Parameter	Apexaiq	Balbix
Compliance	Provides a unified IT risk score that factors in asset compliance and alerts on deviations.	Continuously assesses cybersecurity posture mapped to standards (e.g., HIPAA, ISO 27001).
Maintenance	Flags maintenance gaps; monitors warranty/maintenance expiration in real time.	Uses risk analytics to drive patch prioritization and flag outdated assets.
EOL/EOS/EOM	Dashboard highlights obsolete assets nearing end-of-life/support and end-of-maintenance.	Identifies outdated assets as part of overall risk scoring.
Asset Hygiene	Offers a real-time inventory covering hardware, software, firmware, and IoT.	Continuously monitors asset health using integrated data feeds.
Crown Jewel Identification	Uses its risk score to help prioritize and highlight critical ("crown jewel") assets.	Risk analytics flag high-impact assets requiring extra protection.
Inventory Management	Provides a comprehensive, real-time inventory dashboard for all IT assets.	Maintains continuous asset inventory via broad integration of data sources.
NVD Integration	May leverage external vulnerability data; specific NVD integration is less emphasized.	Integrates with external feeds such as the NVD to assess vulnerabilities.
Patch Management	Lists vulnerabilities by severity to drive prioritized patching.	Prioritizes patch remediation based on risk analytics and external data feeds.
Data Breach Monitoring	Uses its risk scoring and real-time monitoring to help preempt data breaches.	Provides continuous vulnerability assessments to detect exposure risks.
MSP Support	Supports MSP use cases with flexible dashboards and integrations for managed services.	Likely accommodates MSP models within its SaaS-based approach.
Device Types Supported	Covers a broad range including laptops, servers, routers, IoT, and cloud devices.	Monitors both IT and OT assets across various device types.
True SaaS Offering	Delivered as a cloud-based, agentless SaaS platform with real-time dashboards.	Offered as a true SaaS solution with cloud-based analytics and monitoring.
Inbound/Outbound Integration	Provides inbound integrations with partner solutions and outbound alerts via email and dashboards.	Likely supports bi-directional integrations for data exchange.
Compliance Standards Supported	Tailors its compliance features for sectors like healthcare and insurance; supports various standards.	Maps its risk analytics to standards such as HIPAA and ISO 27001.
Audit Report	Generates automated audit reports summarizing IT risk and compliance posture.	Provides detailed risk and compliance reports useful for audit purposes.
Cost Estimation	Helps optimize technology spending through actionable risk scoring insights.	Offers insights that drive cost optimization by identifying high-risk or redundant assets.

Real Time	Features a real-time dashboard that continuously updates asset and risk data.	Utilizes real-time analytics to monitor asset health and vulnerabilities.
Industries They Work With	Primarily serves Financial Services, Healthcare, and Insurance sectors.	Serves a broad range including government, finance, and healthcare.
How They Warn About Vulnerabilities	Uses email alerts and dashboard notifications driven by its risk scoring model.	Sends real-time platform alerts based on continuous risk analytics.
AWS Collectors	Cloud-based design implies AWS integration; specifics are less prominently detailed.	Likely integrates AWS asset data as part of its overall risk assessment.

Armis	Axonius
Offers compliance reporting aligned with frameworks like NIST and CIS.	Aggregates asset data to support audit reporting and helps meet regulatory requirements.
Monitors devices for outdated software and maintenance issues, especially in OT/IoT.	Tracks asset lifecycle events to aid proactive maintenance scheduling.
Detects EOL/EOS conditions in devices, with focus on operational technology.	Provides visibility into asset lifecycle events including EOL/EOS/EOM status.
Excels at discovering both managed and unmanaged assets across IT, OT, and IoT.	Unifies data from multiple sources to ensure complete and current asset records.
Prioritizes high-value assets via threat and gap analysis across diverse device types.	Correlates asset data to identify high-value targets that need immediate protection.
Discovers and inventories a wide range of device types including unmanaged ones.	Offers a centralized inventory drawn from over 1,200 adapters covering all asset types.
Correlates vulnerabilities with asset data; specific mention of NVD is limited.	Integrates with NVD and other vulnerability feeds to provide comprehensive risk data.
Alerts teams on vulnerabilities to prompt timely patching, especially for IoT/OT.	Integrates with patch management tools to automate and prioritize remediation.
Offers real-time alerts on abnormal device behavior to prevent breaches.	Uses near-real-time notifications to quickly alert teams to emerging breach risks.
Offers deployment options suitable for MSPs, especially for complex IoT/OT environments.	Provides robust integrations and reporting that support MSP service delivery models.
Excels in detecting IT, OT, IoT, medical, and industrial devices.	Unifies assets across IT, cloud, SaaS, IoT, OT, and more.
Provided as a cloud-based platform with strong real-time and AI-driven capabilities.	Fully cloud-delivered with extensive integrations and centralized management.
Integrates with existing security tools and external threat feeds.	Offers extensive bi-directional integrations that enable automated workflows and enforcement actions.
Aligns compliance reporting with frameworks like NIST, CIS, and others.	Supports audit reporting and compliance across multiple frameworks via integrated data.
Offers compliance and gap analysis reports that assist in audits.	Delivers comprehensive, automated audit reports with deep asset insights.
Enables cost estimation by highlighting vulnerable and outdated devices.	Provides cost optimization insights through detailed asset and risk analytics.

Delivers real-time asset discovery and threat alerts.

Offers near-real-time updates via extensive integrations and automated processes.

Focuses on industries with significant IoT/OT needs (e.g., manufacturing, energy, healthcare).

Versatile usage across finance, healthcare, energy, education, and more.

Employs AI-driven, real-time alerts on abnormal behaviors and vulnerabilities.

Utilizes a findings center, dashboards, and automated enforcement actions for timely alerts.

Primarily focused on network/IoT, but can include AWS integrations for broader visibility.

Provides dedicated AWS collectors/adapters for comprehensive cloud asset discovery.