WEEK 1

DATE – 10/02/2025 (MONDAY)

**1. Cyber Security -** Cyber security refers to the practice of protecting systems, networks, and data from cyber threats, such as hacking, malware, phishing, and ransomware attacks. It encompasses various domains, including network security, endpoint security, cloud security, and data protection.

**Key Aspects of Cyber Security:**

* **Network Security**: Protects computer networks from unauthorized access.
* **Endpoint Security**: Secures individual devices like laptops and smartphones.
* **Cloud Security**: Ensures safe usage of cloud-based services.
* **Application Security**: Focuses on protecting software applications from threats.
* **Data Protection**: Implements encryption and access controls to safeguard data.

**Types of Cyber Attacks:**

**1. Hacking**

* Unauthorized access to a system or network to steal, modify, or destroy data.
* **Example:** SQL injection, brute force attacks.

**2. Malware (Malicious Software)**

* Software designed to harm or exploit devices and networks.
* **Types:**
  + **Viruses** – Attaches to files and spreads when executed.
  + **Worms** – Self-replicating malware that spreads across networks.
  + **Trojans** – Disguised as legitimate software to trick users into installing them.
  + **Spyware** – Secretly monitors user activity and steals information.

**3. Phishing**

* Fraudulent attempts to obtain sensitive data by disguising as a trustworthy entity.
* **Example:** Fake emails from banks or service providers tricking users into providing login details.

**4. Ransomware**

* Encrypts files and demands payment (ransom) to restore access.
* **Example:** WannaCry, REvil ransomware attacks.

**5. Denial-of-Service (DoS) & Distributed Denial-of-Service (DDoS) Attacks**

* Overloads a network or website with excessive requests, causing service disruptions.
* **Example:** Botnet attacks.

**2. Asset Management -** Asset management refers to the systematic process of acquiring, maintaining, and disposing of assets in a cost-effective manner. It is widely used in businesses to track physical and digital assets, optimize asset usage, and ensure compliance.

**Types of Asset Management:**

* **Financial Asset Management**: Manages investments and financial portfolios.
* **Physical Asset Management**: Deals with tangible assets like machinery and infrastructure.
* **Digital Asset Management**: Handles digital files and software.

**3. IT Asset Management (ITAM)** - IT Asset Management (ITAM) focuses on managing IT-related assets such as hardware, software, and network resources to optimize performance and reduce costs.

**Key Components of ITAM:**

* **Hardware Asset Management**: Tracking servers, computers, and other devices.
* **Software Asset Management**: Managing software licenses and compliance.
* **Lifecycle Management**: Monitoring the procurement, usage, and disposal of IT assets.
* **IT Governance and Compliance**: Ensuring adherence to IT policies and regulatory requirements.

**4. Cyber Security Asset Management (CSAM)** - Cyber Security Asset Management (CSAM) involves identifying, tracking, and securing all assets within an organization to minimize cybersecurity risks. It provides visibility into assets that may be vulnerable to cyber threats.

**Key Elements of CSAM:**

* **Asset Discovery**: Identifying all assets in an organization’s network.
* **Vulnerability Assessment**: Analysing security risks associated with assets.
* **Risk Management**: Implementing measures to protect critical assets.
* **Incident Response**: Quickly addressing security breaches and threats.

**5. Similarities and Differences between ITAM and CSAM -**

|  |  |  |
| --- | --- | --- |
| **Aspect** | **IT Asset Management (ITAM)** | **Cybersecurity Asset Management (CSAM)** |
| **Primary Focus** | Managing IT assets for efficiency, cost control, and lifecycle management. | Identifying and securing assets to protect against cyber threats. |
| **Objective** | - Track and optimize IT resources.  - Reduce costs and improve asset utilization.  - Ensure compliance with software licenses and procurement policies. | - Maintain an up-to-date inventory of assets.  - Identify vulnerabilities and security risks.  - Ensure compliance with security frameworks (NIST, CIS, etc.). |
| **Asset Types Managed** | - Hardware (servers, laptops, printers)  - Software (licenses, applications)  - Cloud and network resources | - All IT assets (hardware & software)  - IoT devices, endpoints, and cloud resources  - Vulnerabilities and security controls |
| **Key Benefits** | - Ensures software compliance and reduces audit risks.  - Supports IT planning and budgeting. | - Reduces attack surface by securing all assets.  - Helps in incident response and threat management.  - Improves overall cybersecurity posture. |
| **Tools Used** | ServiceNow, SolarWinds, Lansweeper | Tenable, Qualys, Axonius, Microsoft Defender |

**6. Emerging Trends in Cyber Security -**

* **Zero Trust Security** – No user or device is trusted by default, requiring continuous verification.
  + **Example:** Google’s **BeyondCorp** security model ensures employees access corporate data only after authentication, even from internal networks.
* **AI and Machine Learning in Security** – AI-powered systems detect and mitigate threats in real time.
  + **Example:** **Darktrace** uses AI to identify unusual network behaviour and prevent cyber threats before they escalate.
* **Cloud Security Enhancements** – Advanced security measures for protecting cloud-stored data.
  + **Example:** **Microsoft Defender for Cloud** provides threat protection across multi-cloud and hybrid environments.
* **Blockchain for Cyber Security** – Securing transactions and preventing data breaches with decentralized encryption.
  + **Example:** **IBM’s Hyperledger Fabric** ensures tamper-proof data storage in supply chain management.
* **IoT Security** – Safeguarding interconnected devices from cyber threats.
  + **Example:** **Cisco IoT Threat Defense** secures IoT networks by segmenting traffic and detecting anomalies.
* **Cyber Resilience Strategies** – Ensuring business continuity despite cyberattacks.
  + **Example:** **Maersk** implemented a robust cyber resilience plan after the 2017 NotPetya attack, restoring operations quickly and improving future security defenses.
* **Conclusion -**

Cyber security and asset management are critical to protecting financial and digital resources. The Cosmos Bank heist illustrates the evolving threats in the cyber landscape and underscores the need for robust security strategies, international collaboration, and continuous monitoring to prevent future cyber attacks.

**ApexaiQ Overview:**

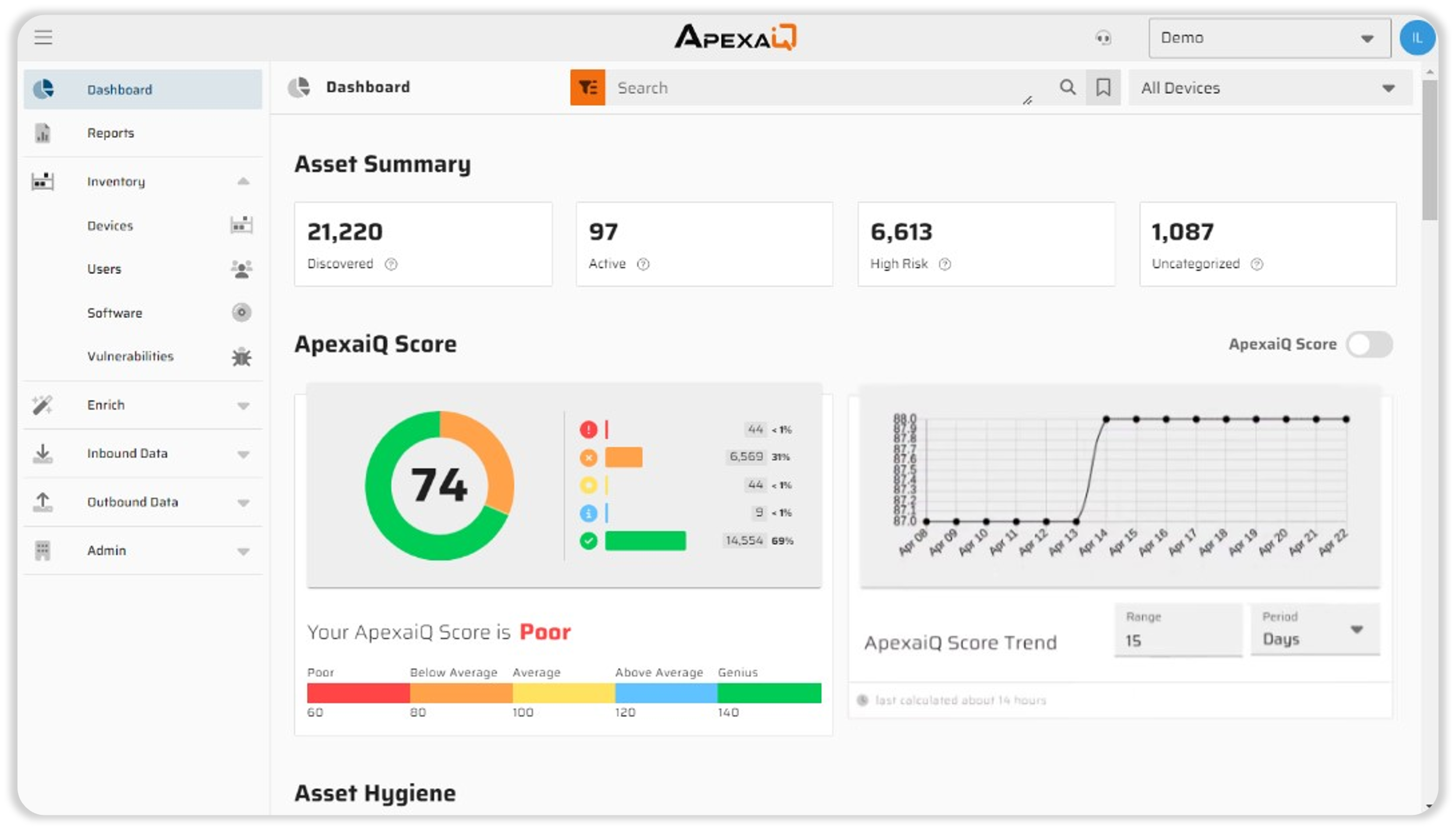
ApexaiQ is a **SaaS-based IT risk management platform** that calculates your **ApexaiQ score**, a credit rating for your IT environment. It assesses **risks, compliance, obsolescence, maintenance, and vulnerabilities** in a single dashboard, helping organizations improve their IT hygiene.

1. **Major clients**

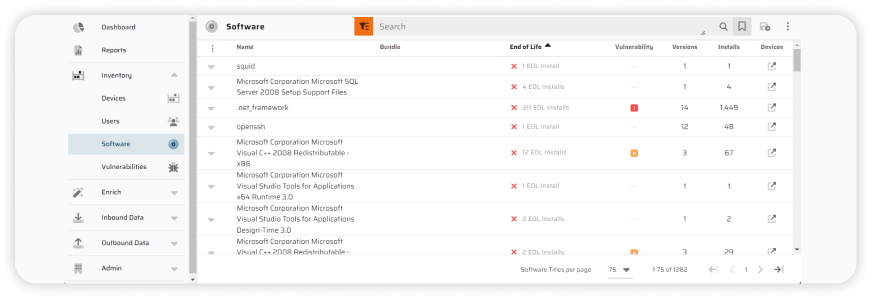
* **Fidelity Bank**
* **Northern Bank**
* **Beazley (Cybersecurity Expert Vendor)**

These clients represent industries such as **banking, financial services, healthcare, and insurance.**

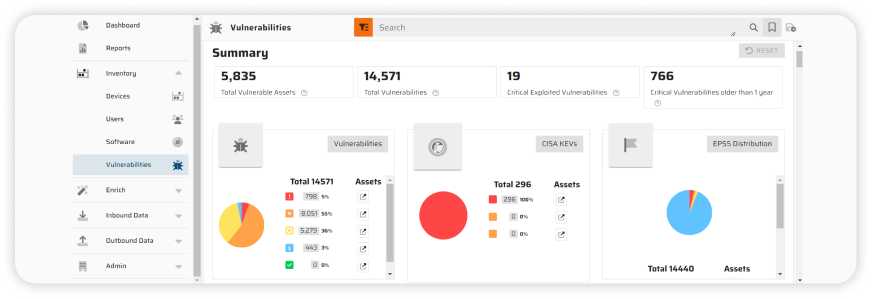
1. **Features of Dashboard:**

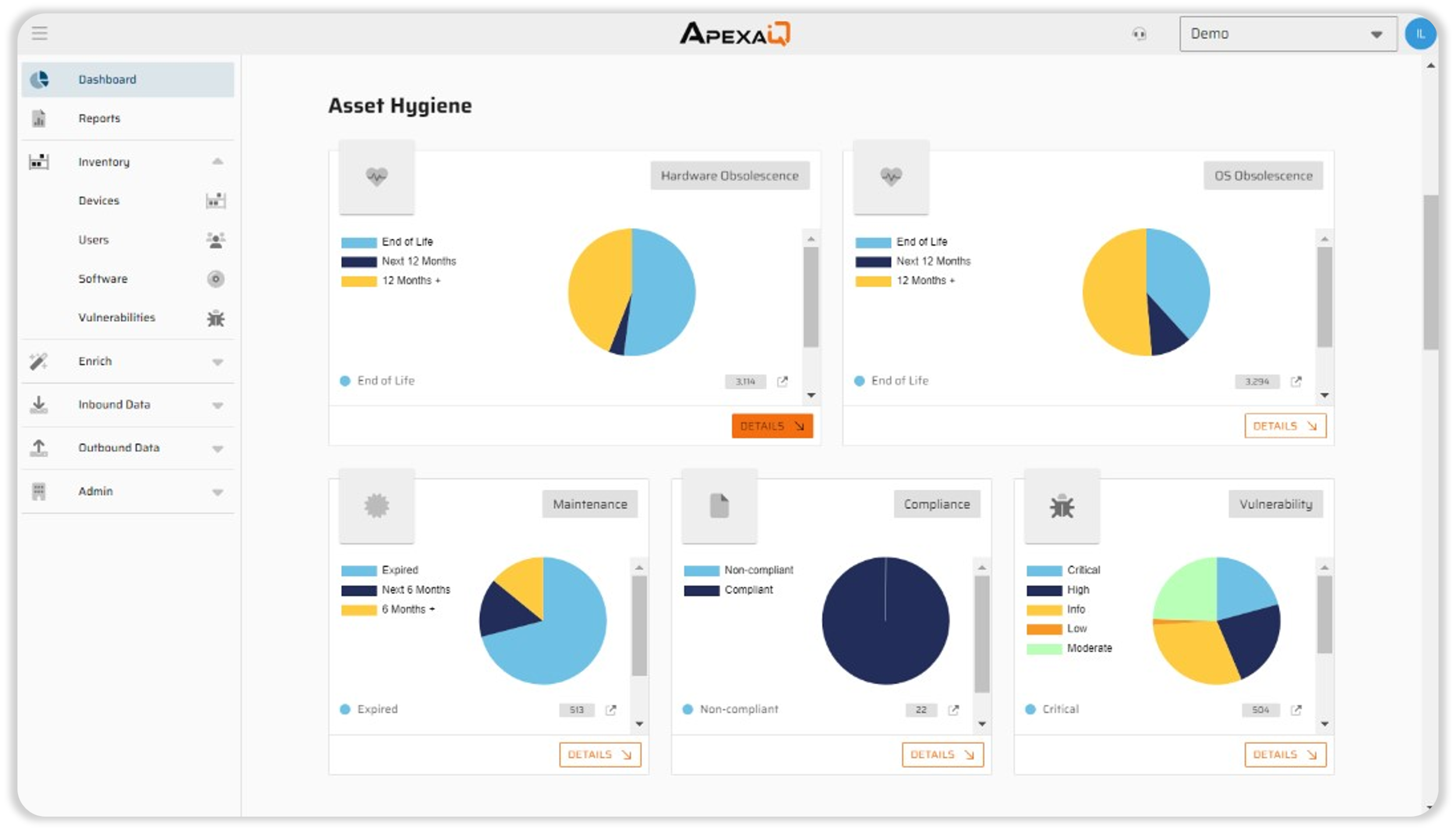


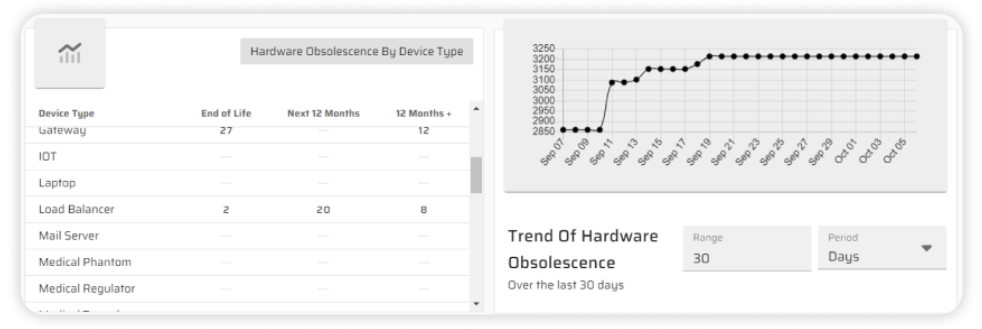
* It computes all your risks and security gaps into a single score, based on the most vital obsolescence and compliance factors.
* The higher the score, the stronger and more secure your IT environment.



Gain visibility into licenses, versions, and vulnerabilities across your entire stack.

Never miss a critical update that could leave you exposed.





From servers to IoT devices, know exactly what you have and its health status.

1. **ApexaiQ vs. Competitors –**

* **Source:** [CB Insights](https://www.cbinsights.com/company/apexa-iq/alternatives-competitors)
* **Focus:** While all three operate in the cybersecurity space, they specialize in slightly different areas.
  + ApexaiQ focuses on overall IT asset security and compliance,
  + Quod Orbis emphasizes continuous security monitoring,
  + Vicarius concentrates on vulnerability management.
* **Key Strength:** This highlights each product's core competency.
  + ApexaiQ excels at real-time asset monitoring,
  + Quod Orbis at compliance and risk monitoring,
  + Vicarius at AI-driven vulnerability remediation.

* **Asset Discovery:** All three offer asset discovery capabilities.
  + ApexaiQ provides full IT asset visibility,
  + Quod Orbis performs broad IT scanning,
  + Vicarius focuses on software vulnerability detection.

While there's overlap, the *scope* of what they discover might differ. For example, ApexaiQ might be more comprehensive across all asset types, while Vicarius might go deeper into software vulnerabilities specifically.

* **Monitoring:**
  + ApexaiQ offers continuous real-time tracking,
  + Quod Orbis provides risk analysis and compliance alerts,
  + Vicarius emphasizes automated patching and scanning.

Again, all three "monitor," but *what* they monitor and *how* they do it varies.

* **Compliance:**
  + ApexaiQ generates automated reports for standards like ISO and GDPR.
  + Quod Orbis focuses on regulatory security compliance,
  + Vicarius on vulnerability compliance.

They each address compliance, but with a different emphasis.

* **Best For:** This summarizes the ideal use case for each product.
  + ApexaiQ is best for organizations needing full IT security and risk insights,
  + Quod Orbis for those requiring enterprise security monitoring,
  + Vicarius for those prioritizing automated vulnerability patching.

**In essence:**

* **ApexaiQ** is the most comprehensive, offering a broad view of IT asset security and compliance. Think of it as a holistic platform.
* **Quod Orbis** is geared towards continuous security monitoring, likely providing in-depth analysis and alerts related to security posture and risk.
* **Vicarius** is more specialized, focusing on identifying and remediating vulnerabilities, particularly in software.

The best choice for a particular organization depends on their specific security needs and priorities. A company needing a broad overview of their IT security posture might choose ApexaiQ. One focused on meeting specific regulatory requirements might lean towards Quod Orbis. And a company struggling with patching vulnerabilities quickly might find Vicarius the best fit.

DATE – 11/02/2025 (TUESDAY)

* **What is data?**
* Data refers to raw, unorganized facts, figures, or observations that lack context but can be processed to derive meaning. It can exist in various formats, such as text, numbers, images, and sounds.
* **Primary types of data**

1. Qualitative **(Descriptive Data)**

* Describes characteristics or attributes (non-numeric).
* Examples: Customer feedback, survey responses, interviews.

1. Quantitative **(Numerical Data)**

* Represents measurable quantities.
* Examples: Temperature readings, sales figures, population counts.
* **Sub types of data :**

**-**  **Transport Data** – Includes vehicle movement, traffic flow, fuel consumption, and logistics data.

**- Geographical Data** – Spatial data, maps, GPS coordinates, elevation levels.

**- Natural Data** – Ecosystem information, biodiversity records, climate impact data.

**- Meteorological Data** – Weather forecasts, temperature patterns, wind speed, precipitation levels.

**- Statistical Data** – Census reports, economic indicators, research statistics.

**- Financial Data** – Stock market trends, company earnings, taxation reports.

**- Scientific Data** – Lab experiment results, DNA sequencing, astronomical observations.

- **Cultural Data** – Artefacts, traditions, linguistic trends, heritage records.

* **What is information?**

Information is processed, structured, and meaningful data that provides insights or knowledge. It is derived from raw data through analysis, filtering, and interpretation.

* **Example:**
* **Raw Data:** 100, 102, 105, 107
* **Processed Data (Information):** The temperature increased by an average of 2°C per hour.
* **Raw data to information**
* **Data Collection** – Gathering unprocessed data.
* **Data Cleaning** – Removing errors, duplicates, inconsistencies.
* **Data Processing** – Organizing and analysing the data.
* **Data Interpretation** – Extracting insights.
* **Data Representation** – Presenting data in graphs, charts, reports.
* **Applications and importance of data :**
* **Business Analytics** – Market trends, customer behaviour.
* **Healthcare** – Patient records, disease prediction.
* **Finance** – Fraud detection, stock analysis.
* **Education** – Student performance tracking, research.
* **Science & Research** – Innovations, experiments.
* **Government & Policy-Making** – Census data, economic planning.
* **Data sources :**

1. **Primary source**
2. **Door-to-Door Surveys** – Direct feedback collection.
3. **Student Thesis** – Original academic research.
4. **Personal Interviews** – One-on-one discussions for insights.
5. **Secondary source** (Pre-collected data from other sources)
   1. **Internet** – Online research papers, reports.
   2. **Books** – Published literature, encyclopaedias.
   3. **Newspapers** – News articles, editorial analysis.

* **Data gathering – (data collection\ data acquisition) :**

Defining Objective --> Identifying Data Sources --> Designing Data Collection Methods --> Data Collection --> Data Recording and Organization.

* **Defining Objective** – Identifying the purpose of data collection.
* **Identifying Data Sources** – Choosing primary or secondary sources.
* **Designing Data Collection Methods** – Surveys, observations, sensors.
* **Data Collection** – Gathering data through selected methods.
* **Data Recording and Organization** – Storing and structuring the data.
* **RDBMS – (Relational Database Management System):**

(Tabular format depends on the format of data)

* Stores data in tabular format (rows & columns).
* Ensures data integrity, consistency, and accessibility.
* Examples: MySQL, PostgreSQL, Oracle DB, MS SQL Server.

DATE – 12/02/2025 (WEDNESDAY)

* **Data Transformation**
* It is the process of converting data from one format, structure, or value into another to make it suitable for analysis, storage, or further processing.
* It involves converting, cleansing, and structuring data into a usable format which is used to analyzed to support decision-making processes.
* **Various methods of data transformation**

1. **Normalization**

* It scales numbers so they are between 0 and 1.
* Makes different types of data easier to compare, even if they have different ranges.
* Ex. Changing income from 10,000 – 1,00,000 to a scale of 0 to 1.

1. **Standardization**

* Helps some machine learning models work better by making all data behave the same way.
* Ex. Adjusting test scores so they all follow a consistent scale.

1. **Encoding**

* Converts words or categories into numbers.
* Computers can understand numbers, not words, so this makes data usable for analysis.
* Ex. Changing "Yes" to 1 and "No" to 0.

1. **Discretization**

* Turns continuous data (like age or salary) into groups or categories.
* Makes complex data easier to analyze by grouping it into simple categories.
* Ex. Grouping ages into "Under 18," "18-35," "36-60," and "Above 60."

1. **Attribute Generation**

* Creates new information from existing data.
* Gives more details for analysis, which can help find patterns.
* Ex. Creating an "age" value from a person’s birth year.

1. **Revising**

* Fixes mistakes or inconsistencies in the data.
* Ensures the data is accurate and reliable.
* Ex. Removing duplicate entries or fixing wrong dates.

1. **Manipulation**

* Changes or calculates new values based on existing data.
* Helps to make data more useful or easier to work with.
* Ex. Combining first and last names into a full name.

1. **Separating**

* Breaks down a piece of information into smaller parts.
* Makes it easier to filter or analyze specific details.
* Ex.Splitting an address into street, city, and zip code.

1. **Combining/Integrating**

* Brings together data from different sources into one place.
* Gives a complete view of the data by merging information.
* Ex.Merging customer data from different databases into a single record.
* **Advantages of Data Transformation**
* Better Data Quality – Fixes errors and makes data more accurate.
* Easy to Use – Converts data into a format that different systems can understand.
* Faster Analysis – Organizes data so it can be processed quickly.
* Saves Space & Time – Removes unnecessary data and improves efficiency.
* More Secure – Helps protect sensitive information.
* **Limitations of Data Transformation**
* Takes Time & Effort – Can be slow and complex, especially for big data.
* Risk of Mistakes – Poor transformation can lose or change important data.
* Expensive – Requires special tools and skilled people.
* Hard to Scale – Some methods may not work well with very large data.
* Can Introduce Errors – If not done correctly, it may create biased or misleading results.
* **Why do businesses need data transformation?**

Organizations generate a huge amount of data daily. However, it is of no value unless it can be used to gather insights and drive business growth. Organizations utilize data transformation to convert data into formats that can then be used for several processes. There are a few reasons why organizations should transform their data.

* Transformation makes disparate sets of data compatible with each other, which makes it easier to aggregate data for a thorough analysis
* Migration of data is easier since the source format can be transformed into the target format
* Data transformation helps in consolidating data, structured and unstructured
* The process of transformation also allows for enrichment which enhances the quality of data

The ultimate goal is consistent, accessible data that provides organizations with accurate analytic insights and predictions.

DATE – 13/02/2025 (THURSDAY)

**Day 4 - Assignment-End of Life**

* **Introduction**

Technology evolves rapidly, and with it, software and hardware products reach their end-of-life (EOL). EOL refers to the point when a manufacturer stops providing support, updates, or services for a product. Understanding EOL policies is crucial for businesses and individual users to ensure security, compliance, and continued efficiency.

This guide covers key parameters related to EOL, how different companies handle it, and what steps users should take when a product is reaching its end.

* **5 Stages of Server Life Cycle**

* **What are indications of EOL?**

For **Hardware** EOL (PCs, servers, storage devices) IT professionals look for slow performance, files opening slowly, slow response when accessing a website, frequent crashing and similar issues.

For **Software** EOL (software, application) indications can be as application don't execute as they originally did or execute too slowly, application doesn't operate on newer hardware or operating systems then replacement might be needed.

* **States of EOL**

1. **Dated EOL**
   * When a specific date is announced for the end of support or discontinuation.
   * Example: Windows 10 has an official EOL date of October 14, 2025.
   * Users can plan ahead for upgrades or transitions.
2. **Undated EOL**

* When no fixed date is given, but the product/service is expected to phase out over time.
* Example: A company hints at discontinuing a product "in the near future" without specifying a deadline.
* Sign: Company may give vague timelines such as “support will end soon” or “phasing out.”
* How to Identify: Check for official announcements, Monitor update frequency, Customer support availability, etc.

1. **Support dated**
   * + A specific end date is provided for support services (updates, security patches, maintenance).
     + Example: Windows 10 support ends on October 14, 2025.
     + Users can plan for upgrades and transitions in advance.
2. **Support undated**

* No fixed end date is announced, but support may phase out over time.
* Example: Some open-source software projects continue support indefinitely until contributors stop maintaining them.
* Signs: No fixed end date, but the product continues to receive updates and patches.
* How to Identify: Product documentation, Official statements, etc.

1. **Unknown**

* No clear information on whether support will continue or end.
* Example: A small company provides software but hasn’t communicated any support timeline.
* Sign: No clear information about whether the product will be supported, updated, or phased out.
* How to Identify: Check for product updates, Search for announcements, etc.
* **How Major Vendors Handle EOL**

1. **Apple Software (macOS, iOS)**:

If older than 5-7 years may no longer receive the latest iOS updates. It is considered outdated and stops receiving new features or security updates.

* URL: <https://support.apple.com/en-us/102772>

1. **Adobe**

Adobe informs customers at least a year in advance before retiring products.

* Users are encouraged to transition to Adobe Creative Cloud or other alternatives.

#### **Example:**

#### **Adobe Flash Player** – Announced for EOL in **July 2017**, officially discontinued on **December 31, 2020**. Users were advised to transition to **HTML5, WebGL, or Adobe Animate**.

* **Reference:** Adobe End of Life Communication

1. **Microsoft**

Microsoft provides clear EOL timelines through its lifecycle policy:

* **Mainstream Support:** Typically 5 years, covering updates and assistance.
* **Extended Support:** Another 5 years of security fixes only.
* Example: **Windows 7** reached **End of Support on January 14, 2020**, meaning users no longer receive updates, making it vulnerable to security risks.
* **Reference:** [Microsoft Lifecycle Policy](https://learn.microsoft.com/en-us/lifecycle/products/windows-7) , End of life documents
* **Key Considerations for End-of-Life (EOL) Products** -

**1. Official Support Timeline**

Manufacturers usually provide products with two types of support:

* **Mainstream Support**: Includes regular updates, bug fixes, and customer support. Typically lasts 3–5 years.
* **Extended Support**: Offers security patches but no feature updates or direct customer assistance.
* **End of Support (EOS)**: The final stage where no more updates, patches, or technical help is available.

**2. Security Risks**

Once a product reaches EOL, it no longer receives security updates, leaving it vulnerable to threats such as malware, ransomware, and data breaches. Businesses and users must transition to supported products to mitigate risks.

**3. Compliance & Legal Concerns**

Industries dealing with sensitive data (e.g., finance, healthcare) must comply with regulatory requirements. Using outdated software can result in legal complications, fines, or data privacy violations.

**4. Performance & Compatibility Issues**

EOL products often struggle to integrate with newer hardware and software, leading to inefficiencies. Performance degradation and incompatibility with modern applications can hinder productivity.

**5. Extended Security Updates & Support Options**

Some vendors offer extended security updates (ESUs) for a fee, allowing businesses additional time to transition without security concerns. It is essential to check if such options are available.

**6. Community Support & Open-Source Alternatives**

Even after official support ends, online communities and forums can be valuable for troubleshooting and continued use. Open-source solutions may also serve as viable replacements.

### **Advantages and Disadvantages of EOL (End of Life)**

#### **Advantages of EOL:**

1. **Encourages Upgrades** – Forces users to transition to newer, more secure, and efficient technologies.
2. **Cost Savings for Vendors** – Companies can stop maintaining outdated products and focus resources on innovation.
3. **Security Improvements** – Older products are more vulnerable; transitioning to newer versions ensures better security.
4. **Standardization** – Reduces compatibility issues by phasing out legacy systems in favour of modern alternatives.
5. **Optimized Performance** – Newer technologies often come with better features, improved speed, and efficiency.s

#### **Disadvantages of EOL:**

1. **Increased Costs for Users** – Upgrading to a newer version can be expensive, especially for businesses using legacy systems.
2. **Compatibility Issues** – Older software/hardware may not work with new versions, requiring additional migration efforts.
3. **Security Risks** – Unsupported products do not receive updates, leaving them vulnerable to cyber threats.
4. **Business Disruptions** – Transitioning to new systems can cause downtime and require employee training.
5. **Data Migration Challenges** – Moving from an EOL product to a new one may lead to data loss or require additional resources.

DATE – 14/02/2025 (FRIDAY)

**1. Common Vulnerability Scoring System (CVSS)**

* A standardized system for assessing the severity of security vulnerabilities.
* Provides an open framework for communicating vulnerability characteristics and impacts.
* **Scoring system:** Ranges from **0 to 10**, where **10** represents the highest severity.

**2. Common Vulnerabilities and Exposures (CVE)**

* A dictionary of publicly known cybersecurity vulnerabilities.
* Each vulnerability is assigned a **unique CVE identifier**.
* Acts as a **universal standard** for identifying and referencing vulnerabilities.
* Does not provide severity scores but includes a brief description of the issue.

**3. A** **Common Platform Enumeration (CPE)**

* Represents a specific product, software, or hardware version. Since vulnerabilities (CVEs) are often **version-specific**.
* It helps in standardizing product names for security tools, making it easier to track vulnerabilities (CVEs), manage assets, and perform security assessments.
* A single CPE can be associated with **multiple CVEs**, each affecting different versions or configurations of the product.
* **CPE Format Example:**
* *cpe:2.3:a:microsoft:windows\_10:1909:\*:\*:\*:\*:\*:\*:\**

This refers to **Windows 10, version 1909**.

* This CPE identifier represents **Microsoft Windows 10, version 1909**.

Break down in detail:

1. **cpe:2.3** → This indicates the **CPE version**. Here, **2.3** means the identifier follows the CPE 2.3 standard.
2. **o** → This represents the **Operating System (OS)**. If it were software, it would be **a** (for applications), and for hardware devices, it would be **h**.
3. **microsoft** → This is the **vendor (company name)** that develops the product. In this case, it is **Microsoft**.
4. **windows\_10** → This is the **product name**, specifying that the CPE refers to **Windows 10**.
5. **1909** → This is the **version number**, indicating that it is **Windows 10 version 1909**.
6. **\* (asterisks)** → These are wildcards, representing optional or unspecified fields (such as updates, language, or edition) that are not explicitly provided here.

**Use Case of This Example:**

* This CPE identifier is used in the **NVD (National Vulnerability Database)** and **cybersecurity systems** to track vulnerabilities (CVE - Common Vulnerabilities and Exposures).
* If any security flaw is found in Windows 10 version 1909, its CVE reports will be linked to this CPE identifier.
* Resource – [Link](https://nvd.nist.gov/products/cpe/detail/3AB38A7B-218B-41F2-9CB9-E7E4F4DFF539?namingFormat=2.3&orderBy=CPEURI&keyword=cpe%3A2.3%3Ao%3Amicrosoft%3Awindows_10&status=FINAL%2CDEPRECATED)
* CPEs are widely used in security databases like the **National Vulnerability Database (NVD)** to link vulnerabilities to specific products and versions.

**3. National Vulnerability Database (NVD)**

* An extension of the CVE system, offering additional analysis and metrics.
* Maintained by the **National Institute of Standards and Technology (NIST)**.
* Provides:
  + **CVSS scores** for vulnerabilities.
  + **Checklists, impact metrics, and fixes**.
  + A **comprehensive repository** of cybersecurity vulnerabilities.

**4. Differences Between CVSS, CVE, and NVD**

* **CVSS** → The **grading system** that evaluates severity.
* **CVE** → The **list of known vulnerabilities**, each with a unique ID.
* **NVD** → The **comprehensive database** containing CVEs, CVSS scores, and additional insights.

**5. Importance of CVSS, CVE, and NVD**

* Helps cybersecurity professionals **identify, evaluate, and manage** vulnerabilities.
* CVSS scores assist in prioritizing vulnerabilities based on severity.
* CVE allows for **standardized reporting** and easier collaboration.
* NVD provides a **detailed repository** to analyze and mitigate threats.

**6. Patching & Limitations**

* **Patching** vulnerabilities is crucial to prevent cyber attacks.
* **Limitations:**
  + CVSS scores focus on **technical severity**, not always **real-world risk**.
  + CVE only catalogs **known** vulnerabilities.
  + Organizations must ensure **timely patching** to mitigate risks.

**Conclusion**

Understanding **CVSS, CVE, and NVD** is essential in cybersecurity for identifying, scoring, and mitigating vulnerabilities effectively. Despite their limitations, they remain **indispensable tools** in securing digital systems.