AXONIUS KEY DIFFERENTIATORS

The challenge of gaining visibility into all assets with sufficient context has hindered IT and security teams for many years… until now. For this reason, many organizations are turning to Axonius to serve as the system of record that allows teams to triage IT and security incidents, improve security operations and vulnerability management, and optimize technology infrastructure decisions.

The Axonius approach is the most effective because of the following key differentiators:

ADAPTERS

IT and security teams cannot rely on a single source for a complete view of an asset (or collection of assets), since individual tools can only provide a myopic view. Each solution provides different data about the asset that the solution manages. The depth and breadth of Axonius adapters makes it easy to aggregate and correlate data from many solutions for greater data accuracy and context for all assets.

Axonius customers get immediate value as they're able to connect to 650+ adapters (pre-built integrations) and leverage 150+ pre-built automated actions. This enables teams to understand and optimize their environments faster, without installing additional agents as Axonius relies on open APIs to connect new digital infrastructure.

CORRELATION

Axonius adapters are built to deduplicate, normalize, and correlate asset data from multiple sources. This provides a holistic and highly contextualized view of every asset in the inventory. Normalizing the data is imperative in order to perform cross-tool correlation, meaning correlating the same device and/or user records from multiple adapters — this provides a holistic and highly contextualized view of every asset in the inventory, which is otherwise impossible to curate.

QUERIES

The Axonius Query Wizard enables customers to ask questions and get answers spanning multiple data sources to quickly see how assets adhere to or deviate from policies. With out of the box queries as well as the ability to create ad hoc queries, customers can filter, customize, and save queries to match their criteria.

ENFORCEMENT ACTIONS

The Axonius Enforcement Center can be used on an ad hoc or programmatic basis to execute a variety of automated actions based upon variances from security policies, regulatory and compliance frameworks, or general IT hygiene. Based on any saved query, enforcement sets allow customers to trigger over 150 actions to notify, enrich asset data, update CMDB data, remediate misconfigurations, and much more. The Axonius Enforcement Center includes over 150 out-of-the-box actions that allow customers to notify, enrich asset data and existing CMDBs, or remediate asset configurations for devices, users, and cloud instances.

The end result for Axonius customers: Actionable data. The options are limitless when customers are able to understand and trigger action on their cyber asset data.

RELIABILITY

Axonius invests significant R&D resources to build, support, troubleshoot, and maintain integrations. This allows customers to trust and rely on asset data in Axonius even when vendor APIs change and customers alter their technology stack.

**To see Axonius and each of its differentiators in action, request a demo.
You can also learn more about Axonius by visiting the website.**