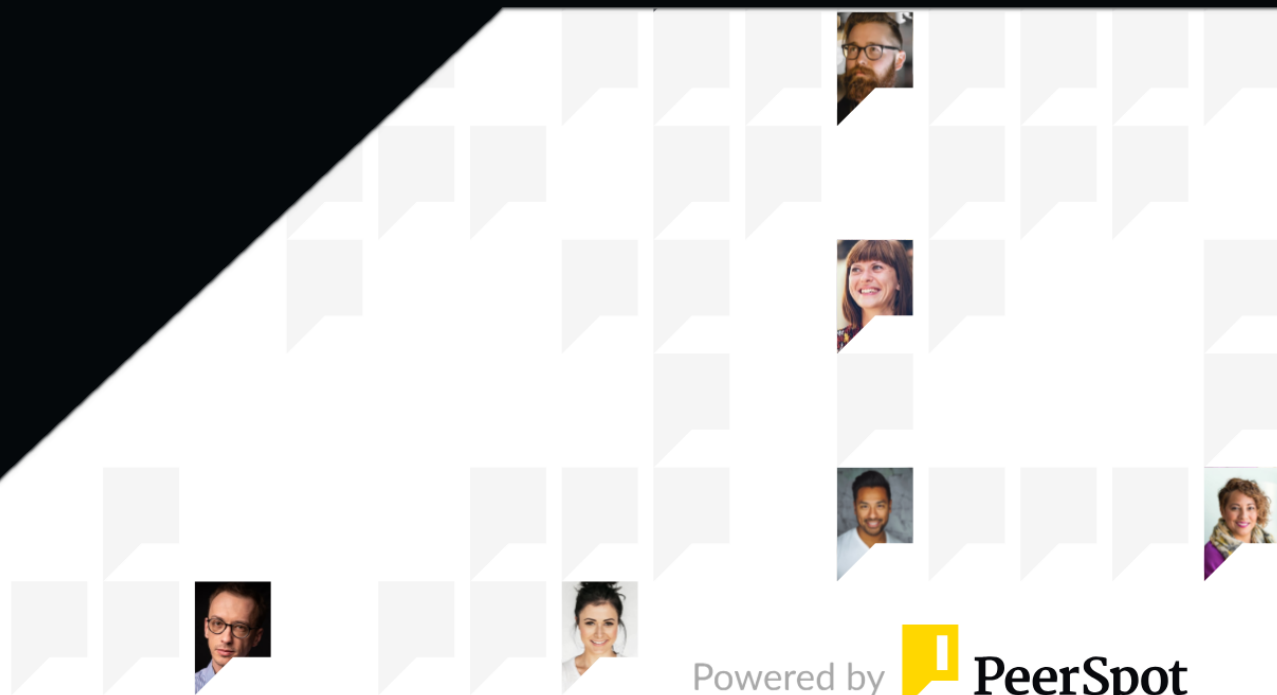




Axonius

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 11

Other Solutions Considered..... 12 - 13

Use Case..... 14 - 17

Setup..... 18 - 25

Customer Service and Support..... 26 - 28

Other Advice..... 29 - 36

Trends..... 37 - 38

About PeerSpot..... 39 - 40

Product Recap



Axonius

Axonius Recap

Axonius offers robust asset management, enhancing network visibility by consolidating data from various devices. It excels in automatic device categorization for up-to-date inventories, crucial for compliance and risk assessments. Key features include automated policy enforcement and comprehensive reporting tools, which streamline workflows and improve organizational productivity and security compliance. Integrations with other IT tools further enhance its efficiency.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Axonius provides preconfigured dashboards that can be customized to your needs.”



Kirubakaran Jayakumar

Security Operations Engineer at Nitro



“The solution's technical support was good...The product's initial setup phase is pretty straightforward.”



Verified user

Sr. Systems Engineer at a tech services company with 11-50 employees



“The automation capabilities in Axonius have streamlined our security operations.”



Eric Vollman

Information Security Business Enablement Mgr. at a insurance company with 5,001-10,000 employees



“Overall, I would rate Axonius an eight out of ten.”



Verified user

Systems Engineer at a tech services company with 11-50 employees



“I like that the tool has a user-friendly interface. It helps organizations and big companies improve business requirements and control processes.”



Alexander Bershtansky

Cross Platform Development/Solutions Architect at Kornit Digital



“he best feature I found in Axonius is that it shows us the duration of eCheck, and it shows us what device is down and in which part of the system life cycle or the checking part the system is down in.”



Leo Frank

IT Security System Administrator I at Mouser Electronics

What users had to say about valuable features:

From a security perspective, Axonius allows users to check for obsolete operating systems, like Windows XP or Windows 7. It highlights vulnerabilities due to unsupported systems, offering insights into network security issues. Axonius' integration with active directories and antivirus servers identifies PCs lacking antivirus solutions, pinpointing potential security vulnerabilities.

Verified user

[Read full review](#) 

Systems Engineer at a tech services company with 11-50 employees

“Within the system life cycle, Axonius does its eCheck. The best feature I found in Axonius is that it shows us the duration of eCheck, and it shows us what device is down and in which part of the system life cycle or the checking part the system is down in. So, investigating makes it a lot easier because we can pinpoint the exact time and location of the asset. And then, when you customize your queries, you can also figure out the reasons. I'm not very familiar with the customization of queries, but I've seen seniors do it, and it's quite brilliant to find or have a tool like that..”

Leo Frank

[Read full review](#) 

IT Security System Administrator I at Mouser Electronics

“The tool's query wizard isn't bad. Suppose you have ever used or even talked to anybody about other products that use vendor-specific queries, like Splunk, which is supposed to be one of the harder ones to use and master. Compared to Splunk, Axonius has made the tool a little more user-friendly where it is a little easier to use, and that is really the bread and butter of the product because that is where you get all your reporting from on your assets to make determinations on what you are looking for, like security or and if you wanted to use it for asset management, you could. As it pulls so much data, there are other options in the query that you could choose from depending on what information you were trying to obtain about your environment..”

Verified user

[Read full review](#) 

Sr. Systems Engineer at a tech services company with 11-50 employees

“The most valuable feature of Axonius is its ability to deduplicate records and identify which ones are old and stale versus those more relevant. For example, if you haven't logged in today but a system somewhere else mentions you have, Axonius can detect this through various logs like Active Directory, file logging, or Wi-Fi connections. Traditionally, someone would have to make numerous calls and spend a lot of time to find out if you are on-site or connected to a Wi-Fi network. The tool simplifies this process.

From my experience, onboarding and adding connectors was pretty easy, especially when integrating with the ServiceNow environment. It worked well for my use case, but the ease of use can depend on the customer's specific needs and what they are trying to achieve..”

Ashok Gunnia

[Read full review](#) 

Sr. IT Automation Technical Consultant at IBM

“Axonius has been the most effective in enhancing our security posture. When it comes to something like Axonius, the tool is only as effective as the source connections that you provide. Essentially, what Axonius does is it connects to a number of disparate sources in your environment, whether on-prem or SaaS applications, via API connections. Right now, Axonius has upwards of 900 or so of those out of the box. It comes down to what sources you want to connect to it to identify gaps in your ecosystem.


The automation capabilities in Axonius have streamlined our security operations. You're bringing all this data in, and Axonius does a great job of taking all this data, normalizing it, and correlating it together. It does all the deduplication and stuff for you. Then, you can build queries in the tool to see what you want to see.

For example, if I want to see everything that's not being scanned by a vulnerability scanner that's part of my Linux server population, I can do that. On top of that, Axonius has what's called an enforcement action feature. You can take action on the data you build in these queries. A good example of how to use this might be if you've got geolocation data coming in. You can build enforcement to say, "If I see someone logging in from anywhere outside of the continental US, I want CrowdStrike to go out there, and network isolate that machine, and cut it off from the network." You can orchestrate all of that from Axonius.

There are some machine-learning pieces at the back end of the tool. There is a feature that we're not currently using right now for query building. When you construct queries in Axonius, you don't need to learn any sort of query language or anything like that. It's got a logic builder that you can use. However, to make things even simpler, you can integrate it with OpenAI and ChatGPT, and you can use Axonius' company license for that, or you can use your own enterprise license. That allows you to really just text the questions, and it gives you the answers. It's as simple as it gets..”

Eric Vollman

Information Security Business Enablement Mgr. at a insurance company
with 5,001-10,000 employees

[Read full review](#) 

“It's the agentless solution. It doesn't rely on specific agents. We integrate Axonius with APIs, which are called adapters or connectors. Essentially, it's API connectivity between different platforms. Getting Axonius up and running only takes a few days. If you have a server or solution, you create firewall rules to integrate with other platforms. This way, Axonius can communicate and collect data from them without needing much infrastructure. It sits on a device and collects data from multiple environments and sources, aggregating everything into a single console.

It also creates multiple dashboards. Axonius provides preconfigured dashboards that can be customized to your needs. What I like is that everything is in one solution, and you don't need agents running on every process to collect information. Other platforms like ServiceNow rely on agents installed on assets, but Axonius doesn't.

Axonius is agentless and can easily integrate with other platforms. It uses API access accounts with other security solutions. They support a lot of different solutions. When we first started using Axonius, they supported around 400 IT solutions. Now, I think they support more than 600 or 700. I've lost count.


When we started working with them, Axonius was a small company with just a few engineers, but now they've grown into a large enterprise. They've been great at fixing issues and customizing solutions for clients. They maintain all of that really well.

It is a good solution; it lets you customize the solution based on customer requirements. They can even create custom adapters. For example, if you have a legacy platform or a new solution that doesn't have official support yet, Axonius can deliver quick fixes by developing custom adapters. I've worked with them when we needed to integrate a solution that wasn't in their supported integrations. They gathered the requirements, asked us what data we wanted to pull, and quickly delivered a custom adapter. They also added that adapter to their product timeline, ensuring it would become an official integration in future releases.

In that sense, Axonius has been fantastic at delivering these solutions. We've had no issues with them..”

KirubakaranJayakumar

Security Operations Engineer at Nitro

[Read full review](#) 

Other Solutions Considered

“Probably, if you have other solutions like ServiceNow, because a lot of companies already have ServiceNow, you might not find much value in moving to Axonius. Whatever Axonius provides, ServiceNow also provides it. So, you need to assess what you’re planning to use it for and check the features that Axonius provides.


See whether you want to move platforms. They have a few unique features within the platform. But if a company already has a proper CMDB or an asset management solution, you should review your current internal solutions and see the benefit of moving toward Axonius. It might be a financial decision or just a couple of features that Axonius provides additionally on top of the CMDB..”

KirubakaranJayakumar

Security Operations Engineer at Nitro

[Read full review](#) 

“Gartner classifies Axonius as a CASM tool. I am not familiar with the tool's competitors. I don't know because that is kind of a newer thing and not brand new, but probably within the last two or three years. It is the first time I have heard of it. I know there are other tools that offer a similar capability. Axonius is an attack surface type tool, and what is cool is that when you have a known vulnerability, like, a day zero, and there's no real fix for it just yet or the vendors are working on it, and they may have to have some workarounds, you can run queries against your whole environment to find those assets that may be affected so that you know right away what your security posture would be in the event of a day zero for whatever asset we're talking about. In this case, then you would have a clear picture of the number of assets that I need to perform this workaround until the vendor can come up with a patch. In that instance, it kind of serves as an asset manager because you are looking at it for assets. The confusing thing to people about the product is that it grabs so much data about your environment that you can use it for a multitude of purposes, and asset management, which could definitely be one of them, but they don't market the product as an asset management tool. We used it as a CASM tool..”

Verified user[Read full review](#) 

Sr. Systems Engineer at a tech services company with 11-50 employees

Use Case

“We use Axonius as an asset monitoring tool. Our adapters and assets are tagged into Axonics using an AD group. We have segregated into region-wise assets, and it's easy to look at the dashboard and see if an investment is down in a particular region..”

Leo Frank

IT Security System Administrator I at Mouser Electronics

[Read full review](#) 

“In my company, we did a production pilot in my environment where I work to evaluate the tool's capabilities, and our use case was looking for unmanaged endpoints, like workstations that may have fallen out of management by their management server, like McAfee, Tanium, SCCM, or similar things..”

Verified user

Sr. Systems Engineer at a tech services company with 11-50 employees

[Read full review](#) 

“The tool's main use case is connecting multiple IT systems using various adapters. It helps identify device registration, uptime, usage, and deviations from expected performance. When deviations are detected, you get alerts and can take necessary actions. A major use case is its integration with ServiceNow, which provides a landscape of your devices and allows you to see them and write policies accordingly..”

Ashok Gunnia

Sr. IT Automation Technical Consultant at IBM

[Read full review](#) 

The general use case for Axonius is cybersecurity asset management. My company, an IT solution provider, works with Axonius to offer both asset management and cybersecurity asset management. This provides full visibility of the assets in the network. Axonius integrates with the customer's existing setup, such as Office 365, Zoom, servers, firewalls, antivirus, email security, and active directories, to give a comprehensive view of the assets they have in their network.

Verified user

Systems Engineer at a tech services company with 11-50 employees

[Read full review](#) 

“We use it for reporting, noncompliance reporting, and identifying gaps. We use it for API monitoring within our company.

And we also use it as a CMDB. Our security team, people within the SOC team, and people within other IT departments use it as a CMDB. We have integrated Axonius with a few of our solutions, so it has good inventory mapping. It provides information like installed software, running services, file shares, patches, and more. We have integrated it with many different solutions that we use internally.

We refer to Axonius as a CMDB, but the tool was actually onboarded for KPI monitoring and to alert against noncompliances. For example, if a device is running with an out-of-date agent or if a device is missing an agent it is supposed to have, Axonius helps us find unauthorized software installations within corporate devices. We use it for various KPI metrics and send out automated alerts to the relevant IT personnel to address and fix those noncompliances.

Right now, we use it mainly as a CMDB, but the tool was onboarded for KPI monitoring and metrics..”

KirubakaranJayakumar

Security Operations Engineer at Nitro

[Read full review](#) 

“We've got we've got a ton of use cases for the solution. However, a lot of companies will use it primarily on the IT asset management side, which it does a terrific job of. We do use it for specific use cases tied to that. That said, being in the security realm, we really use it as a cyber attack surface and security control gap tool.

For us, on the security side, we connect our EDR solution, like CrowdStrike and Carbon Black or any access control like Azure Active Directory and regular Active Directory, et cetera. It allows you to identify whether or not what you consider the asset source of truth in your environment is actually doing a good job or not. A CMDB, for example, a lot of folks want to rely on that as a source of truth for all assets.

However, when you connect these disparate sources to Axonius, you're able to see and identify the gaps that you might have in that inventory. If you've got a vulnerability scanner scanning an asset or EDR on a specific tool that you can see but don't see in your CMDB, you've identified a gap. You can use that for a number of cases. You can, for example, see stuff that's in your CMDB that you don't have malware coverage for. That's really where the power of Axonius comes in – to be able to identify those gaps. That's one major use case, and that's a really big one in our space..”

Eric Vollman[Read full review](#) 

Information Security Business Enablement Mgr. at a insurance company
with 5,001-10,000 employees

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

If the customer has prepared all prerequisites properly, Axonius can be deployed within one or two days. The initial setup is quite fast and efficient if all requirements are met beforehand.

Verified user[Read full review](#) 

Systems Engineer at a tech services company with 11-50 employees

“I was not involved in the initial setup process. But as per the deployment team, it is a relatively straightforward tool, especially if you're good at writing queries. Axonius has all the information so neatly documented that if a non-technical person looks at the dashboard, they can set it up. The solution was deployed on-premises, but now we are migrating to the cloud. .”

Leo Frank[Read full review](#) 

IT Security System Administrator I at Mouser Electronics

“The deployment was straightforward for us. There are a number of deployment methods. There's a strictly on-prem one. There's a hybrid deployment. We went with vendor-managed deployment. As far as deploying the instance, it took them a matter of minutes to turn it on.

In terms of deploying it with connecting sources to it, that's largely dependent upon your organization's speed. That said, they make the adapter connections really easy to connect. It's pretty simple.

If you have experience with APIs, the setup is pretty easy..”

Eric Vollman


[Read full review](#) 

Information Security Business Enablement Mgr. at a insurance company
with 5,001-10,000 employees

“The product's initial setup phase is pretty straightforward. My company operates in a VMware environment, so we get the pre-configured VMware servers that are offered. We just import those into VMware, the servers, and basically figure them out for our environment with TCP/IP and DNS. NTP and all the normal stuff that you would do for servers to deploy are good for working with, but they don't give you full SSH access. The tool has a menu-driven tool that you can use too, and it has been maturing over time because when the product was first rolled out, and we started using it, we had a lot of interaction with their security and their engineers because they don't want you to go in and have full SSH access because you could cause issues as you won't know what you are doing. You could break their product, and so they limit your access on purpose so that you won't cause any issues. If you need anything that requires more access, then they give you access, after which you have to get with them. They are responsive and help you troubleshoot with Microsoft Teams so that they can see what we are doing. We can have sessions where we can share stuff, and they just tell us what to do. And they'll send us, you know, syntaxes that we need to input, you know, stuff like that. As we have gone along, the menu-driven tool they call the toolbox, or Axonius toolbox, is what you use for, like, day-to-day administration to do the basic back-end server stuff, and that toolbox is actually reachable through SSH access on the back-end servers on the CLI. You don't see that in the user interface where the regular users would be doing queries and using the product as a user. I am talking about administrative stuff here.

For us, the product's deployment phase was a little challenging because we had to deal with other departments and business units. We were dependent on the tool's team because they had the keys to their kingdom, so we had to work with them to get the product deployed and get it connected to their systems because they had to, in some cases, make a service account for us and configure it to be read-only, give us the password, and then we would input that on our side to be able to connect to their system their back end system. There was change management involved. There were server firewall rules. Typically, we did that collector, which was a server role, and we would implement a collector in the environment, and then we would just the collector in that environment would just fetch the data from those different servers with those pre-configured accounts. Sometimes, they could be

domain accounts if whatever solution it was was domain joined. It was able to have a Windows service account if it wasn't a Windows system. Windows systems are pretty much domain-joined, and you could use an Active Directory service account on those systems that we could set up. Then, we would tell them what we made, and then they would add it on their side, and then it would work. There were some hiccups here and there, of course, getting that stuff straightened out. It probably took about six months for us to get everything working just because of the scale of our environment and all the different people that we had to work with. It really becomes a delay because they own those systems..”

Verified user[Read full review](#) 

Sr. Systems Engineer at a tech services company with 11-50 employees

“ Since it’s an OVA package, it’s a virtualization package that you can just deploy on your VMware, ESXi, or whatever virtualization solution that your company internally uses. It’s just, like, import it, and then they’ll provide you with a license key. If you do a POC, they’ll provide you with a license key for a month so you can try it out and see how the product is going. Once you’re happy, they can provide you with a proper license for however many years you are going to sign the contract with them.

But, the initial setup is pretty straightforward. It’s not like you need to change a lot of things in your environment. It runs in a standalone installation. They also provide a cluster-based solution. If your IT presence is across the globe and you have huge latency that you want to reduce, you can have multiple instances in your different data centers and then aggregate that information in a centralized cluster and show it in a single dashboard. They started offering this around the same time we began working with them.

In terms of onboarding, it only takes a couple of days. It's mostly dependent on your organization's RFCs, change requests, and approval processes. There aren't a lot of configurations needed. You just need to open a few firewall ports for product updates.

The product runs on a Debian-based operating system, and you can scale it based on your requirements. If you're trying to pull 50,000 assets, the requirements will be a bit different. You'll need something like 8 cores, 16 or 32 gigs of RAM, and probably 5 terabytes of storage to store the data.

One of the good features of the product is snapshots. You can go back to specific dates and check the inventory status at that time. Axonius has an option to take daily snapshots within the product.

Axonius collects data from other platforms, and you can configure it to take snapshots at specific times. It keeps the snapshots for as long as you want, impacting your storage. You can keep the snapshots for ten years and still go back to a specific date to check how many assets you had, how many were identified for

a specific noncompliance, and when it was fixed. You can check all of those details going back to a specific point in time and still get that information.

Lots of other products, like CMDB products or cyber asset management products, don't have that functionality. Other platforms give you live data but don't provide an option to go back and check how it was ten months or a year ago. Axonius gives you historical information and keeps it as long as you want. You can configure it to store the data for one year or ten years based on your storage capacity.

That's one of the good features we heavily rely on internally..”

KirubakaranJayakumar

Security Operations Engineer at Nitro

[Read full review](#) 

Customer Service and Support

The support provided by Axonius is good, but it requires improvement as the company is still growing. They respond when contacted, but during high demand, the quality can be affected. Overall, the knowledge base is good.

Verified user

Systems Engineer at a tech services company with 11-50 employees

[Read full review](#) 

“They’re really great people to work with. Every customer has a dedicated technical account manager. We usually have weekly calls with them to check on everything. When we onboarded the platform, we had regular calls, and they were always available. That was a great experience working with them..”

KirubakaranJayakumar

Security Operations Engineer at Nitro

[Read full review](#) 

“The solution's technical support was good. The tool has a technical account manager and then an engineer. Both of them worked with you, and they were very responsive and quick to help us fix any issues that we had with the tool. At some point in time, I know that the product will mature. When you go to patch the product or upgrade the product, it was being developed when we were using it, so we weren't able to use it yet because it was still under development, and it was, like, a patching server, which is almost like what Microsoft WSUS server is, where you have a server in your environment that you can use potentially, or you could even go across the internet. There are machines that are more air-gapped where they can't talk to the internet directly. You could potentially have a server like in your DMZ, and it could talk to Axonius and pull down patches. Then, your servers inside could talk to that to automate patching, and Axonius was working on it. As it is going to be a year in December, I think the tool is probably up and running, and it might even be using it now. There were different kinds of initiatives that Axonius was working on at the time to improve the product, and now the tool is getting more cloud integration as well. The tool has its Azure and AWS offerings. If you know anything also about the architecture, the main server is called the core server, and it has a database known as MongoDB, which basically collects and stores all the data. We have the other server role. We used a couple of server roles, and one was the core server because you have to have that since it is where the GUI is hosted. When you connect to the GUI, you are actually connecting to the core node. It's presented from the core node, and then they have what they call collectors. You can take those collectors and place them throughout your environment, and what is nice about the collectors is that they only use a single TCP port. You could place the collector in an environment that may collect several different types of data from different assets. In such a case, if you didn't use the collector, you would have to have multiple firewall rules. If you are collecting data from Microsoft servers, like Active Directory and SCCM, DHCP, and certain Microsoft services or Linux services or other products as well, Axonius integrates with a ton of tools. The tool had around 700 adapters that it had developed, and some of them were better than others as far as their maturity and what they gathered because we would go into it, and we would connect one of these adapters thinking that we were going to get all the data. Axonius publishes what you can collect. It is good to go out and look at the adapter and what kind of data it can

gather before you use it. It may not give you what you are looking for. We connected to probably ten or twelve different connections or adapters to different products in our environment. We had multiple collectors deployed, and it was nice because you just had to get one firewall rule implemented, as it would collect everything locally in that subnet where all those back-end servers lived. Then, all those ports and protocols were there because it was in a VLAN, and they were already opened anyway, so you didn't need any firewall rules there. The tool saves you time with firewall rules because where I work, firewall rules can be a headache because you have to go through change management and do all this stuff to get them implemented, and that can take time as it all gets scrutinized. It is nice to be able to just have one port open or one TCP port, really, for the collector node, which is the communication from the core node to the collector node to actually pump that data back from the collector to the core node to be put into the database. I rate the support a ten out of ten..”

Verified user[Read full review](#) 

Sr. Systems Engineer at a tech services company with 11-50 employees

Other Advice

Overall, I would rate Axonius an eight out of ten. It's a unique tool with great potential and offers excellent asset management capabilities combined with cybersecurity insights. I would rate the overall solution an 8 out of 10.

Verified user

Systems Engineer at a tech services company with 11-50 employees

[Read full review](#) 

“I'm a customer.

I'd rate the solution eight out of ten. I'd recommend the solution to others.

People need to keep in mind that the data that Axonius provides is only as good as the data you give it. So, if you've got a messy environment, be prepared to come up with inventive ways to look at the right scope of resources or assets in the tool to facilitate cleaning up your environment. That can be challenging at the outset..”

Eric Vollman

Information Security Business Enablement Mgr. at a insurance company
with 5,001-10,000 employees

[Read full review](#) 

“I use the tool's SaaS version. As an IT operations professional, you should know what you're doing before using this tool. It's not an end-user tool; it's meant for IT engineering, operations management, or developers. It depends on what you're trying to accomplish. So, I would advise understanding your goals clearly before integrating this tool into your operations.

Ensure you label and use tags appropriately. Tagging can get out of hand, so everyone must agree on the tagging system. This approach will help you scope your reports and policies effectively.

I rate the overall product an eight out of ten. .”

Ashok Gunnia

Sr. IT Automation Technical Consultant at IBM

[Read full review](#) 

“I would advise the new users that Axonius is an asset management tool. If you have a lot of assets that are not registered or have not been assigned, then Axonius is one of the tools you could use to tag your assets individually. Axonius makes your entire life easier when you want to know where each asset is.

We have a policy in place regarding the usage of AI. We have yet to figure out the security measures for how our data will be fed into Axonius and how it will be used to train the model; hence, we will not be using AI for now. Another piece of advice is that the reporting feature is brilliant. You'll have one of the best reports if you know how to get what you want from the query tools.

Overall, I would rate the solution a nine out of ten..”

Leo Frank

IT Security System Administrator I at Mouser Electronics

[Read full review](#) 

“At this stage, I would rate it an eight out of ten. The product needs to mature a little bit more in terms of following up on compliances.

Axonius is a US-based company. We had a few difficulties in getting the legal documents signed when we started working with them. If they had an EU presence, our legal department might have directly worked with them, and it would have been much easier. But since they are completely US-based, we had to sign a lot of data processing agreements and deal with transferring data between the EU and US. The legal department had a few hiccups, and it took some time to go through all those processes.

In the future, if they have a regional headquarters in the EU or where there is no data transfer from the EU region to other regions, it would be much easier for companies to start working with them quickly. In the initial days, we had to sign a lot of contracts because when we started working with them, we had to provide some sample data, and they had to sign a lot of DPA (Data Processing Agreements) between both companies and the legal team. It was a back-and-forth conversation, editing that legal agreement, and putting it in place between both companies.

We had a few issues in getting the single agreement signed in the initial days. But apart from that, no issues.

It's pretty much company-focused decision to choose a solution. If you don't have any solution for CMDB, I think it's good to go with Axonius because they have good integration. They support a lot of different tools. Within their platform, you have a separate section per adapter where they've mentioned probably 600 to 700 IT solutions that they can integrate and work with. You can also check within the description what kind of use cases you can get from that integration. For example, if you have some kind of vulnerability management solution or MECM or a BitLocker administration tool, Axonius will give you information on what kind of data it will pull from the individual sources. You can create reports, check BitLocker statuses, and see what kind of encryption has been applied and how it is maintained.

It will give you those use cases as well, showing what you can get out of that particular integration between Axonius and whatever solution you are looking for. You can list down all the solutions you use internally within your company and

then check the Axonius portal or website to see what use cases you can integrate with the platform. You can at least get an idea before you even try to speak with the Axonius team and start working with them yourself to see the benefits of utilizing the platform.

We don't use it to the fullest. We just use it for a few pieces because we have other solutions for that. But they have a lot of different features within the platform. We are not actually replacing everything. We just use a few bits and pieces, like enforcement center actions, CMDB, and a few other features within the platform..”

KirubakaranJayakumar

Security Operations Engineer at Nitro

[Read full review](#) 

“Axonius is used in our company's daily security operations to manage and secure assets, and it has its own query analyzer. You can run queries against the data that has been retrieved in the database to make assessments of your environment on a daily basis. The tool has what is known as adapters, and those adapters connect to systems within the environment to pull data into a central repository to basically crunch data and deduplicate it down to what is called a master endpoint record, which is a single entity that represents basically one machine across multiple management platforms as a client machine, and then you can do queries against it. The tool pulls in so much data that you could actually use it for other things. The first thing that comes out of anybody's mouth when they hear about the product is that it is an asset management tool, but our use case really wasn't associated with it, and we didn't get it for that. The tool is more secure than some other products. The tool is all about security. We have high-level security audits where someone will randomly come in and evaluate your environment by surprise, so you don't have time to prepare because they want to see what your operating stature is and if you have a normal operating stature. When someone comes in to evaluate our environment, and they look for machines that are not being managed by their

servers, and they could actually present a vulnerability, then it can definitely hurt your security score in the end when they are coming in to evaluate your security posture.

The tool has automated capabilities that can remediate machines. It can. The tool definitely has automation capability, but we didn't use that. We were just basically using it to pull data from our management servers about the clients they manage to make determinations on our endpoints. You won't always know sometimes if your endpoint is functioning or not if you have so many of them. Basically, what it does is that it just connects you to all your management servers that manage those clients, and you can see graphically because, in the interface, it actually shows for the entity in question, like, say, it is just a workstation. It will show each management tool and the icon for that management tool, as well as the vendor's icon next to it, to show you that it is checked in with that server and that it's actually communicating with that server as a client machine to give you an idea if you have any endpoints that aren't being managed from any one of your management servers for your management tools.

When it comes to integrations, the tool uses service accounts to do it, and they have a notion of a read-only service account, which is what we use. Or you can have one that has more authority or rights where it can actually take action. We did a production pilot because we needed real data. Originally, we did a pilot in a lab environment, but those servers in our lab environment don't really have a lot of data that is meaningful to us. We did a production pilot, which was accepted because we used read-only accounts, and all they will do is just pull data, and all the system needs, the management servers need, or all the service account needs is a read-only role on the servers so that it can just read the data and pull that data. It was a safer bet for us because we were just doing the production pilot. We needed real data to evaluate the product and see if it would meet our needs. The accounts were actually just read-only, which was the safe way to go in a production environment. The only thing that you had to worry about was that Axonius advertises that certain systems can take a performance hit when they get when that job runs, and they call it a fetch, and it runs periodically, and you can control that. You are in complete control of what time it fetches. We did it off hours, and we actually worked with the different teams to schedule it because if they had any

operations that they ran off hours, we didn't want to interfere with that. We worked within the individual teams that manage those servers, like SCCM's team, McAfee's team, and Tenable's team, to be able to make sure that we were optimizing our fetches around their schedule that was good for that platform.

The performance issues in the tool have been optimized to a level by Axonius, where the tool can tell by the stream of data what kind of performance they are getting across the wire, like the network. The tool knows the network bandwidth that is being used and things like that, and it will actually adjust that on its own. There are only really a couple of systems that advertise, and one of them was SCCM, which is now MECM. I believe that Microsoft has changed SCCM to MECM. I think it was Tenable because Tenable can have multiple repositories that you can configure for the product to use, and we can schedule those off hours. I just think that certain systems, depending on how much data they are going to fetch, can take a hit depending on how busy they are and stuff like that. In the end, we really didn't have any problems once we worked with the individual teams to polish and schedule the right fetch for the platform because they were SMEs who knew about the product. SMEs have worked with the tool, and we really didn't have any issues in the beginning because we worked with those individual teams where there was some coordination with the tool.

The tool does have AI initiatives, but we have not yet integrated the product with any AI features. We didn't get the funding to continue our pilot as well. In December, I think it will be a year since the product has been turned off. Users have liked the product, and it is possible that it may receive funding in the future, in which case it could be powered back on and then brought back to life because, basically, they are virtual machines in VMware on-premises. Axonius does have a SaaS offering that you can run on AWS and Azure. We had an on-premise solution, and we managed everything completely. For more infrastructure as a service, we have a little private cloud.

I would recommend the tool to others because it is kind of unique in what it does. I have never seen another tool do this before where it doesn't talk to any clients itself, so it is agentless. It pulls from your back-end servers and then correlates the data that it receives on those servers to create what I was saying before is what they call a master endpoint record, which represents a single entity across all

those servers that may be like a workstation that is being managed that is definitely communicating and getting its updates to its management servers with all you know, and it could be because it is a client with multiple servers. I don't know any other tool that really does that in that fashion where there is no impact on the endpoint itself.

I have been out of the loop for a little while now, and I haven't been using the tool. There are probably all kinds of new capabilities in the tool that I am not even aware of because when we were on it, I was working on it day to day for, like, a couple of years. So we were pretty up to date on all the new features that were coming out, some of their roadmap items, and where they were going with their product. Now, I have kind of been out of the loop for a little bit. I guess what you would probably think about is whether or not you would use it on-premise or in the cloud environment, depending on what kind of assets you have. As I understand, I think now it can reach back from the cloud through a gateway of some kind that you may have in your environment so that it could potentially get your on-premise stuff and cloud stuff altogether to where you didn't have to have separate installations. The tool does have integrations where you can have multiple sites, and they roll up all their data to a server in the cloud. You could just report right from the cloud on all the assets that were on-premises across your enterprise. The tool has a lot of capability. The product that we had was actually used on Rocky Linux, which is a Red Hat tool. The tool would release patches periodically or a monthly patch that was a security patch that they would give you that you would install for security. The tool would also have updates or upgrades where you could roll out upgrades, which is something that we usually did during the evenings when we had a maintenance window so that the user base wouldn't be using it.

I am not really a security person. I am more of a virtualization engineer, so I work with VMware stuff and infrastructure and stuff like that. Our security people loved it because it did what the vendor said it would do, as they were able to find workstations and even other devices that weren't being managed. Not only that, it is good to find network devices that you may not be aware of that may be causing you a problem or could be security-related. One of the things with Axonius was that in some environments, it could find these little networks, like a Raspberry Pi or something like that, plugged into the network or something that shouldn't be

plugged into the network. It would be able to find these devices where nothing else really could. The tool really kinda does work as they say, and it could help you with your security posture.

I rate the tool a ten out of ten..”

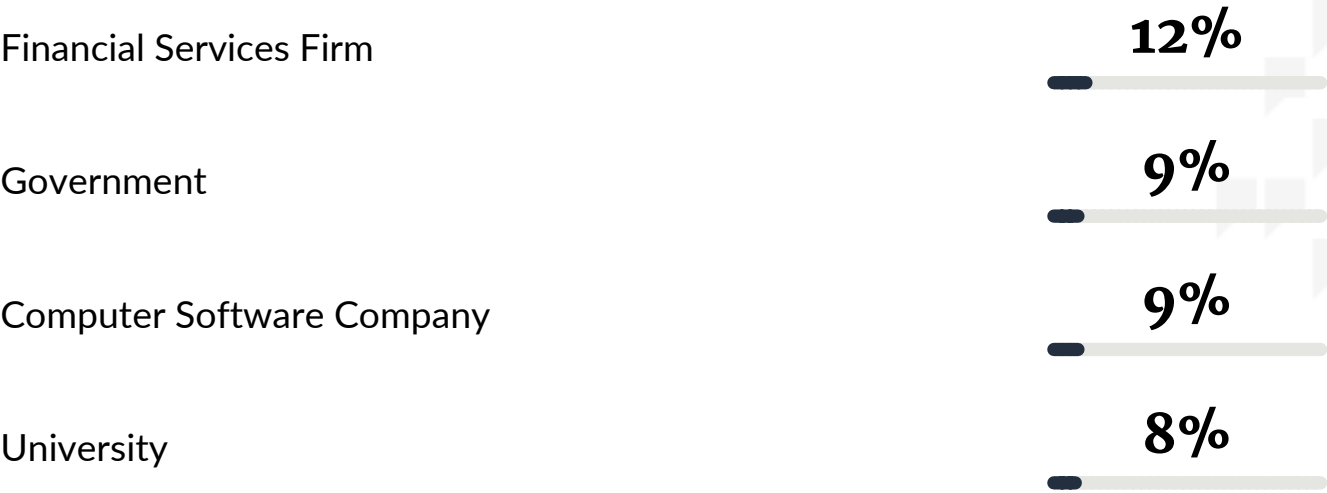
Verified user

Sr. Systems Engineer at a tech services company with 11-50 employees

[Read full review](#) 

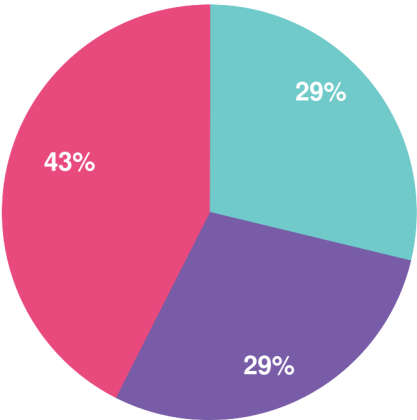
Top Industries

by visitors reading reviews

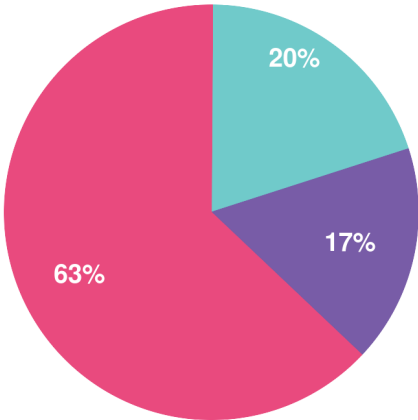


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsized Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a [customized report](#) of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

[Get your personalized report here](#)

About PeerSpot

PeerSpot is the leading review site for software running on AWS and other platforms. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944