CIS495 Course Project

- Skylar York

Goal

- We have been tasked to create and provide a functional network that will be contracted for 1 year.

- The three areas that will be covered in the initial roll-out is Washington DC metro area (National Institutes of Health), Los Angeles metro area (Cedars-Sinai), and Rochester, Minnesota (Mayo Clinic).

Objectives

1. Create a working network

2. The network is secure

3. Deadlines are met on time

HIPPA Rules

- Privacy Rule:
  - Data Protection and Privacy Regulations

HIPPA Rules

- Security Rule:
  - PHI and ePHI Protection Guidelines

HIPPA Rules

- Breach Notification Rule:
  - Data Breach Reporting Requirements

Equipment Specs: Cisco Firepower 9300

- Throughput
  - SM-40 – 55 Gigabits per second
  - SM-48 – 65 Gigabits per second
  - SM-56 – 70 Gigabits per second
  - SM-56x3 – 190 Gigabits per second
- Software Compatibility – Cisco Secure Firewall Adaptive Security Appliances (ASA) or Threat Detection (FTD) Software
- Notable Information
  - 8 x SFP+ Interfaces for Scalability
  - Cisco Malware Defense for Networks*
  - URL Filtering – 80 Categories and more than 280 million categorized

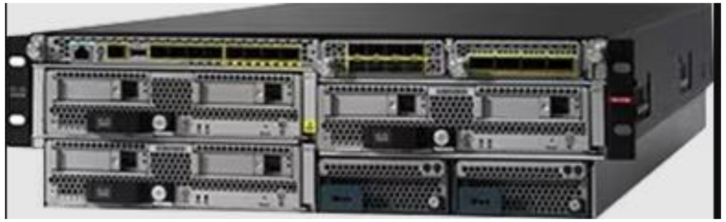


Figure 1: Cisco Firepower 9300 model SM-56. Adapted from "Cisco Firepower 93300 Series" by Cisco, 2021, Cisco Systems Inc. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/security/firepower-9000-series/datasheet-c78-742471.docx/_jcr_content/renditions/datasheet-c78-742471_0.png

Equipment Specs: Cisco 8608 Router

- Maximum Bandwidth – 12.8 Terrabits per second, maximum of 8 modular port adapters running at 1.6 Terrabits per second per MPA.
- MPA Variations
  - MPA-14H2FH-M
  - MPA-24Z-M
  - MPA-4FH-M

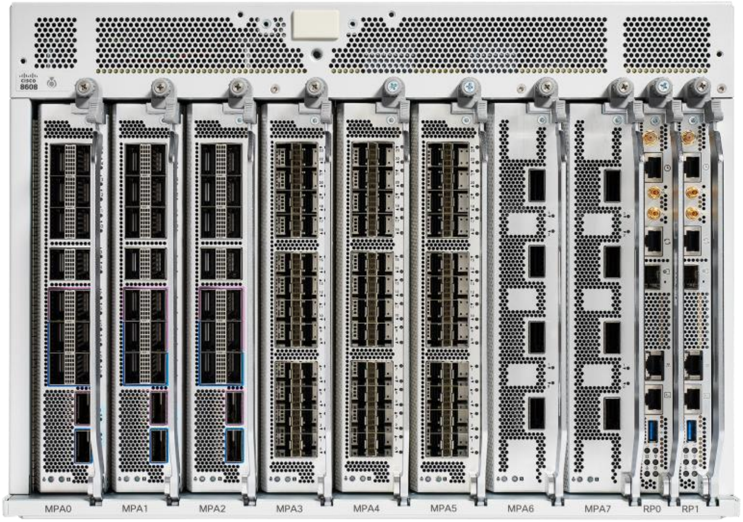
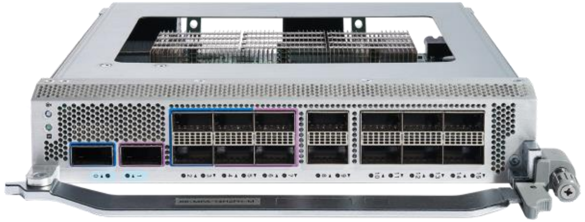
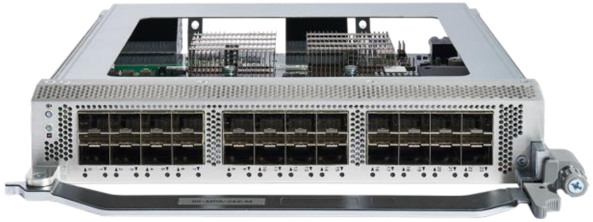
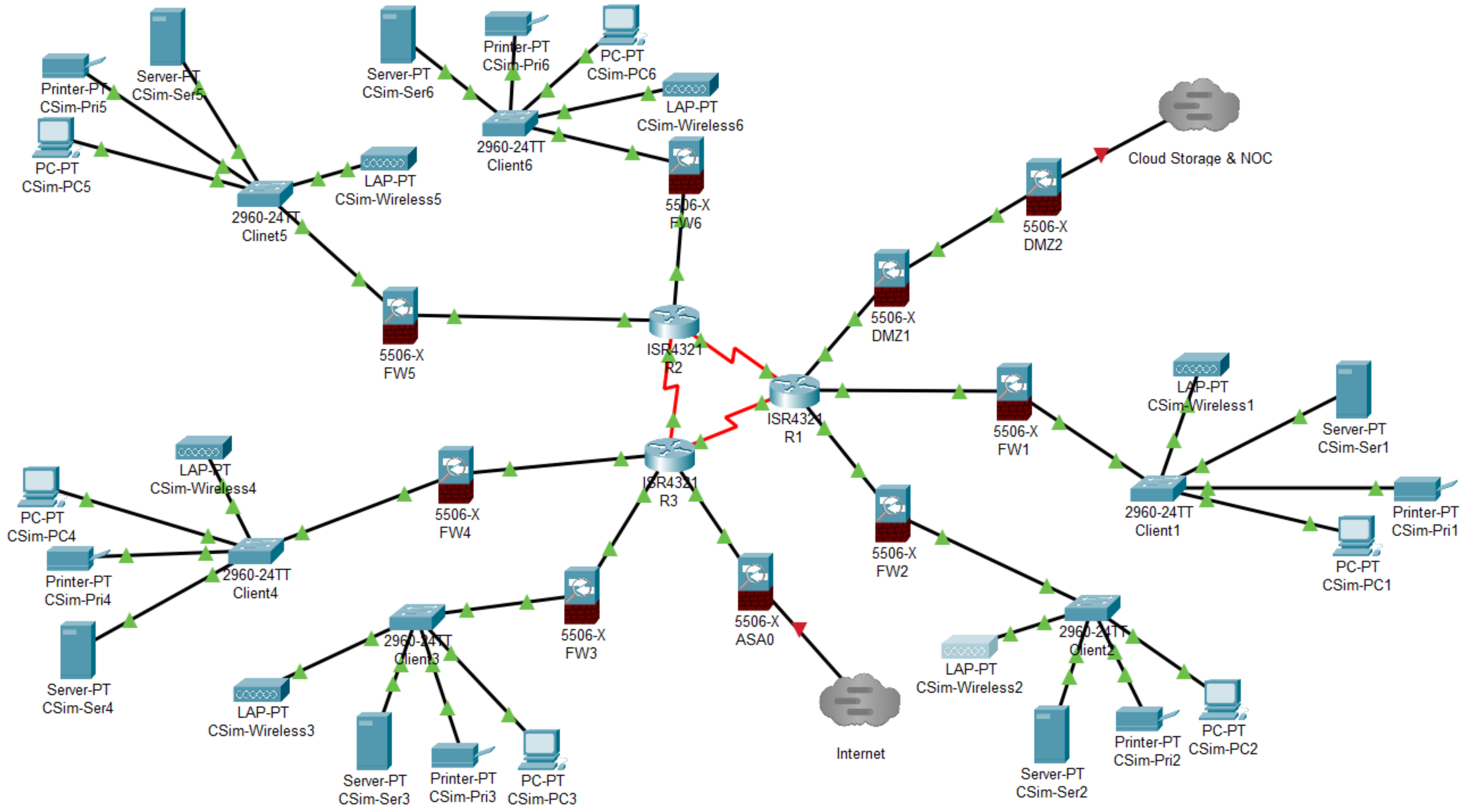


Figure 1: Front view of the Cisco 8608 Router with installed MPAs. Adapted from "Cisco 8608 router front view" by Cisco, 2023, Cisco Systems Inc. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/routers/8000-series-routers/8608-router-ds.docx/_jcr_content/renditions/8608-router-ds_0.png.






Printer-PT
CSim-Pri5
Server-PT
CSim-Ser5
PC-PT
CSim-PC5
LAP-PT
CSim-Wireless5
2960-24TT
Clinet5
Server-PT
CSim-Ser6
Printer-PT
CSim-Pri6
PC-PT
CSim-PC6
LAP-PT
CSim-Wireless6
2960-24TT
Client6
5506-X
FW6
5506-X
FW5
ISR4321
R2
Cloud Storage & NOC
5506-X
DMZ2
5506-X
DMZ1
ISR4321
R1
5506-X
FW1
LAP-PT
CSim-Wireless1
Server-PT
CSim-Ser1
2960-24TT
Client1
Printer-PT
CSim-Pri1
PC-PT
CSim-PC1
LAP-PT
CSim-Wireless4
PC-PT
CSim-PC4
Printer-PT
CSim-Pri4
2960-24TT
Client4
Server-PT
CSim-Ser4
5506-X
FW4
ISR4321
R3
5506-X
FW3
2960-24TT
Client3
LAP-PT
CSim-Wireless3
Server-PT
CSim-Ser3
Printer-PT
CSim-Pri3
PC-PT
CSim-PC3
5506-X
ASA0
Internet
5506-X
FW2
2960-24TT
Client2
LAP-PT
CSim-Wireless2
Server-PT
CSim-Ser2
Printer-PT
CSim-Pri2
PC-PT
CSim-PC2

- The three router formation is the center and each one will support 2 sites
- Firewalls exist between each entrance and exit to maintain high security
- Both wired and wireless internet options are supported

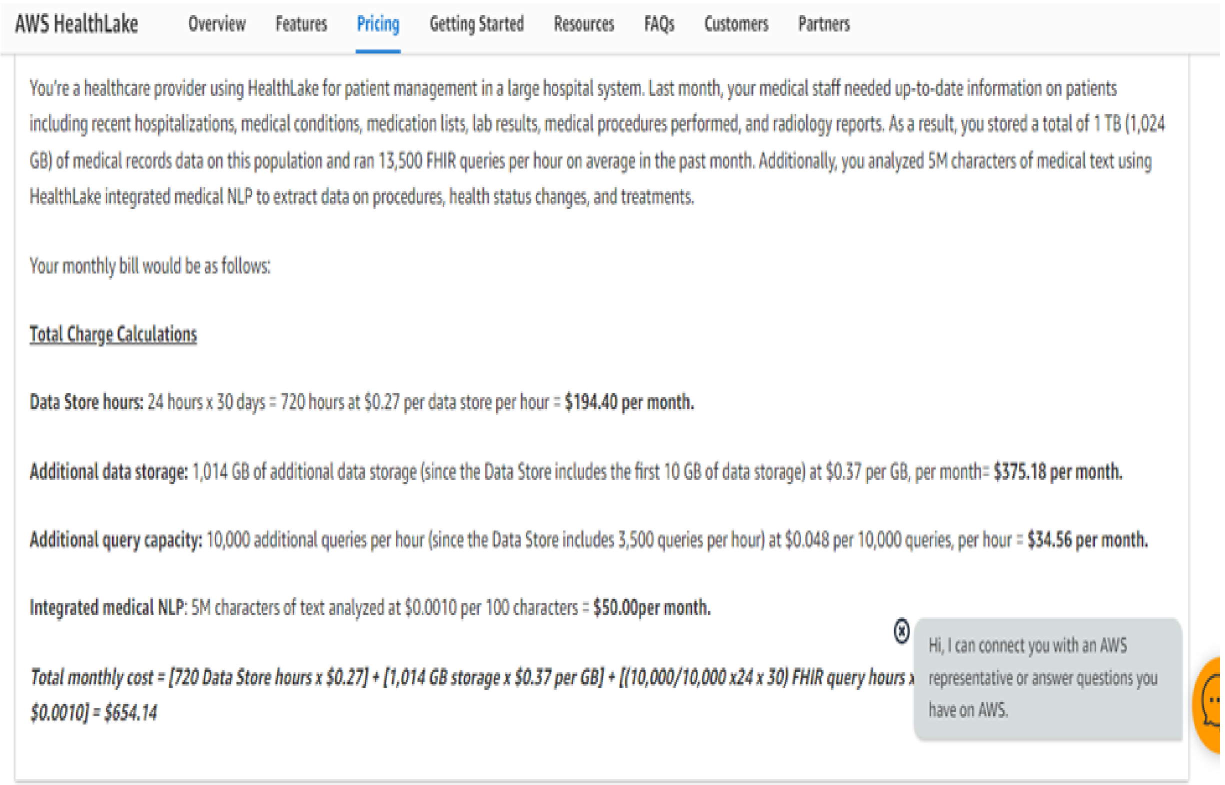
Database

- We will be using an AWS HealthLake database service.
- It has HIPAA-eligible functionalities. It enables healthcare organizations to securely store, transform, transact, and analyze health data at scale using FHIR (Fast Healthcare Interoperable Resources) APIs.
- It also features built-in natural language processing (NLP) models to extract meaningful medical information from raw health data.

Databases Security

- **AWS's Responsibilities**: AWS is responsible for the security "of" the cloud. This includes protecting the infrastructure that runs AWS services, including hardware, software, networking, and facilities. AWS ensures the security and integrity of their cloud infrastructure and offers services and features that help with compliance and security.
- **The Hospital's Responsibilities**:
- Data encryption: Ensuring that data is encrypted in transit and at rest.
- Access management: Implementing strong identity and access management policies.
- Network security: Setting up appropriate network access controls.
- Compliance: Ensuring that their use of AWS services complies with healthcare regulations like HIPAA (Health Insurance Portability and Accountability Act) in the U.S. and other relevant data protection laws.
- Application security: Securing any applications they host on AWS.

Cloud Service Cost



You're a healthcare provider using HealthLake for patient management in a large hospital system. Last month, your medical staff needed up-to-date information on patients including recent hospitalizations, medical conditions, medication lists, lab results, medical procedures performed, and radiology reports. As a result, you stored a total of 1 TB (1,024 GB) of medical records data on this population and ran 13,500 FHIR queries per hour on average in the past month. Additionally, you analyzed 5M characters of medical text using HealthLake integrated medical NLP to extract data on procedures, health status changes, and treatments.

Your monthly bill would be as follows:

Total Charge Calculations

Data Store hours: 24 hours x 30 days = 720 hours at $0.27 per data store per hour = **$194.40 per month.**

Additional data storage: 1,014 GB of additional data storage (since the Data Store includes the first 10 GB of data storage) at $0.37 per GB, per month= **$375.18 per month.**

Additional query capacity: 10,000 additional queries per hour (since the Data Store includes 3,500 queries per hour) at $0.048 per 10,000 queries, per hour = **$34.56 per month.**

Integrated medical NLP: 5M characters of text analyzed at $0.0010 per 100 characters = **$50.00per month.**

Total monthly cost = [720 Data Store hours x $0.27] + [1,014 GB storage x $0.37 per GB] + [(10,000/10,000 x24 x 30) FHIR query hours x
$0.0010] = $654.14

Hi, I can connect you with an AWS representative or answer questions you have on AWS.

- Total Number Of Queries per Month

100k

- Integrated NLP Settings

= 100K

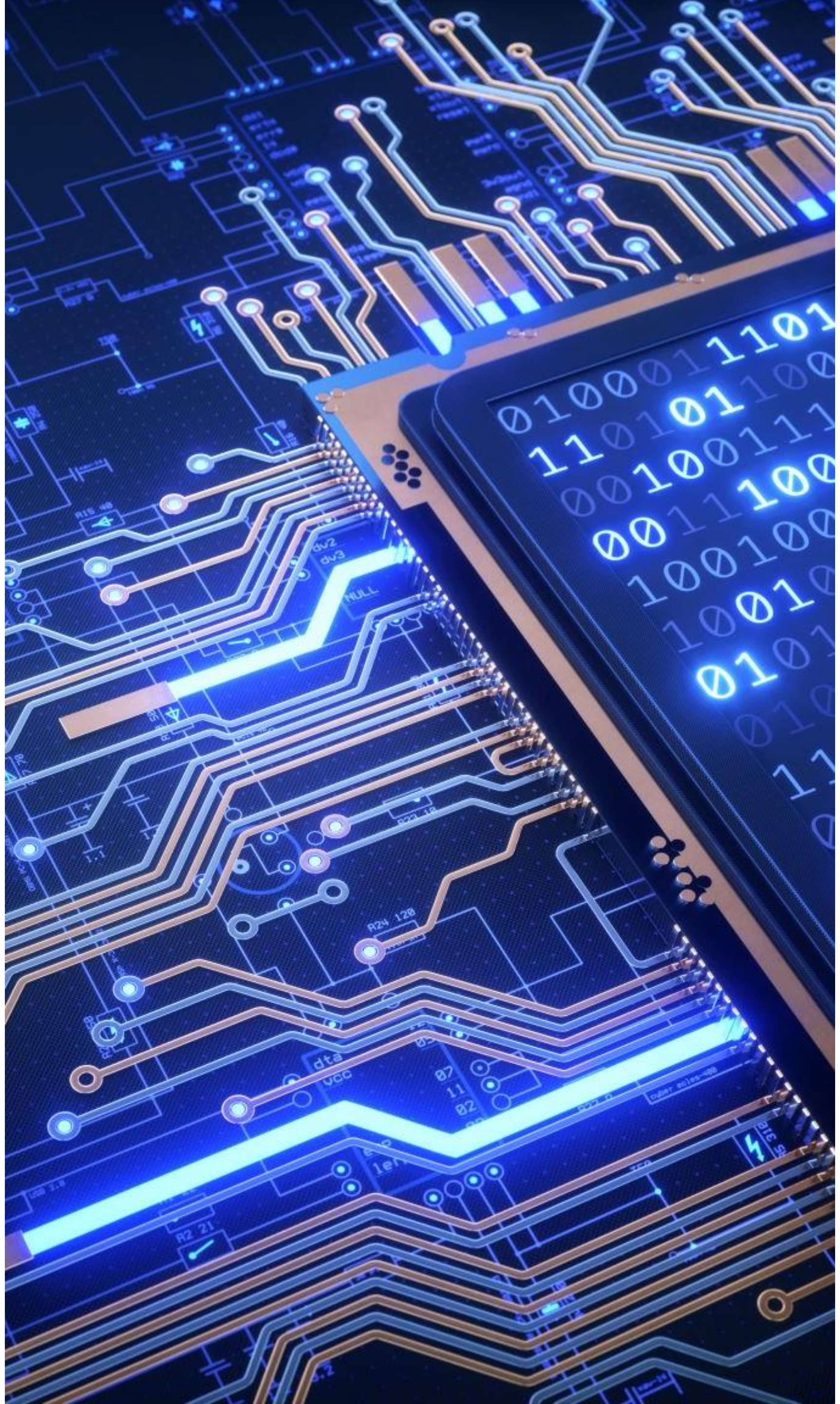
- Exported Data per GB

= 10k GB

- Additional Data Storage

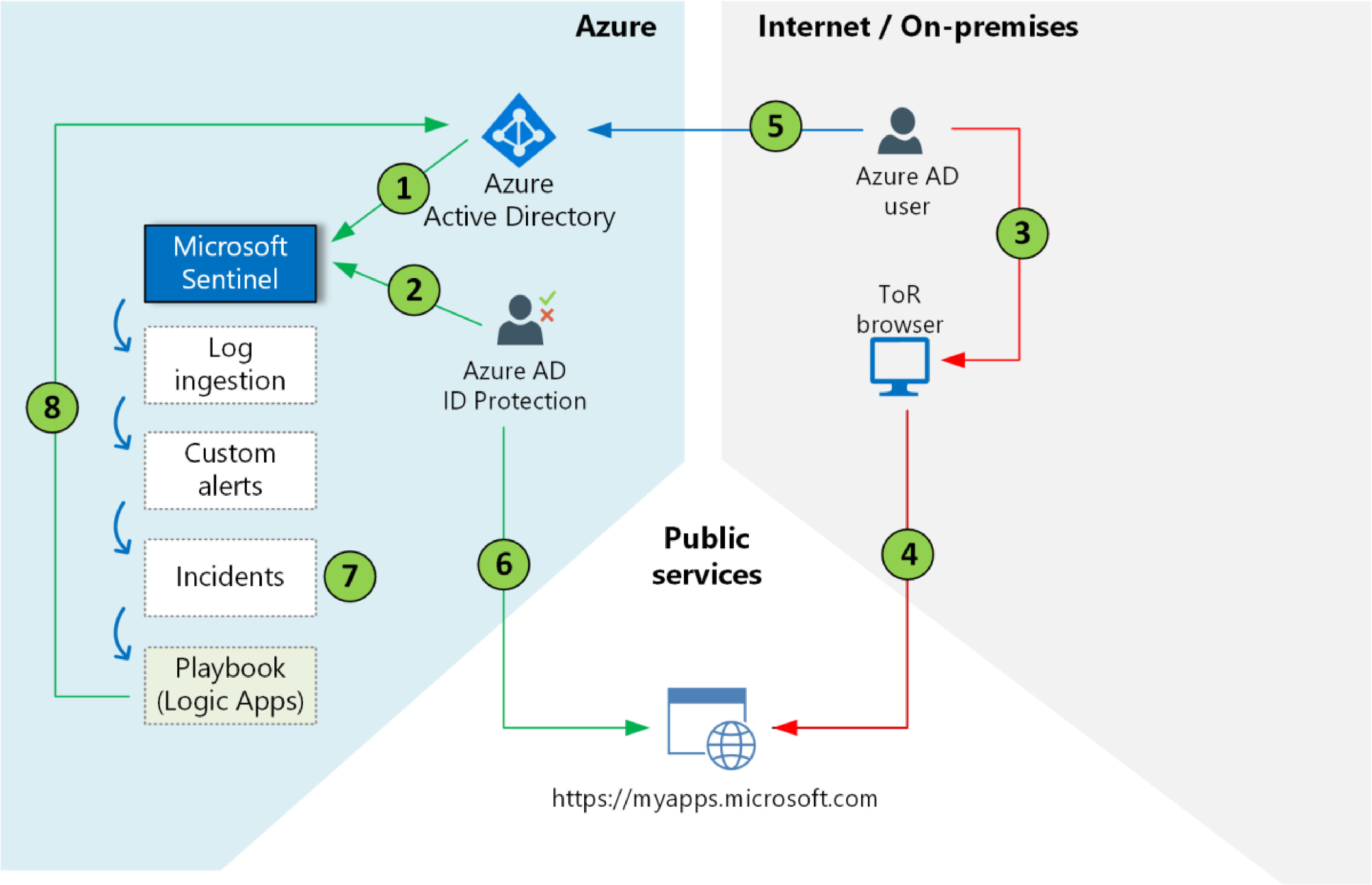
= 10k GB

Total Cost monthly = 5,794.40 USD



Introduction to Microsoft Sentinel

- Microsoft Sentinel is a cloud-native SIEM system that provides intelligent security analytics and threat intelligence across the enterprise. It offers real-time threat detection, automated response capabilities, and advanced AI-driven analysis to proactively identify potential security threats, ensuring comprehensive protection of digital environments in healthcare settings.


Azure
Internet / On-premises
Azure Active Directory
Azure AD user
Microsoft Sentinel
Log ingestion
Custom alerts
Incidents
Playbook (Logic Apps)
Azure AD ID Protection
ToR browser
Public services
https://myapps.microsoft.com
1
2
3
4
5
6
7
8

Sentinel's Role in Hospital Security

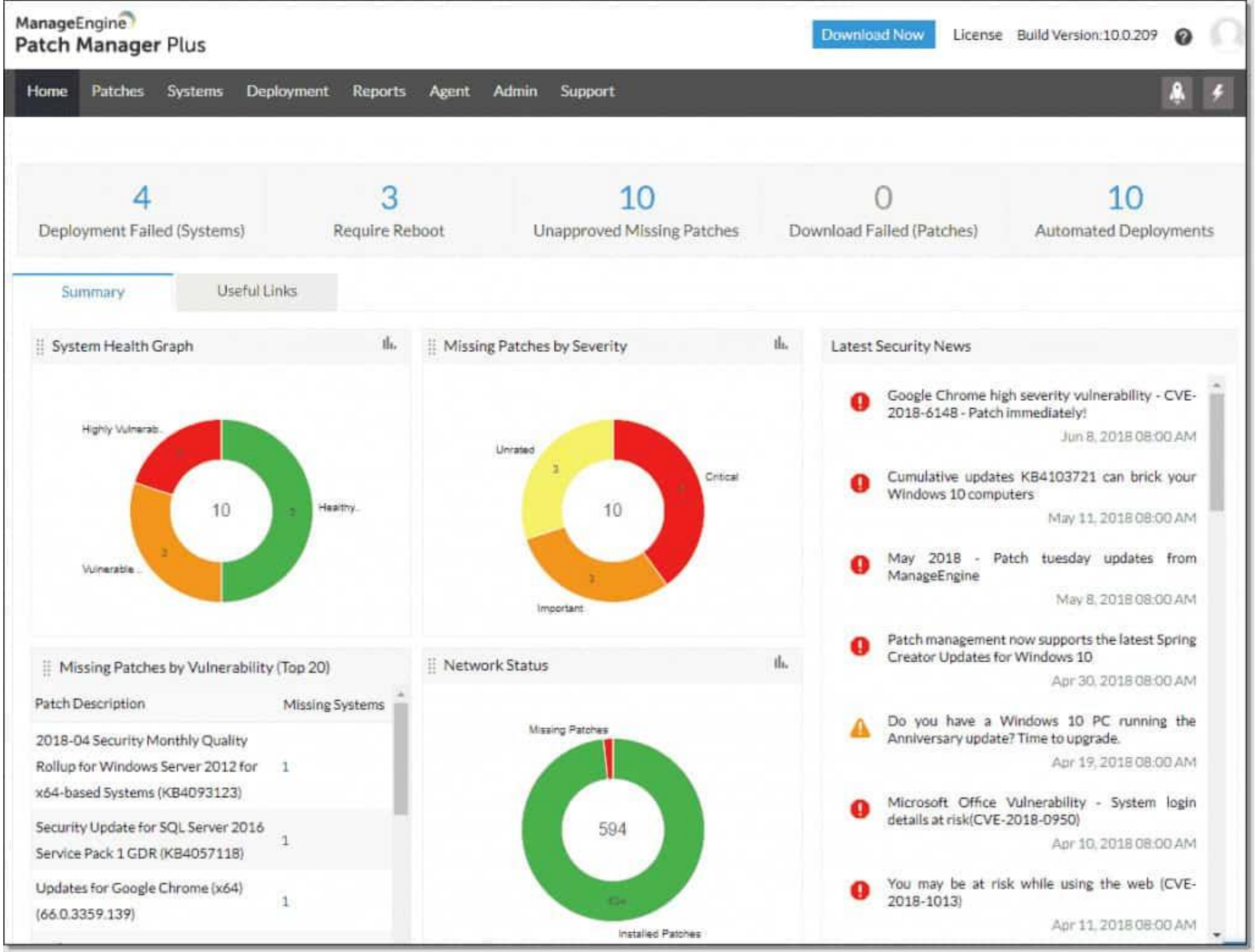
- By integrating Microsoft Sentinel, hospitals can enhance their security infrastructure to detect, respond to, and investigate threats in real-time. This ensures the protection of patient data and healthcare services from cyber threats, maintaining patient confidentiality and the continuity of care.

Importance of Patch Management

- Patch management is crucial for securing IT systems in healthcare. Regular updates and patches fix vulnerabilities that could be exploited by cyber attackers. A comprehensive patch management strategy ensures the security of software and the continuous operation of healthcare services.

Patch Management with ManageEngine

- ManageEngine provides tools for effective patch management, automating the process of updating systems and applications with the latest security patches. This ensures that all elements of a hospital's IT infrastructure are protected against vulnerabilities, safeguarding patient data and healthcare operations.



4	3	10	0	10
Deployment Failed (Systems)	Require Reboot	Unapproved Missing Patches	Download Failed (Patches)	Automated Deployments

Missing Patches by Vulnerability (Top 20)

Patch Description	Missing Systems
2018-04 Security Monthly Quality Rollup for Windows Server 2012 for x64-based Systems (KB4093123)	1
Security Update for SQL Server 2016 Service Pack 1 GDR (KB4057118)	1
Updates for Google Chrome (x64) (66.0.3359.139)	1

Latest Security News

Google Chrome high severity vulnerability - CVE-2018-6148 - Patch immediately!
Jun 8, 2018 08:00 AM

Cumulative updates KB4103721 can brick your Windows 10 computers
May 11, 2018 08:00 AM

May 2018 - Patch tuesday updates from ManageEngine
May 8, 2018 08:00 AM

Patch management now supports the latest Spring Creator Updates for Windows 10
Apr 30, 2018 08:00 AM

Do you have a Windows 10 PC running the Anniversary update? Time to upgrade.
Apr 19, 2018 08:00 AM

Microsoft Office Vulnerability - System login details at risk(CVE-2018-0950)
Apr 10, 2018 08:00 AM

You may be at risk while using the web (CVE-2018-1013)
Apr 11, 2018 08:00 AM

Sources

- https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html#:~:text=Your%20health%20information%20cannot%20be,purposes%20or%20sell%20your%20information
- https://aws.amazon.com/healthlake/pricing/
- https://www.cisco.com/c/en/us/products/collateral/routers/8000-series-routers/8608-router-ds.html#Security
- https://www.cisco.com/c/en/us/products/collateral/security/firepower-9000-series/datasheet-c78-742471.html