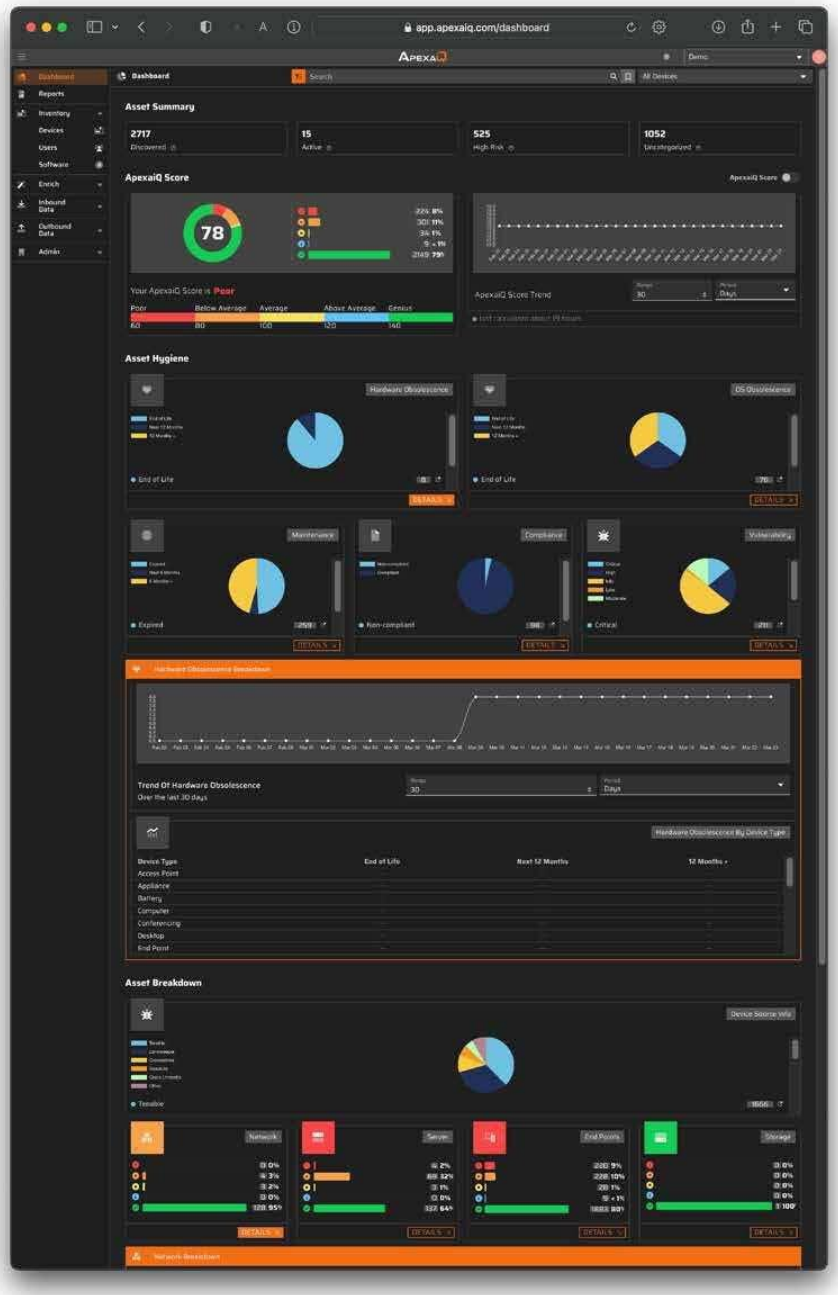
ApexaiQ:

ApexaiQ is a SaaS-based, agentless continuous asset assurance platform in the cybersecurity sector. The company offers a solution for asset data management that includes deduplication, prioritization, enrichment with obsolescence, warranty, vulnerability, and compliance information, all accessible through a single dashboard. ApexaiQ primarily serves sectors such as fintech, healthcare, technology, and retail, providing tools for CISOs, CTOs, CIOs, CFOs, and CEOs to manage and secure their technology assets. It was founded in 2021 and is based in Milford, Massachusetts.



1. What does ApexaiQ do? What industry problem does it solve?

Asset Inventory Management:
Through a centralized asset repository providing holistic intelligence, ApexaiQ facilitates cost optimization, risk mitigation, operational streamlining, and strategic investment alignment.
Prioritises data to improve data accuracy in alignment with organizational requirements
Tags assets to categorize asset types and prioritize investigations involving high-value "crown jewel" assets
Query asset data to rapidly access data-driven intelligence

Optimize Asset Utilization and End-of-life monitoring:
By streamlining asset data and identifying redundancies, ApexaiQ enables strategic budget reallocation towards high-impact initiatives.
Customizable rules for automated asset management and precise insights
Identify underutilized assets and redundant licenses reallocating funds strategically
Enables proactive planning for cost-effective decisions aligned with financial goals

Implements a Proactive Approach to Risk Mitigation:
Implement a proactive approach to risk mitigation with effective data management to minimize operational disruptions and ensure smooth business operations.
Query for comprehensive analysis of all assets with the ApexaiQ risk score
Enables real-time asset insights to assess risk and vulnerabilities
Establishes performance standards using comprehensive data points for improved security posture
Takes action with the use of automation for ticketing, APIs, alerts, and asset tagging

Regulate Compliance:
Clean, enriched, and customized IT asset data enables organizations to boost profitability through optimized asset utilization, regulatory compliance adherence, and cost-efficiency measures that drive competitive advantage.

Industry Problems:

1. Lack of visibility and control over organisations IT infrastructure
   Source: https://www.apexaiq.com/comprehensive-asset-inventory-management/

2. Redundant licensing and underutilized assets which maximize technology spending.

   Source: https://www.apexaiq.com/maximized-technology-spending/

3. Failure to track asset warranties, licenses, and maintenance schedules can result in slow response times or the inability to remediate security vulnerabilities, increasing the likelihood of compliance and security breaches that can lead to financial losses and reputational damage.
   Source: https://www.apexaiq.com/risk-reduction-at-scale/

4. A lack of business context about what's critical in organisations technology environment often leads to slow response times.
   Source: https://www.apexaiq.com/clean-data-for-a-competitive-edge/
   Source: https://www.virtualtech.com.mx/apexa-iq

2. What is IT asset management and why companies need asset management software?

Asset Management:

Asset management is a systematic approach to the governance and realization of all value for which a group or entity is responsible.

Asset management is a systematic process of developing, operating, maintaining, upgrading, and disposing of assets in the most cost-effective manner (including all costs, risks, and performance attributes).

IT asset:

An information technology (IT) asset is any piece of information, software or hardware that an organization uses in the course of its business activities. Hardware assets include physical computing equipment like physical servers in data centers, desktop computers, mobile devices, laptops, keyboards and printers. Software assets, on the other hand, include applications for which licenses are typically issued per user or machine, as well as software systems and databases built using open-source resources. Software assets also include cloud-based assets, such as Software-as-a-Service (SaaS) applications.

IT asset management:

IT asset management (ITAM) is the end-to-end tracking and management of IT assets to ensure that every asset is properly used, maintained, upgraded and disposed of at the end of its lifecycle.

ITAM involves using financial, contractual and inventory data to track and make strategic decisions about IT assets. The main objective is to ensure that IT resources are used efficiently and effectively. ITAM also helps optimize costs by reducing the total number of assets in use and extending the life of those assets, avoiding costly upgrades. An important part of ITAM is understanding the total cost of ownership and finding ways to optimize asset use.

Source: https://www.ibm.com/think/topics/it-asset-management

3.3-5 competitors of Apexaiq and how they are different from Apexa. Case studies.

ApexaiQ Competitors:

BeyondRisk:

BeyondRisk focuses on automating risk and compliance processes in the cyber risk and compliance industry. The company offers services such as data-driven risk assessments, compliance automation, and continuous risk monitoring. These services aim to transform static, point-in-time assessments into real-time oversight with automated alerts, and to integrate various compliance standards effortlessly through application programming interface (API) adapters for seamless automation. It was founded in 2022 and is based in San Francisco, California.

Start Left Security:

Start Left Security offers an analytics-driven application security posture management (ASPM) platform with security analytics and threat detection capabilities. The platform monitors security analytics and threat detection, automates full lifecycle vulnerability governance, remediation, and performance analytics, and tracks security issues back to individual developers. It was formerly known as Tauruseer. The company was founded in 2019 and is based in Jacksonville Beach, Florida.

ESProfiler:

ESProfiler focuses on providing enterprise security profiling tools within the cybersecurity industry. Their platform offers continuous assurance of security investments, enabling chief information security officers (CISOs) to visualize their security capabilities, usage, and spending in alignment with their key threat priorities. It was founded in 2020 and is based in Manchester, United Kingdom.

Nanitor:

Nanitor specializes in Continuous Threat Exposure Management (CTEM) within the cybersecurity industry. The company offers a platform that provides visibility and control over IT infrastructure, focusing on asset-centric security and issue prioritization to enhance organizational cybersecurity. Nanitor's platform serves various sectors by offering tools for compliance reporting, remediation guidance, and collaborative security project management. It was founded in 2014 and is based in Reykjavik, Iceland.

Source: https://www.cbinsights.com/company/apexa-iq

4. Why is ApexaiQ an agentless platform?

Agent based platform:

In cybersecurity, agents represent specialized software components that are installed on devices for performing security-related "actions."

Those actions include, but are not necessarily limited to:

- Security scanning and reporting
- System restarting and rebooting
- Applying software patches
- Making changes to configurations
- General system monitoring

Agentless Platform:

Agentless security performs many of the same actions, but without the agents. In practice, this means that we can inspect and review security scans and vulnerabilities on a remote machine without having to install an agent on that system. You may have to install software on a different layer of the system (like networking) to capture associated risk metrics, but you won’t need to have direct access to the host to install any service. It typically uses remote management protocols or APIs to access and control the target system remotely. This is achieved through non-invasive methods such as cloud APIs or by processing log files.

Agentless systems, then, are based on the push communication style. With agentless systems, the associated software pushes data to a remote system on a periodic basis. Because of the flexibility of this setup, agentless security solutions work well for baseline

security monitoring. You can configure them to scan the whole infrastructure without having to install them to each subsystem. A central system, though, still needs to be available to coordinate scanning and the deployment of patches.

To summarize, agentless systems have a number of features that make them appealing, including:

- Quicker setup and deployment: You don't need to have direct access to all hosts to perform security scans.
- Less maintenance and lower provisioning costs.
- Wider initial visibility and greater scalability.
- Ideal for networks with large amounts of bandwidth.
- Need for a center host available to perform actions.

Agent-based systems have the following benefits over agentless systems:

- Enable in-depth scanning and monitoring of hosts: Agents can perform more specialized scanning of components and services.
- Can be used as a firewall, since it can block network connections based on filtering rules.
- Offer runtime protection per host or per application.
- Provide security controls, like the ability to block attacks and patch live systems.
- Ideal for networks with limited bandwidth, locations within DMZ zones or laptops that can be out of network reach. You can install the agent in systems without network connectivity.
- Do not need a central host since they can perform tasks independently: Once installed, the agent will run its set of actions on demand without needing to establish a connection to a server beforehand – even when it is disconnected from the enterprise network.

Source: https://www.paloaltonetworks.com/cyberpedia/what-is-the-difference-between-agent-based-and-agentless-security

By avoiding agent installations, agentless solutions reduce the potential attack surface. Malicious actors cannot target or compromise agents to gain access to systems.

Therefore, ApexaiQ does not installs agent on devices that's why it's agentless.