

aws marketplace

Automox

# Reviews, tips, and advice from real users



Powered by  PeerSpot



# Contents

- Product Recap..... 3 - 4
- Valuable Features..... 5 - 13
- Other Solutions Considered..... 14 - 16
- ROI..... 17 - 19
- Use Case..... 20 - 23
- Setup..... 24 - 29
- Customer Service and Support..... 30 - 32
- Other Advice..... 33 - 36
- Trends..... 37 - 38
- About PeerSpot..... 39 - 40

# Product Recap



Automox

# Automox Recap

Automox offers automated patch management with cloud-native architecture, cross-platform compatibility, and ease of use. It provides real-time visibility and streamlines operations across Windows, macOS, and Linux, making it ideal for complex IT environments.

Automox empowers organizations with features like Worklets and remote management, enhancing security and efficiency through customizable patching policies, PowerShell script execution, and detailed reporting. It's primarily used for automated patch management, patch remediation, and compliance maintenance across diverse systems, ensuring cybersecurity and reducing vulnerabilities. Enhancements are desired for user access control, policy synchronization, and integration with tools like Tenable. Support for offline patching, rollback features, enhanced reporting, and notification customization are in demand. Improvements in cost effectiveness and multi-group policy applications are also suggested.

## What are the key features of Automox?

- **Automated Patching:** Streamlines updates across operating systems.
- **Cloud-Native Architecture:** Offers real-time visibility and ease of use.
- **Cross-Platform Compatibility:** Supports Windows, macOS, and Linux.
- **Worklets:** Custom scripts for automating tasks.
- **Remote Management:** Manage devices from anywhere.
- **Custom Patching Policies:** Tailor updates for specific needs.
- **Insights Reporting:** Generate detailed reports to enhance efficiency.

## What benefits and ROI can users expect when evaluating Automox?

- **Time Efficiency:** Saves time by automating complex tasks.
- **Increased Security:** Enhances security through effective patch management.
- **Compliance:** Maintains cybersecurity compliance.
- **Network Visibility:** Provides comprehensive device network oversight.
- **Scalable Management:** Handles extensive network updates effectively.

In industry applications, Automox is widely used for managing and updating vast fleets of devices, particularly in sectors requiring stringent cybersecurity measures. It ensures seamless operations through its centralized automation and management capabilities, making it essential for organizations handling extensive IT networks.

# Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Out of all these features, if I had to pick one which I'm relying on the most, I would say the automatic patching, because it saves a lot of time and ensures all devices are updated.”



**Naqash Ahmed**

Senior Data Reporting Analyst at University of Bradford

- ✓ “Automox has positively impacted my organization with significant time-saving, improved our security posture by automatically patching vulnerabilities, and is easy to manage and deploy while offering Automox University as a great resource for learning the platform.”



**Dennis Mascot**

Data at Infosys

- ✓ “Automox has eased our operations; it is very simple to use and does not have heavy workflows.”



**Tushar Prasad**

Technical Product Manager at Hireright

- ✔ “Automox's real-time visibility and control through its intuitive dashboard is important for our response to emerging threats because it tells us which applications need to be updated on a real-time basis.”



**Robert Araya**

Network & Security Administrator at a legal firm with 51-200 employees

- ✔ “They've been adding some new features lately, which I'm not nearly as familiar with, but the ability to just deploy patches and exempt certain machines from certain patches is helpful. For instance, for our servers, we may not want to roll out zero-day patches. We are able to exempt those and make sure that they don't get those policies. We've got certain servers that have to run a particular version of Java, and being able to exempt those servers from receiving Java updates is pretty fantastic.”



**Verified user**

Senior Project Manager at a government with 51-200 employees

- ✔ “It's easy to deploy agents to endpoints.”



**Jack Leung**

EMEA Senior Systems Engineer at Quaker Chemical Corporation



“The fact that it's just one product that can patch multiple operating systems is really great.”



**Jeremy Loudon**

Director Of Business Operations at Ihloom Cybersecurity

### What users had to say about valuable features:

Its biggest strength is cloud-native simplicity. Unlike different SCCM tools, it has no distribution points, no complex infrastructure, no heavy VPN dependencies, and no large management servers. It has very strong patch automation, particularly in automated OS patching, third-party patching, policy-based rollout, patch scheduling, and vulnerability remediation. It offers cross-platform support from Windows to Mac OS to Linux.

**Tushar Prasad**

Technical Product Manager at Hireright

[Read full review](#)

“The flexibility in creating tools to make changes on remote machines is most valuable to me. The reporting feature is also fantastic because on any given day I can bring up a list of machines that don't have patches, for example. Or I can bring up a list of machines that are in my environment on a certain day. The solution helps me with not only my own role, and what I look for internally myself, but it also helps during audits. I can go in and look at the number of machines in there, and their owners and timelines. It certainly helps tell a story for anything that IT requires.

Being a cloud-native platform was one of the features and reasons we went with Automox. Having machines that are hosted in a particular facility is limited in a lot of cases to VPNs and subject to slowness and outages.

Automated patching has helped us to a great degree to know that patches will happen regardless of whether we jump in or not. And it's a positive feature..”

**Joseph Taylor**

IT Director at a healthcare company with 501-1,000 employees

[Read full review](#) 

“The best features Automox offers include automated patch management, ease of deployment, visibility, and reporting.

“The visibility and reporting features of Automox help me with great oversight of current patching status on our infrastructure.

“I would add that the ease of deployment across a large number of endpoints is commendable. Additionally, the user interface is very intuitive and user-friendly.

“Automox has positively impacted my organization with significant time-saving. Automated patching has saved countless hours on manual patching and updating endpoints, approximately three to four hours. It has also improved our security posture since automated patching has allowed vulnerabilities to be patched automatically. Automox is easy to manage and deploy and offers Automox University, which is a great resource to use for learning the platform..”

**Dennis Mascot**

Data at Infosys

[Read full review](#) 

“If I want to add more about my daily workflow, first of all, I would say it saves a lot of time. It reduces manual work for updates and patching. I don't have to go device by device myself because Automox does it automatically for me. It improves security as well, keeping the devices secure with the latest patches. It's much easier for me to monitor which devices need attention.

One of the best features I appreciate about Automox is automated patching. It automatically updates computers and servers without manual intervention. It supports many platforms. For example, in our organization, we use Windows, macOS, and Linux. The good thing is it supports all of them. I can patch laptops and servers of different types at the same place and at the same time. It's much easier to control because I can see all the devices in one online portal. No VPN or local server is needed. Automox helps me update applications like Chrome, Adobe, Java, and other third-party tools, not just operating systems. It's much easier to remotely control. It also shows me pre-built reports, giving me the ability to view and download reports to show management that the updates are complete.

Out of all these features, if I had to pick one which I'm relying on the most, I would say the automatic patching. The reason is because it saves a lot of time and ensures all devices are updated. I don't have to manually update each Windows, Mac, or Linux device; Automox does it automatically. It's very important because it keeps all devices secure and current. I can quickly see in the dashboard which devices were updated successfully and which ones need updating. Everything can be viewed in the dashboard, which stands out greatly to me and is my favorite feature.

Automox allows me to do custom automation beyond updates. For example, I can use it to update third-party applications and customize things in my dashboard. I can build my own report and see which devices and patch status I want to see on my dashboard based on each role. Different levels of access for team members require different types of access. The customization I can do in my dashboard means I can see and change the report style and design of my own choice. .”

**Naqash Ahmed**

Senior Data Reporting Analyst at University of Bradford

[Read full review](#) 

“The fact that it is pretty much hands-off is most valuable. Basically, you set up your policies and give it free rein, and it just does its thing.

They've been adding some new features lately, which I'm not nearly as familiar with, but the ability to just deploy patches and exempt certain machines from certain patches is helpful. For instance, for our servers, we may not want to roll out zero-day patches. We are able to exempt those and make sure that they don't get those policies. We've got certain servers that have to run a particular version of Java, and being able to exempt those servers from receiving Java updates is pretty fantastic.

Its patch management abilities are perfect. We've gone through probably five different solutions in the past 10 years. Automox is the only one that we've found that we can just set and then forget. It simply works. It is the best.

Its speed in carrying out functions is good. We've never experienced any performance issues. We've never noticed any delays. If we have to do a manual update, when we click update, within moments, we can tell that our computers are being updated. The actual UI is quick. Navigating between menus is seamless, and the actual communication between the console and the clients is seemingly instant as well. So, everything is as fast and quick as it can be.

It doesn't require much brainpower to navigate the UI and to figure out how to update. Building schedules and different groups is very intuitive. It is just a matter of a few checkboxes, and they've got great examples already in the software when you first get hold of it. Their support staff is fantastic in helping you get those configured if you do have any questions, but the likelihood of you needing that is pretty minimal. It is built to make sense.

It is very simple to set up policies using Automox. They've got several sample policies that are actually out there when you get access to the portal. The process is very simple. They've already got the samples out there, and it is so easy to duplicate them and modify them the way you want. It is just a matter of clicking a few checkboxes. It does not take much at all..”

“Among the most valuable features are its ease of use and the Worklets. Both of them are time-savers. Worklets enable us to customize things for a given environment. It's something like when Apple lets other people create applications. Other peoples' Worklets can be used in our environment and in our customers' environments. That saves a lot of time, and it's really cool.

It's also extremely important that the solution is a cloud-native platform because of the distribution of networks and where the things that are being patched are located. They're not all in one place, and neither are the people doing the patching. When you have people patching from different locations—and a lot of this is due to COVID, with people not being in the office—a cloud-native platform is what you need.

Automox also provides visibility for any laptop, desktop, or server in an environment, regardless of whether they are on-prem, in the cloud, or on the move. Visibility is key to security; you can't protect what you can't see. That's the biggest reason that the visibility it provides is important. There is also an ease-of-use aspect. No one has time to track down people and continually remind them that they have to patch. And you can't count on the security of an unpatched computer coming into your network, or on a situation where a person thinks they have patched it but it hasn't been patched. The ability to see what's on an endpoint before it connects to anything is key to the security picture.

In addition, the patch management it provides, from a single console, across Windows, macOS, and Linux endpoints is excellent because of the completeness of the platforms it supports and the things that get patched. WSUS only patches Windows, but nobody has just Windows. With Automox you can patch multiple platforms and multiple vendors' software in the same place. You don't have to patch using WSUS and then remember to manually patch anything with Adobe or Java. You can do it all from Automox. The cross-platform feature is extremely important. If I could just use WSUS and call it good, I would do that, but I can't.

The patching automation is also excellent. It makes things much easier, again, saving us time. There is also the level of confidence it creates, meaning that I'm

not wondering if everything got done.

And the speed of Automox speed in carrying out its functions is great. We haven't seen any problems in that area..”

**Verified user**

Owner at Saje Network Systems

[Read full review](#) 

# Other Solutions Considered

If you are looking for a solution that requires less infrastructure overhead and you have a strong remote workforce, then Automox will be the best tool for safeguarding your systems, as it provides patches on a need basis, safeguards the systems, and ensures the systems are protected from malicious intent, viruses, or any other threats.

**Tushar Prasad**

Technical Product Manager at Hireright

[Read full review](#) 

---

“We were using Qualys before and we're still using it, but we found Qualys to be a little bit lacking since it wasn't really eliminating all the vulnerabilities. We have been using it for years and it's almost as if we still have the same vulnerability count..”

**Robert Araya**

Network & Security Administrator at a legal firm with 51-200 employees

[Read full review](#) 

“We evaluated other options while choosing Automox. Some of the options we looked at were ManageEngine, Ivanti, and Microsoft Endpoint. We chose Automox because it was easier to use, cloud-based, and supports multiple platforms, which obviously saves us time and reduces manual errors..”

**Naqash Ahmed**

Senior Data Reporting Analyst at University of Bradford

[Read full review](#) 

---

“We were not evaluating other options when we chose Automox. My IT director gave me the task of trialing it and using it, and eventually, we purchased it.

“We did not perform any other evaluations..”

**Robert Araya**

Network & Security Administrator at a legal firm with 51-200 employees

[Read full review](#) 

---

“The team used to struggle a lot. We were using manual patching with some basic scripts to update devices, but that was not a good solution. We switched because manual updates were time-consuming and there were more chances of errors. We switched to Automox because it updates automatically across Windows, Mac, and Linux devices. The benefit of switching is it saves a lot of time, improves security, and gives us control and monitoring in more real-time..”

**Naqash Ahmed**

Senior Data Reporting Analyst at University of Bradford

[Read full review](#) 

“I previously used Microsoft 365 as a different solution.

“I switched from Microsoft 365 to Automox because we wanted a tool that would automatically patch our devices, thereby saving a lot of time and cost. It was also very cost-effective compared to Microsoft 365, which is why we made the switch. Automox also gave us the capability to automate patch deployment for operating systems and support third-party software to allow for consistent patching and quantifiable reduction in security vulnerabilities..”

**Dennis Mascot**

Data at Infosys

[Read full review](#) 

# ROI

Real user quotes about their ROI:

“We have seen a return on our investment with Automox, although it is difficult for me to quantify. I do know that our consultants who utilize the product have had a good response. Also, I know that, simply from a management perspective, it makes things super easy to accomplish..”

**Jeremy Loudon**

Director Of Business Operations at Ihloom Cybersecurity

[Read full review](#) 

---

“Automox saves time because it does the automatic updates and reduces manual work. Our team used to spend 10 hours per week just to update these things, and now we're doing it automatically. It's saving about 70% to 80% of time. The security has improved a lot. If I compare our issues to one and a half years ago, there used to be many more, and now it has gone very low. Another metric is that not many devices are left behind as we ensure all devices are up to date with the new patches and updates..”

**Naqash Ahmed**

Senior Data Reporting Analyst at University of Bradford

[Read full review](#) 

“While I cannot supply you with specific numbers, the savings in man-hours alone has been a great ROI on the use of Automox. On the flip side, as we are heavily involved in the security compliance sector, we have to take into account HIPAA, PCI, SOC and the like. We need an offering for auto-patching. Whether or not the customer actually opts for it, the ability to provide him with the option at least gets us in the arena to bid on the deal. If we didn't have that as an offering, then we would have lost a lot more deals over the years..”

**Verified user**

Vice President at Atlantic.Net, Inc.

[Read full review](#) 

---

“I have seen a return on investment since we save a lot of hours for management. We are able to focus on critical areas and devote our work time to the areas that need more of our attention. It has also been a great tool because we are able to reduce both manual labor and operational expenses by automating patching of roughly 200 Windows servers. Automox being a cloud-native platform has removed our need for on-premises patching infrastructure, saving expenses and overhead for management, improved visibility, and consolidated control of our endpoints, thus reinforcing our ability to quickly respond to vulnerabilities..”

**Dennis Mascot**

Data at Infosys

[Read full review](#) 

“We have seen ROI. The cost isn't really an issue because our clients bear the cost of that. They pay for it. We have seen the benefit in process improvement, streamlining our operations, and peace of mind, e.g., being able to pull up a console and see how many systems are not compliant.

Previously, we would run a report, scan it, and compare it. We were spending 15 to 30 minutes a month on each machine on this stuff because you would find stuff that wasn't up to date, then you had to fix it. This solution takes that time down to minutes. Automox saves us easily many hours a month..”

**Verified user**

President / CEO at B/Net Systems

[Read full review](#) 

---

“We have seen a return on our investment. Number one, fewer man hours are spent trying to understand how to roll out patches. Number two is reporting. You can go inside Automox and get reports to see exactly what you have.

The visibility, far beyond patching, allows us to see which machines have what sort of software installed, or which users are using old hardware. The old hardware is all available inside so you can go in and say, "Show me everybody who's using this particular model of a laptop, which is four to five years old." You can plan to reach out to these people in good time and get them swapped out with newer hardware. So the list of things is endless. It's just really up to the user to be creative in how they use it..”

**JosephTaylor**

IT Director at a healthcare company with 501-1,000 employees

[Read full review](#) 

# Use Case

“We use it to patch distributed networks for offices that have different locations, such as home users and the like. Especially with COVID, people are working from home and computers are not all on-premises. We have customers that have over 1,000 nodes..”

**Verified user**

Owner at Saje Network Systems

[Read full review](#) 

---

“We are a municipality, so we are not a traditional business. We've got it deployed throughout the city. We've got it on roughly 120 servers. We've also got about 1,400 other endpoints. So, there are roughly 1,300 computers, and those computers are also police vehicles, EMS vehicles, and fire vehicles. We are continuously monitoring them and patching them to make sure that they stay up to date and meet all the criteria for compliance. Obviously, EMS has to worry about HIPAA, and police have to worry about CJIS. So essentially, we're making sure that we stay within the guidelines of compliance.

It is web-based, so we are using the version that they're currently on..”

**Verified user**

Senior Project Manager at a government with 51-200 employees

[Read full review](#) 

“I mainly use Automox to manage updates and automate tasks on company devices. In my day-to-day uses, I primarily use it for updating devices and reviewing patch management. I focus on keeping Windows and macOS devices up to date manually. Another daily example is using Automox to automatically check for devices that need updating, such as installing security patches without manual intervention. Every morning, I check Automox and it shows which device got updated overnight, and I review and approve anything that is pending..”

**Naqash Ahmed**

Senior Data Reporting Analyst at University of Bradford

[Read full review](#) 

---

“My main use case for Automox is automated patch management for our whole organization, managing and patching our endpoints. Automox has helped us reduce security vulnerabilities with automated patching being deployed with minimal manual intervention. This has helped us reduce the number of vulnerabilities that are susceptible for an attacker to exploit. Automox has also been easy to deploy with a large scope of endpoints across many operating companies in our organization.

“A specific example of how Automox helped me with automated patch management is that it was easy to create and configure policies and schedule patching that is done automatically..”

**Dennis Mascot**

Data at Infosys

[Read full review](#) 

“We use Automox to maintain the software on all our computers. We were using Qualys before and we're still using it, but we found Qualys to be a little bit lacking since it wasn't really eliminating all the vulnerabilities. We have been using it for years and it's almost as if we still have the same vulnerability count. We wanted to try something new with Automox in that most of the vulnerabilities are taken care of just by updating the applications that we use on our computers.

“We have not used Automox's scripting capabilities for automating routine tasks such as software deployment and configuration changes yet, but we're probably not going to see a massive need for that since we don't have many in-house applications or a development team..”

**Robert Araya**

[Read full review](#) 

Network & Security Administrator at a legal firm with 51-200 employees

---

Automox is used in our system primarily to manage patch management. It helps in managing Windows updates, third-party application updates, browser patching, and security updates across employee laptops, verification teams, recruiters, operational staff, and our distributed workforce.

Since we have a remote culture, Automox helps in policy enforcement, software deployment, scripting, and remediation without requiring VPN connectivity or corporate LAN presence. It also handles third-party application patching, such as Chrome, Zoom, Adobe, Java, and Slack, ensuring that all these tools are properly patched. It provides patch compliance visibility, endpoint reporting, and vulnerability reporting, which helps during audits, customer security reviews, and SOC 2 compliance assessments.

“Automox has helped us in automated patch management, specifically for Windows patches, third-party software patching, and remote endpoint remediation. Since we follow a remote culture, it is very important that our systems are safe. Automox has been a good tool and helps us in managing all those security capabilities. .”

**Tushar Prasad**

Technical Product Manager at Hireright

[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.

“The initial setup was not complex at all, but I understand it could get complex depending on what you want to do, and we're still at the stages where I need to be able to do that..”

**Robert Araya**

[Read full review](#) 

Network & Security Administrator at a legal firm with 51-200 employees

---

“My experience with pricing, setup cost, and licensing was good. Pricing was very straightforward through a subscription process via AWS Marketplace. We pay clear monthly and yearly fees, so billing is simple. The setup cost was minimal because it's SaaS, so there was no hardware to buy. Licensing was also flexible per device licensing..”

**Naqash Ahmed**

[Read full review](#) 

Senior Data Reporting Analyst at University of Bradford

---

“We just need to deploy the agent to the endpoints. We don't need to set up anything. For a single agent, it takes one or two minutes. However, we deployed globally, and you need to take into consideration the time it will take to deploy across each endpoint. It's very simple to deploy.

We had three or four engineers take care of the implementation. .”

**Jack Leung**

[Read full review](#) 

EMEA Senior Systems Engineer at Quaker Chemical Corporation

---

“The initial setup is straightforward.

I walked through it with one of our customers that has 1,200 or 1,500 endpoints, and I was extremely impressed with the Automox customer success team. They were great on the calls that we had and how they walked through things. We were scheduled for four or five calls but when we got to the end of the third call, the customer said, "You know what? We're good. This was so easy. We're all set up and rocking and rolling." We didn't have to do the rest of the calls. That almost never happens in our world and was really great.

Setting up of policies is really easy.

For that client I just mentioned, they had it rolled out in eight to 10 hours, and that was a fairly large deployment. I know that they were very surprised at how fast it went. When we set up Automox for ourselves, internally, it took less than an hour because we only have about 20 nodes..”

**Verified user**

[Read full review](#) 

Owner at Saje Network Systems

---

“It takes a little bit of time to ramp up and understand how the Automox tool works and how effective it can be. So once you put a few days of moving through the system and understanding it, the solution becomes very easy to use.

The solution setup is straightforward. We have some intelligent people who were involved in the patching process, who understand Active Directory, who understand the patching process and understand internally our users and how they work. All along the way, AutoMox was excellent in providing us with all the help and resources we needed to understand how to do stuff. They were there for our questions and suggestions as we hit roadblocks, and to try and figure out different ways of doing things. They were instrumental in getting us up and running very quickly.

I think it took us two or three weeks to get comfortable with how we had set it up and to start not only pushing out the first patches, but also to try and run different software packages and do different things with it. We didn't exclusively dedicate time to AutoMox. We jumped in and out for a period of two weeks while emailing support at AutoMox on maybe one or two questions. We were up and running very, very quickly. Being a small company, we realized that we needed a product that would do the work. Our implementation was essentially just to look at what we had existing in our patch rollout tool prior to AutoMox, and to get AutoMox side-by-side with this tool and copy over dates, times, groups. This way we could get the patches rolled out whilst at the same time, we're looking at our software management tool. The team had no trouble setting up policies with Automox..”

**Joseph Taylor**

[Read full review](#) 

IT Director at a healthcare company with 501-1,000 employees

---



“I could have slept through it. It was very simple. It took minutes when we first set it up. The console was already configured. We installed a couple of agents, and within minutes, they showed me how to use it. There were very few questions after that. They give you kind of a rundown of standard practice about how they recommend setting up servers versus just traditional clients. It was painless and very easy. It was the least time-consuming thing I've ever done.

Deployment took a long time just from our side because we had other things going on. It took no time at all in terms of Automox giving us full reigns over the software. The day after signing the contract, we were on the phone with their engineers. We already had the environment set up, and everything was kosher. So, it took just a day. They had offered to help us with the deployment to all of our clients, but we just politely declined because we knew we wouldn't be able to focus on it.

In terms of the implementation strategy, because we are a government organization and we have a lot of projects going on, our main focus was ensuring that our whole critical infrastructure has the clients so that we can make sure all critical systems are getting patched and are up to date. So, our main focus was getting our servers updated to the front line, and then from there, we started updating all the core infrastructure that is actually attached to our network. We have a lot of satellite sites and places like landfills and water reclamation that aren't directly connected to us. They're just connected via VPN. So, our main focus was getting all of our core infrastructure updated, which was a pretty quick process.

We made use of Automox's free trial before deciding to go with it. It was very important in our decision to go with Automox. Being able to put your hands on it and actually use it in a live environment has a huge benefit. During our trial, we probably got about a hundred devices on it and made sure it worked. We were able to show it off to the other folks in IT and let them drive in it for a little bit to see if they saw any big red flags as to why we shouldn't purchase it. Once we made sure everybody was on board, we pulled the trigger, but it was a great experience. The free trial was very important.

For deployment, we had three people involved, but they really weren't required. We had our two network admins and me. Essentially, that was just so that we could get familiarity with the product and how it worked, and then from there, we began deploying the clients automatically, and they automatically enroll in Automox. So, when you're doing the install, you have silent install options that allow you to put them in groups and assign them to different policies and things of that nature. So, literally, you can do it hands-off and never even touch it. It doesn't require any maintenance..”

**Verified user**

[Read full review](#) 

Senior Project Manager at a government with 51-200 employees

# Customer Service and Support

“We have had no complaints about the technical support. We've used it twice in almost four years now and have had no issues, and no complaints from our side. It's been great..”

**Verified user**

Vice President at Atlantic.Net, Inc.

[Read full review](#) 

---

“I have not talked to their technical support personally, but I always hear from my customers if something's not right, and I have not heard from them about Automox's support..”

**Verified user**

Owner at Saje Network Systems

[Read full review](#) 

---

“Customer support is usually good. Whenever we have something to ask or requirements we need, we can send them emails and they are very helpful. For example, we had an issue and the team responded within a few hours. They're very knowledgeable and have given us many channels for support, including email, chat, and documentation..”

**Naqash Ahmed**

Senior Data Reporting Analyst at University of Bradford

[Read full review](#) 

“I would rate Automox's customer service and technical support as excellent. They are really good because they don't take five days to get back to me; they respond within 24 hours with really good information. The initial reply is great, providing advanced information if I want to handle it on my own, or I can just wait for the tech to interact with me..”

**Robert Araya**

Network & Security Administrator at a legal firm with 51-200 employees

[Read full review](#) 

---

“Automox's technical support for their product is very good. They're responsive, they're knowledgeable and they help out when needed. I have encountered no issues in which a support case has dragged on or where concerns have been brushed off. The technical support always answers things directly and quickly..”

**Jeremy Loudon**

Director Of Business Operations at Ihloom Cybersecurity

[Read full review](#) 

“I would rate Automox technical support as really excellent. There were times when we needed them. We haven't always gotten the answer back immediately because they've misunderstood what we said or something has happened. Yet the quality of the people answering our questions, and the attentiveness to our business, is way beyond what we get with comparable tools and products from much bigger companies. We're really, really happy with the support we get from Automox..”

**JosephTaylor**

IT Director at a healthcare company with 501-1,000 employees

[Read full review](#) 

## Other Advice

“My advice for others looking into using Automox is that it is well-suited for centralized patch management within a remote or distributed environment because it is cloud-native. However, it is not suitable for legacy or overly customized systems that need unusual update processing. I would rate this product a 9 out of 10..”

**Dennis Mascot**

Data at Infosys

[Read full review](#) 

---

“I would tell others to identify your needs, whatever you're looking for. If you want to save your time, take advantage of automation, go for Automox. If you want to start small and scale later on, Automox is good. If you want nice reports and want to leverage your support across all your devices at the same time, go for Automox. I would rate this product an 8 overall..”

**Naqash Ahmed**

Senior Data Reporting Analyst at University of Bradford

[Read full review](#) 

“I am a strong proponent of Automox. It's a huge time-saver, it's accurate, it's easier to use, and it's way more stable than any endpoint security add-on. I don't know every product out there, but I have not heard of any other solutions that are just as good or better.

We have two customers with over 1,000 nodes, and one of them, after using Automox for a year, did a three-year renewal. I have heard nothing negative from the other one and I can promise you I would hear if they weren't happy..”

**Verified user**

Owner at Saje Network Systems

[Read full review](#) 

---

“This is a cloud-based version that updates by itself automatically.

I'd recommend the solution to others.

I would rate the solution seven out of ten overall.

It's good for endpoints. However, it's not as good on the server end. There is overhead for you when you deploy on the server. .”

**Jack Leung**

EMEA Senior Systems Engineer at Quaker Chemical Corporation

[Read full review](#) 

---

“Since switching over from Qualys, we have seen no positive impacts for our organization other than being able to update the applications on an endpoint.

“We haven't used Automox's reporting capabilities.

“My experience with the pricing and licensing for Automox is good, and I think we got a pretty good deal. On a scale of 1 to 10 for how pricey Automox is, I would place it at a six.

“Overall, I would rate Automox as 10 out of 10.

“We are just clients of Automox, not partners or resellers..”

**Robert Araya**

Network & Security Administrator at a legal firm with 51-200 employees

---

[Read full review](#) 

Our company purchased Automox last year only.

Automox has eased our operations. It is very simple to use and does not have heavy workflows. The security teams regularly use it. It has a triangle-like icon which ensures that the system is patched and proof.

“Since we have a remote workforce, Automox provides VPN-less patching. We have distributed operations, so it provides cloud-native management. It provides different kinds of patch automation and helps us in reducing infrastructure overhead. It is suitable for cross-platforms including Windows, Mac OS, and Linux, and it is easier than any other SCCM solution.

“Automox is a strong tool for managing the remote workforce. It ensures that our systems are not vulnerable and issue-proof, with all systems properly patched on a timely basis without needing VPN connectivity.

“Automox is used in a centralized cloud-native approach across our globally distributed employee devices.

“I believe Automox is moving in the right direction. If it can contain the cost, I think its demand will rise and it will consolidate a major market share.

“I gave this product a rating of eight out of ten. .”

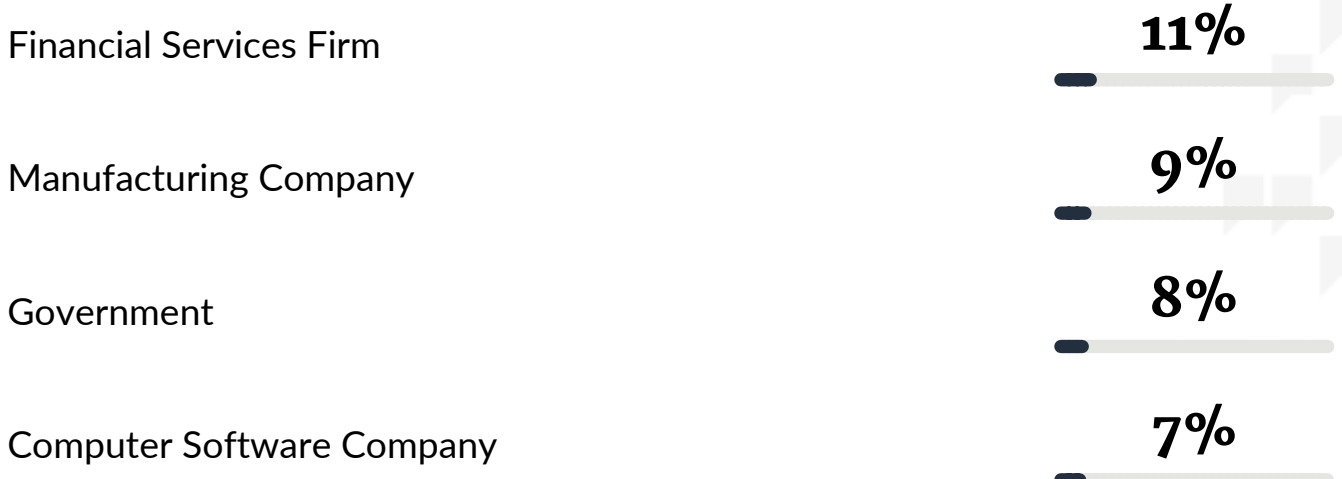
**Tushar Prasad**

Technical Product Manager at Hireright

[Read full review](#) 

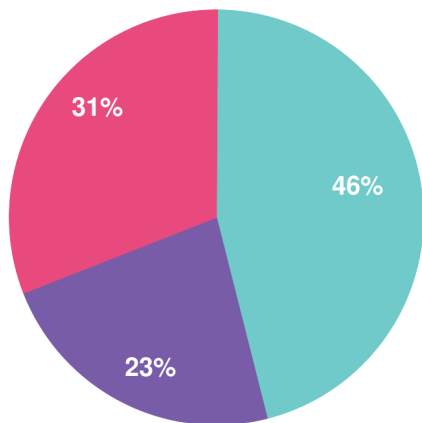
# Top Industries

by visitors reading reviews

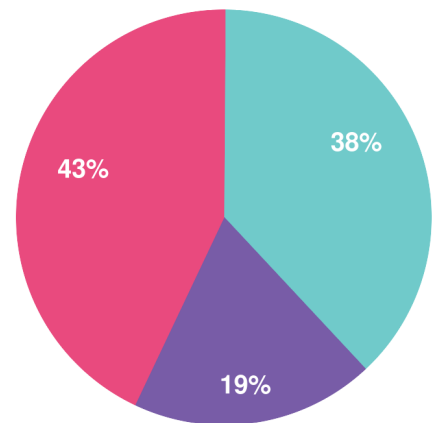


# Company Size

by reviewers



by visitors reading reviews



Large Enterprise      Midsize 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](http://www.peerspot.com)

## PeerSpot

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

[reports@peerspot.com](mailto:reports@peerspot.com)

+1 646.328.1944