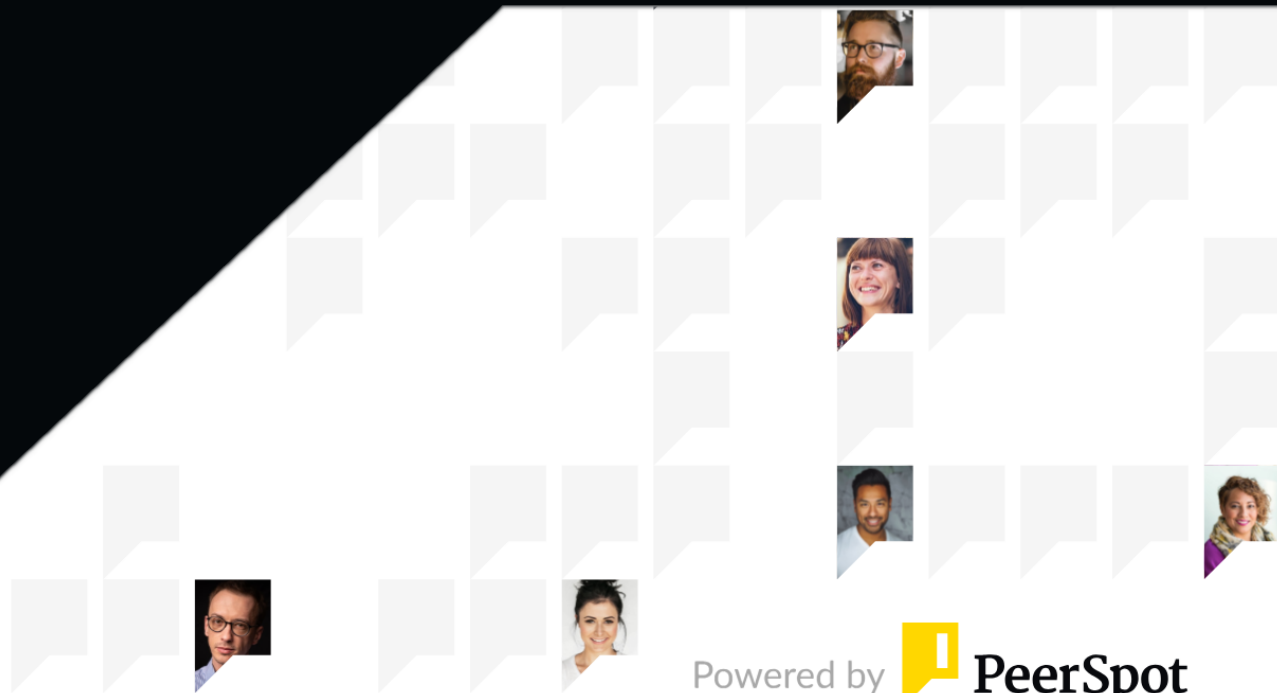




Axonius

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13 - 15

ROI..... 16

Use Case..... 17 - 20

Setup..... 21 - 28

Customer Service and Support..... 29 - 31

Other Advice..... 32 - 35

Trends..... 36 - 37

About PeerSpot..... 38 - 39

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 has positively impacted my organization significantly, as we discover thousands upon thousands of devices that don't have EDR tools, which means they are not protected.”



Zhtay Zhtay

senior security engineer at a educational organization with 5,001-10,000 employees



“With this solution in place, we are now 100% compliant along with security functions or operations area management.”



Sakkemgari Tamagari

Director of cloud security at Nuxeo



“In comparing Axonius to other products, I believe its main competitors on the market offer similar functionalities, but my experience with other solutions has shown me that Axonius stands out.”



Leo Frank

IT Security System Administrator I at a manufacturing company with 1,001-5,000 employees



“Axonius offers excellent features including ease of use, the ability to ingest all assets at one central display, creating multiple visualization dashboards, the ability to create an enforcement center to complete tasks and support the program, and support for government operations.”



Sam Al-Shaheri

Axonius System Engineer at a tech services company with 10,001+ employees



“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

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

“Axonius offers excellent features including ease of use, the ability to ingest all assets at one central display, creating multiple visualization dashboards, the ability to create an enforcement center to complete tasks and support the program, and support for government operations.

“I find myself using dashboard creation and creating new enforcement actions the most, as they have helped me in my day-to-day work.

“Axonius has positively impacted my organization by making it easier to create visualized dashboards, enabling the creation of easy-to-visualize asset counts, asset summaries, CVE reports, and CVE vulnerability data reports..”

Sam Al-Shaheri

[Read full review](#) 

Axonius System Engineer at a tech services company with 10,001+ employees

“I find that the features I have found most valuable include its comprehensive functionality.

“I am using Axonius's centralized dashboard for visualization of security coverage, and I find it quite useful.

“I find that the integration capabilities of Axonius with IT and security solutions are good.

“In my opinion, the main benefits Axonius provides for me as a point user include saving time, saving money, and streamlining processes..”

Leo Frank

IT Security System Administrator I at a manufacturing company with 1,001-5,000 employees

[Read full review](#) 

“The best features Axonius offers, in my opinion, are asset discovery, finding rogue devices, and vulnerability management.

When I mention device discovery and management, the speed of discovery, the level of detail, and network-level discovery stand out to me.

Axonius has positively impacted my organization significantly, as we discover thousands upon thousands of devices that don't have EDR tools, which means they are not protected. With Axonius, we were able to find them and deploy the EDR tool that they needed.

I can share that we found about the Linux servers and Windows servers, hundreds of them, that were deployed. They were re-imaged and didn't have an EDR tool, and the integration with other tools proved that these devices are live on our network, and they just don't have a specific tool that we need to deploy to them. .”

Zhtay Zhtay

senior security engineer at a educational organization with 5,001-10,000 employees

[Read full review](#) 

“The best features Axonius offers are inventory and tracking of the changes. The tracking of changes feature works for my team through recording all config changes as they happen over the period, showing who made the change and when, giving us visibility especially when someone made a change with associated reference information such as IT or Jira tickets, providing insights on the reasons behind the change.

“The main appreciation I have with this tool is the governance, as we had a big gap for the NIST and other compliance programs where we didn't have a good asset inventory or maintain the config database. With this solution in place, we are now 100% compliant along with security functions or operations area management.

“Axonius has positively impacted my organization, with one great improvement being the compliance program, which has centralized everything in one place. Additionally, with this solution in place, we can track quickly, helping us accelerate the incident response process.

“The acceleration of our incident response is notable because in the past, identifying assets and their ownership was really difficult. Now with this solution, we could quickly log into the system, identify the asset, and see the owner, allowing us to reach out to the right people and identify the group the asset belongs to. Having tags assigned helps indicate the application or environment it is currently running on, enabling us to quickly revert changes or mitigate issues that arise due to recent changes, which significantly improves our incident response process, especially containment and remediation..”

Sakkemgari Tamagari

Director of cloud security at Nuxeo

[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

“In comparing Axonius to other products, I believe its main competitors on the market offer similar functionalities, but my experience with other solutions has shown me that Axonius stands out..”

Leo Frank

IT Security System Administrator I at a manufacturing company with 1,001-5,000 employees

[Read full review](#) 

“Previously, I was using a custom in-house solution that was not performing well, as well as an AWS solution that did not provide full insights and was more manual..”

Sakkemgari Tamagari

Director of cloud security at Nuxeo

[Read full review](#) 

“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

ROI

Real user quotes about their ROI:

“I have seen a return on investment with Axonius. As part of the EDR deployment, we have saved tons of time pinning down these devices, where they are, and how we can deploy to them..”

Zhtay Zhtay

senior security engineer at a educational organization with 5,001-10,000 employees

[Read full review](#) 

Use Case

“My main use case for Axonius is as a sysadmin. I use Axonius to ingest data from security tools, provide access to users, create dashboards, and provide reports..”

Sam Al-Shaheri

Axonius System Engineer at a tech services company with 10,001+ employees

[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 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

[Read full review](#) 

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

“My main use case for Axonius is asset management and asset discovery.

For asset management and discovery, we scan our network through our entire environment and network level, and then we pick up all the devices that don't have an EDR tool or that are not protected by our EDR tools.

We run those scans weekly, and then we will find the device, and if it's applicable for deployment of the EDR tool, we will deploy them. .”

Zhtay Zhtay

[Read full review](#) 

senior security engineer at a educational organization with 5,001-10,000 employees

“My main use case for Axonius is config management and asset inventory. I use Axonius to maintain the asset inventory up to date and also to identify the owners quickly; these are the primary requirements, and it will help us build governance across all the assets that we have provisioned in different AWS accounts and the on-premises environment.

“Our team especially leverages Axonius for asset tracking and ownership. In terms of security incidents, it was really challenging for us to identify who created the asset, who the owner is, and how we can track what changes happened over the period; those are the big challenges in the past. Now with this solution in place, we can quickly track what the asset is, who is the owner, what changes have happened, and what caused a real incident or changes that really impacted the system, which can be easily tracked and identifiable, enabling us to reach out to the owner to fix things quickly..”

Sakkemgari Tamagari

Director of cloud security at Nuxeo

[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](#) 

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 a manufacturing company with 1,001-5,000 employees

“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 very much recommend Axonius and I tell everybody that they should use Axonius because it's one of the best discovery tools and asset discovery tools. I would rate this product an 8 out of 10..”

Zhtay Zhtay

senior security engineer at a educational organization with 5,001-10,000 employees

[Read full review](#) 

“My advice to others looking into using Axonius is to focus on centralized asset inventory, governance, and ownership. I do not have any business relationship with this vendor other than being a customer. I think Axonius is doing well overall. I would rate this review an eight out of ten..”

Sakkemgari Tamagari

Director of cloud security at Nuxeo

[Read full review](#) 

“I have not had the ability to use Axonius's AI governance and security feature yet, but I am looking forward to using it. I have not used Axonius's AI accuracy and reliability of output feature yet.

“I advise others looking into using Axonius to understand how the tools and data are ingested. Understanding how the data is gathered and how it's correlated gives the end user the ability to understand why Axonius is a great tool. I rate Axonius an eight out of ten..”

Sam Al-Shaheri

Axonius System Engineer at a tech services company with 10,001+ employees

[Read full review](#) 

“Regarding Axonius's automated enforcement actions, I find them useful, and I am actively using them in that area.

“I do use Axonius in maintaining compliance with regulatory frameworks like GDPR or HIPAA, and I think that is a good approach.

“I would give this review a rating of 10 out of 10..”

Leo Frank

IT Security System Administrator I at a manufacturing company with 1,001-5,000 employees

[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](#) 

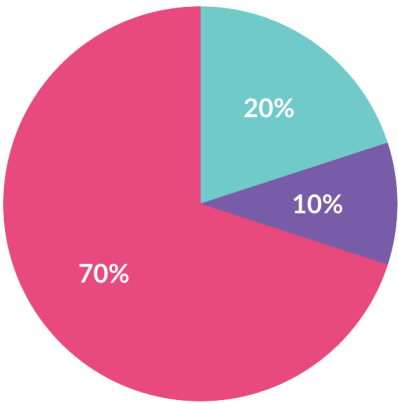
Top Industries

by visitors reading reviews

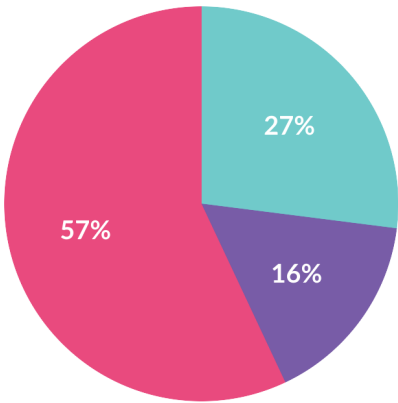


Company Size

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 cloud, AI, and business software. 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