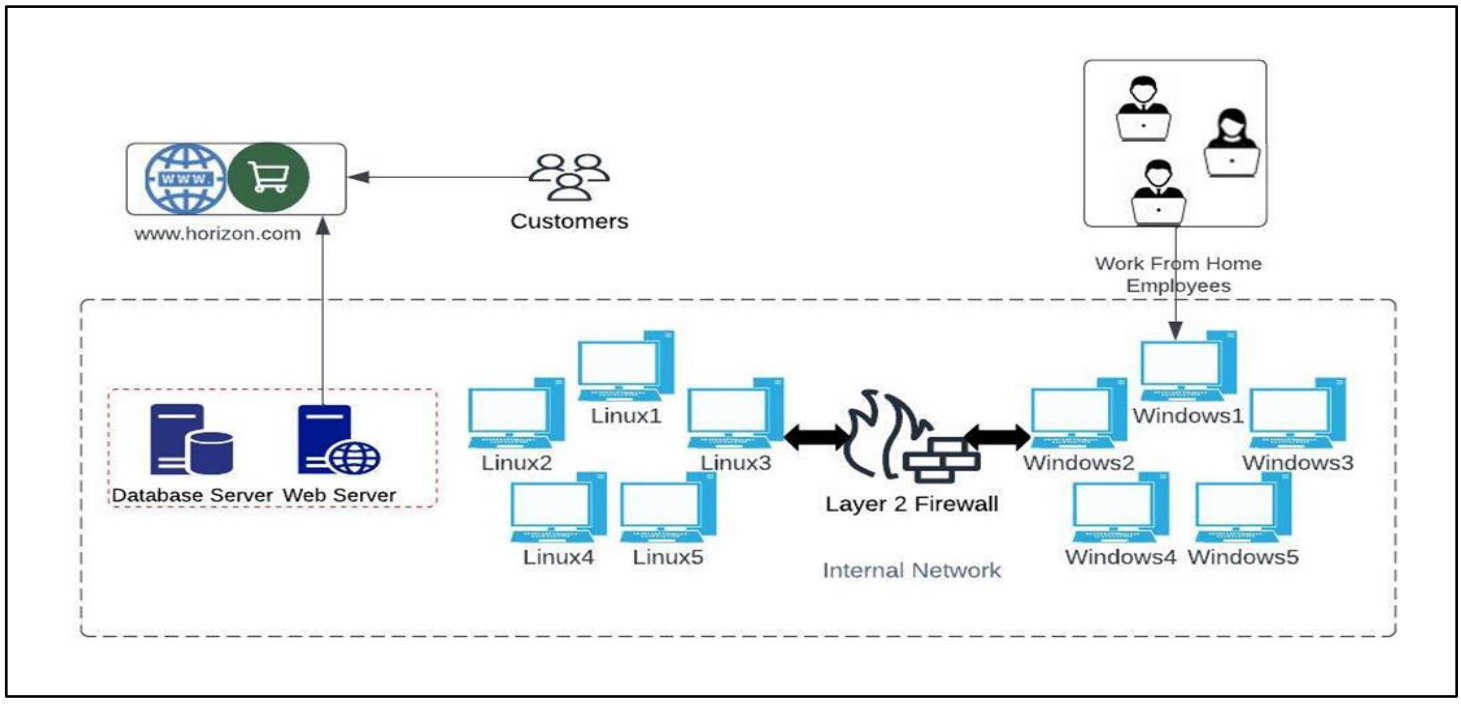
**Proposed Plan for Work-From-Home Setup Security:**

**Assets Impacted:** Scott, the CEO of Horizon Inc lost his corporate MacOS laptop and personal iPhone during travel, and some Product Designs were stolen by Horizon Inc's competitor, Statue Inc. This is because Horizon Inc currently follows a **BYOD** (Bring Your Own Device) policy to provide flexibility for its employees without adequate security planning and this **data breach** incident confirmed the security loophole. Hence, the main assets here are any corporate laptop/mobile devices with intellectual data, or supply chain vendor details of Horizon Inc. **Solutions:** As a new working model, the Work-From-Home Setup must follow ideal security best practices to prevent any vulnerability from arising through this channel. This includes **Mobile Device Management (MDM), VPN** usage, **GeoIP** or **Geolocation**, and a **DLP** (Data Loss Prevention) solution for the production workload assets listed above. MDM techniques can also be applied to Windows, Linux, and MacOS-based computers using **Jamf Connect** for authenticated logins and real-time monitoring, along with support for MFA. We can segment the personal and work profiles in any device under the BYOD scheme to keep corporate data secured from unauthorized exposure which also enables Remote Wipe in case a device gets compromised.

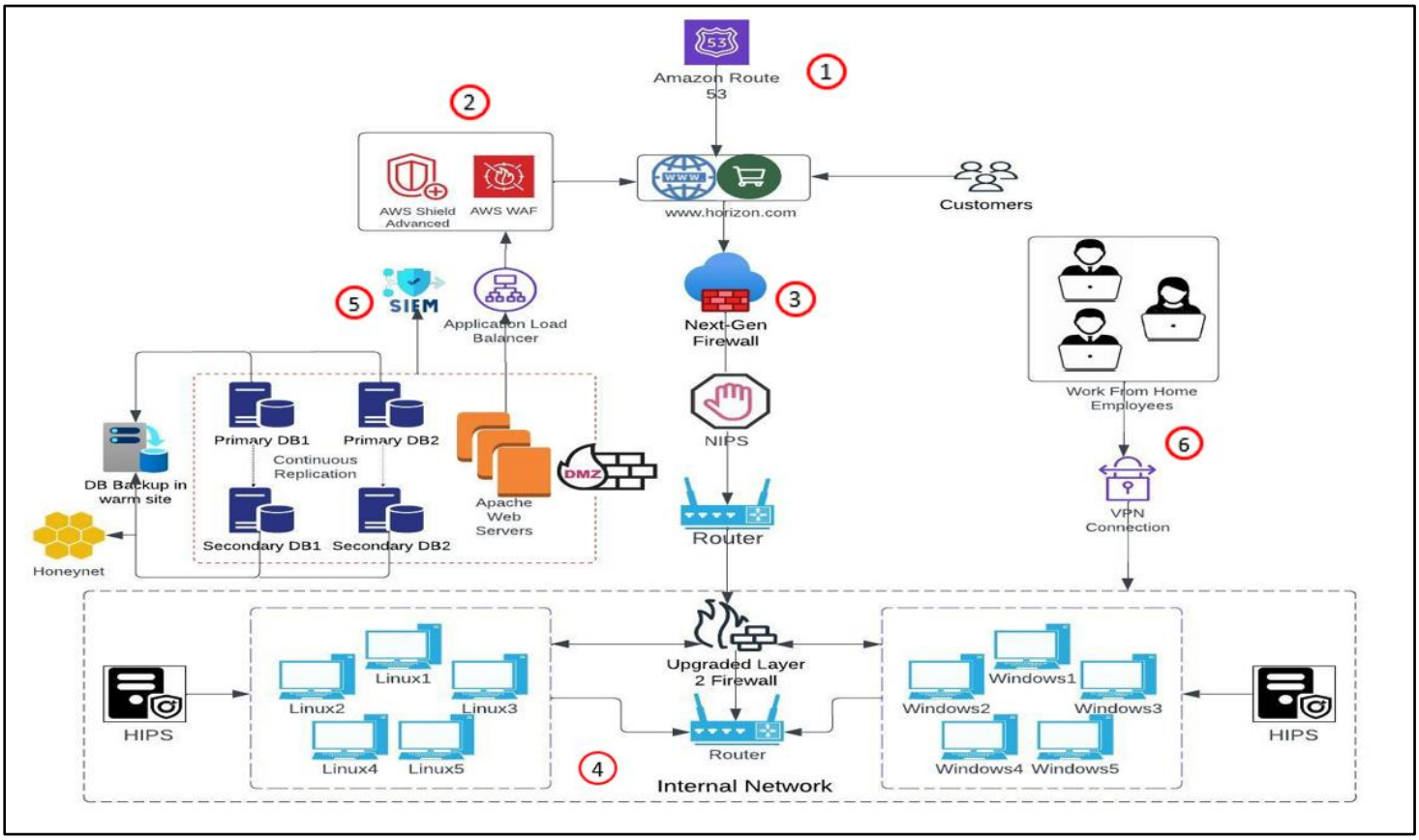
It costs around **$24** for an annual subscription per device. A Data Loss Prevention (DLP) solution can detect and prevent whenever large amounts of data are trying to be exfiltrated from a network at any point in time. Hence, even if the user's credentials get hacked, no confidential data can leave the device. **Forcepoint DLP** is a DLP solution that has Unified Data Protection, Behavioral Awareness, and Automation to help identify any exfiltration attempts. The Forcepoint DLP Suite with IP Protection costs **$60.99** annually per device.

A **Virtual Private Network (VPN)** provides a secured encryption tunnel between remote employees and the internal network. All remote employees can use **OpenVPN** to gain access to Horizon Inc's internal network. An OpenVPN Access Server costs **$150** per user per year.

## Current Architectural Diagram



## Proposed Architectural Diagram




The Proposed Solution of Horizon Inc is a hybrid architecture of both an On-Premise and Cloud environment which illustrates the security measures proposed in this study in comparison with the existing infrastructure with multiple issues without built-in security. The explanation is divided into 6 major sections (highlighted in red circle):

1. www.horizon.com is hosted using AWS Route 53 and we can see that customers are logging in securely through the Web Application or web interface to buy various products offered by the company. In the initial diagram, this was hosted locally with no security.
2. This client login portal is secured from DDoS attacks, Web Application attacks like SQL Injection and Cross Site Scripting, etc with the help of AWS Shield Advanced and AWS WAF respectively. In the initial diagram, DDoS Mitigation was absent.

3. Advanced Next-Generation firewall with web traffic filtering, URL blocking, Quality of Service (QoS) functionality, a Network Intrusion Prevention System (NIPS), and a Router are keeping the environment secured from external threats proactively. None of these tools other than the Layer 2 Firewall was deployed.
4. The internal assets network of Linux and Windows machines along with other devices such as printers, fax machines, routers, and desktops are secured with an upgraded Layer 2 Firewall & Router along with Host Based Intrusion Prevention (HIPS) and Endpoint Detection and Response (EDR) tools using the Defense-in-Depth approach. These were absent in the initial infrastructure.
5. We are suggesting keeping the Primary & Secondary Databases & Apache Web Servers in a Demilitarized Zone (DMZ) which is a subnetwork that contains data that needs to be exposed to a wide network such as the Internet. Finally, this is ten connected to an Application Load Balancer. We are maintaining backups of Databases as a proactive measure for data loss or Ransomware attacks. Moreover, this portion is enabled for logging and monitoring using a SIEM solution like Splunk. Furthermore, all entries in the Database will be Anonymized/Masked to balance both security and usability and are replicated with Secondary Database Servers too. A Honeynet is also present to act like a decoy for potential attackers. These measures were absent in the current environment.
6. To secure the extended Work From Home devices, we are implementing the VPN connections technology where employees can securely connect to the network using OpenVPN. Also, their devices will be monitored remotely by the IT team using JamfConnect, a Mobile Device Management service. They will also have the Forcepoint

DLP built-in to prevent any data from getting compromised from these remote devices. There was no DLP, VPN, or MDM solution in the initial environment.

## Estimated Cost to Secure Horizon Inc

The following table shows the estimated implementation cost for the Proposed Plan with a given budget of $600K. Please refer to this section for the asset information included in the costing.

| **Assets** | **Number of Entities** | **Entity split-up Cost** | **Total Cost in $ (Annual)** | **Costing References** |
|---|---|---|---|---|
| Phishing Campaign | 200 Employees | | 1850 | Link |
| Anti Phishing Software | 200 Employees | 10 * 200 | 2000 | Link |
| Incremental Backups in Warm Site | 50 GB per day | 0.05 * 50 | 2.5 | Link |
| Apache Web Servers | 3 | 3 * 1576 | 4728 | Link |
| Application Load Balancer | 1 | 12 * 88.78 | 1065.36 | Link |
| DDoS Vendor Cloudflare | 1 | | 2400 | Link |
| Primary Production MySQL Databases (Cluster Carrier Grade Edition) | 2 | 2 * 10000 | 20000 | Link |
| Secondary Production MySQL Databases | 2 | 2 * 10000 | 20000 | Link |
| Cisco Routers (C921-4P) | 2 | 2 * 700 | 1400 | Link |
| AWS Shield Advanced | 1 | 12 * 3000 | 36000 | Link |
| Cloud Security Architect Salary | | 1 * 158376 | 157376 | Link |
| 2 Security Administrator's Salary | | 2 * 91763 | 183526 | Link |
| Web Hosting Route 53-1 zone | 1 | | 10.8 | Link |
| Web Application Firewall – 50 rules | 1 | 5 * 50 | 250 | Link |
| PCI-DSS Compliance + Auditing | | 20000 + 10000 | 30000 | Link |
| Next-Gen Firewall and NIPS (Cisco NGIPS) | 1 | | 31900 | Link |
| CrowdStrike EDR and HIPS | 240 (All Endpoints) | 240* 299.95 | 71988 | Link |
| HoneyNet Setup | 1 | 1 * 2500 | 2500 | Link |
| OpenVPN | 10 | 70 * 12 * 10 | 8400 | Link |
| Jamf Connect | 10 | 24 * 10 | 240 | Link |
| Forcepoint DLP | 10 | 60.99 * 10 | 609.9 | Link |
| **Total** | | | **576246.56** | |

The total cost of the Proposed Plan comes to **$5,76,246.56**, which is well within the given budget.

## Conclusion:

In conclusion, Horizon Inc must incorporate this Proposed Plan in phases into their architecture and prioritize them according to what is mentioned in this document. If they follow this proposed flow, a majority of their risk will be reduced, they will comply with the standard Information Security laws/policies and they will be able to boost their business securely.

## References:


- Kudisch, E. (2016). *The backup*. Amazon. Retrieved April 30, 2023, from https://aws.amazon.com/backup/pricing/?nc=sn&loc=3
- *Phishing protection solutions: Cofense email security*. from https://cofense.com/
- *Shield*. Amazon. Retrieved April 30, 2023, from https://aws.amazon.com/shield/pricing/
- *The key to enterprise resilience*. Splunk, from https://www.splunk.com/
- *Cisco secure IPS*. Cisco. (2023, January 6). Retrieved April 30, 2023, from https://www.cisco.com/c/en/us/products/security/ngips/index.html
- *CrowdStrike* from https://www.crowdstrike.com/products/endpoint-security/
- https://learn.jamf.com/bundle/jamf-connect-documentation-current/page/Jamf_Connect_Documentation.html
- *DLP Data Loss Prevention*. Forcepoint. (2023, April 28). Retrieved April 30, 2023, from https://www.forcepoint.com/product/dlp-data-loss-prevention
- *PCI DSS checklist from https://www.drummondgroup.com/pci-dss-checklist/*
- Burdova, C. (2023, February 23). What is EternalBlue and why is the MS17-010 exploit still relevant? Retrieved May 2, 2023, from https://www.avast.com/c-eternalblue