



Ping Identity Platform

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 9

Other Solutions Considered..... 10 - 13

ROI..... 14

Use Case..... 15 - 18

Setup..... 19 - 22

Customer Service and Support..... 23 - 25

Other Advice..... 26 - 29

Trends..... 30 - 31

About PeerSpot..... 32 - 33

Product Recap



Ping Identity Platform

Ping Identity Platform Recap

IDENTITY DEFINED SECURITY PLATFORM delivers a unified, standards-based platform that can be deployed as SaaS, software or both and can scale to handle millions of identities. From multi-factor authentication and single sign-on to access security, directory and data governance, our capabilities work together to give employees, partners and customers secure access to cloud, mobile and enterprise applications, securing and streamlined everything from sign-on to sign-off and everywhere in between.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“I would recommend PingFederate as an IAM solution for its no-code environment, single sign-on, multi-factor authentication, bidirectional services, and advanced features.”



Shruthi R Varikoti

Senior ServiceNow Developer at Wells Fargo



“It's convenient for users to log in through Ping using the Kerberos adapter because it doesn't require them to authenticate again.”



Faiz Mohd

Sr. IAM Engineer at Southwest Airlines



“From a security perspective, I highly value the product's biometric authentication methods such as FIDO, FaceID, YubiKey, and the mobile app.”



Verified user

Sr IAM Consultant at a healthcare company with 10,001+ employees



“I like PingFederate.”



MAHESHKUMAR7

Cyber Security Engineer at TECHMINDZ DIGITAL CONSULTING PRIVATE LIMITED



“I work on the application onboarding process because we have multiple customers and get data from different sources.”



SandeepKumar30

Senior IAM Platform Enigeer at Loblaw Companies Limited



“It is a scalable solution.”



Dilip Reddy

Ping Engineer at Equitable



“It offers robust features and customization options that justify the cost.”



Lakshmi Kanth Muthyala

IAM lead at Tata Consultancy

What users had to say about valuable features:

“From a security perspective, I highly value the product's biometric authentication methods such as FIDO, FaceID, YubiKey, and the mobile app. These methods provide a higher security level than email authentication, which can be compromised if the email is breached..”

Verified user

Sr IAM Consultant at a healthcare company with 10,001+ employees

[Read full review](#) 

“The platform's most valuable feature is its identity management capabilities. It allows us to integrate multiple identity providers (IDPs) seamlessly and manage access policies effectively. Performance-wise, it has been quite reliable compared to other tools..”

Lakshmi Kanth Muthyala


IAM lead at Tata Consultancy

[Read full review](#) 

I appreciate that the Ping Identity Platform does not require coding and offers flexible integrations and federated identity management. Generative AI helps to automate access review and streamline governance workflows. The platform enhances security measures by analyzing multi-factor authentication attempts, highlighting suspicious patterns, and generating compliance reports.

Shruthi R Varikoti

Senior ServiceNow Developer at Wells Fargo

[Read full review](#) 

“Centralizing the management of authentication and authorization policies simplifies administration. Organizations can enforce consistent security policies across all applications, improving overall security posture and compliance with regulatory requirements. PingFederate can adapt authentication requirements based on risk factors such as user behavior, location, and device..”

SandeepKumar30

Senior IAM Platform Enigeer at Loblaw Companies Limited

[Read full review](#) 

“The most valuable feature of the solution is the role-based access control. We use role-based access control in our project while onboarding applications. I get to understand how the user provisioning is done and the roles currently available in the system, and we will integrate them with SailPoint IIQ and make those roles requestable. Once the user requests the roles, we can follow the workflow, and SailPoint IIQ will provide the user with the ability to request the roles in Active Directory. While using SSO, we will read the roles and pass them to the application..”

Dilip Reddy

Ping Engineer at Equitable

[Read full review](#) 

“It's convenient for users to log in through Ping using the Kerberos adapter because it doesn't require them to authenticate again. If a user is already logged into the organization's domain, the system automatically checks the Kerberos ticket in the background when they try to access another application through Ping. It logs them in without prompting for a password or reauthorization.

You don't need prior experience to use this; you need to understand how it works. Experience is only necessary when integrating it with systems. For instance, when using any application through Ping in your organization, it just needs to be connected to the organization's domain. This setup works seamlessly on a PC, automatically detecting the Kerberos ticket and logging you in. However, it won't work on a mobile device since the mobile doesn't have a Kerberos ticket. On a mobile phone, you'll be prompted to authenticate again..”

Faiz Mohd

Sr. IAM Engineer at Southwest Airlines

[Read full review](#) 

Other Solutions Considered

“We also recommend ForgeRock. It is used for access management. It doesn’t have many configurations but allows customizations. We can achieve a lot of things using customizations. Wherever PingID is not suitable for the customer, we ask them to choose ForgeRock so that we can customize it as per the requirements and deliver the solution..”

Verified user

[Read full review](#) 

Lead IAM manager at a tech services company with 11-50 employees

“I have evaluated other solutions in the past, but I found this platform to be the most comprehensive regarding security, scalability, and ease of integration. Its strong support for various authentication protocols like OAuth, SAML, and MFA, along with its robust disaster recovery capabilities and adaptive clustering model, made it the ideal choice for our organization's needs..”

Verified user

[Read full review](#) 


Sr IAM Consultant at a healthcare company with 10,001+ employees

“My company started to use Ping Identity Platform since it is quite robust, easy to use, user-friendly and provides a lot of features with its own directory, access management tool, and identity management tool.

I would choose Ping Identity Platform over the other platforms in the market..”

Priyanshu Sharma

Ping Identity Engineer at CYBERSOLVE


[Read full review](#) 

“Based on the environments, I would say that I used to work in two environments, like development and production. PingFederat is a standard tool. The product has four nodes, out of which, one node is both admin and engine. The remaining engine nodes, we use direct cluster, like, Ping in front of the proxy and external LBs on the top of it.

There are some issues with the tool's stability, such as where improvements are required..”

Dilip Reddy

Ping Engineer at Equitable

[Read full review](#) 

“you can make an informed decision about whether PingFederate or another IAM solution is the best fit for your organization's needs. Each solution has its strengths and potential drawbacks, so aligning the choice with your specific requirements and environment is key to a successful implementation. Some other popular IAM solutions you might evaluate Like Okta, AzureAd , IBM Security and forgerock..”

SandeepKumar30

Senior IAM Platform Enigeer at Loblaw Companies Limited

[Read full review](#) 

“ I have around eight years of experience in total IT and six years of experience in the Identity and Access Management domain. I've worked with different identity and access tools, such as PingFederate, PingDirectory, PingOne, Oracle Identity and Access Manager, ForgeRock, SailPoint, and CyberArk. I have more experience with US clients, and my last organization was Ping Identity.

At my previous company, I implemented a CDP identity portal with a Python DevOps model. We worked with four types of customers: CPB, QRadar, DUP, and DIRAS. We used PingFederate as an Access Manager and Federation Server to enable user authentication, single sign-on operations, and multi-factor authentication (MFA). It operated as an identity federation and provided secure access to authorized resources.

We also used PingDirectory as a structured repository for customer, partner, and external employee identity data to build unified user profiles. Apart from that, I've worked with Python and Shell scripting for about three years, enabling automation in Azure and AWS cloud environments..”

SandeepKumar30

Senior IAM Platform Enigeer at Loblaw Companies Limited

[Read full review](#) 

ROI

Real user quotes about their ROI:

“The product generates a return on investment especially for organizations prioritizing on-premises control and security. It offers robust features and customization options that justify the cost..”

Lakshmi Kanth Muthyala

IAM lead at Tata Consultancy

[Read full review](#) 

“I see an ROI. It's not a revenue generator. So it's purely from a cost perspective, but on the other hand, because we protect so much of our data now through multi-factor, I don't know the statistics of how many times we've been hacked or passwords were stolen. But because we have done that, we've probably saved ourselves a lot of money in reputational damage in breach recovering from breaches.

.”

Verified user

Senior Staff Technical Program Manager at a manufacturing company with 10,001+ employees

[Read full review](#) 

Use Case

“Managing customer identities and providing a secure and seamless login experience for consumer-facing applications. Protecting APIs from unauthorized access and ensuring secure communication between services..”

SandeepKumar30

Senior IAM Platform Engineer at Loblaw Companies Limited

[Read full review](#) 

“I usually deploy single sign-on and multi-factor authentication using PingOne for customer-facing applications to enhance security and user convenience. I use PingFederate to integrate with Kerberos-based systems, such as Salesforce, AWS, ServiceNow, and Google. I configure various OAuth grant types and set up Windows Service Federation and SAML 2.0 protocol service provider endpoints using PingOne and PingFederate..”


Faiz Mohd

Sr. IAM Engineer at Southwest Airlines

[Read full review](#) 

“I primarily use the platform for OAuth and SAML-enabled applications, especially third-party and SaaS applications. I utilize the SAML protocol for those that support SAML, while for OAuth-supporting applications, I use OAuth, OIDC, and OpenID tokens. Additionally, for server-to-server communication, I employ the client credentials grant. For mobile-based native applications that require refresh tokens, I utilize those as well. I manage OAuth client ID registrations for certain SaaS applications and implement various authorization flows, such as Kerberos authentication for intranet requests and form-based authentication for external network requests. Furthermore, I have integrated Multi-Factor Authentication (MFA) to enhance the security of critical applications..”


Verified user

[Read full review](#) 

Sr IAM Consultant at a healthcare company with 10,001+ employees

I work with Governance, Risk, and Compliance (GRC), IT Service Management (ITSM), and Customer Service Management (CSM) modules of ServiceNow. My project is related to cybersecurity. I have touched on generative AI and integrations like SOAP APIs. I have used the Ping Identity Platform for seamless Single Sign-On (SSO) in enterprises, offering flexible integrations and federated identity management within a mid-sized enterprise environment.

Shruthi R Varikoti

[Read full review](#) 

Senior ServiceNow Developer at Wells Fargo

“I have around ten years of experience with IAM tools, and I have been working mostly on access management for the last few projects. My overall experience, considering that I have worked with various access management tools, like PingFederate and Okta. In terms of identity management, I have worked with IDM and SailPoint. In terms of privileged access management, I want to work closely with CyberArk to provide the service account and administer it to the vault. I also understand the concept of PSM and password rotation. Integrating CyberArk with Ping, you get both RADIUS and SAML. Coming to my roles and responsibilities, in my current project for new application onboarding and access assigned to the IAM team who are assigned service tickets. We pick up those tickets and assign them to us, and then we communicate with the application owners..”

Dilip Reddy

Ping Engineer at Equitable

[Read full review](#) 

“I am into cybersecurity IAM and have excellent experience with Ping Identity, especially. I work on implementing SSO using Ping Identity with application support protocols such as SAML 2.0 and OAuth/OIDC connections in production and non-production environments.

I validate applications and functionalities on PingFederate and PingAccess, provide 24/7 support on prod/non-prod environments, troubleshoot issues, renew certificates, gather requirements, implement changes, and integrate new applications into Ping.

I also provide authentication and authorization services to applications. I have been working with the operations team and, for the last six months, have upgraded to the engineering team. I create policies, adapters, and selectors for clients..”

MAHESHKUMAR7

Cyber Security Engineer at TECHMINDZ DIGITAL CONSULTING PRIVATE LIMITED

[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 of PingFederate in a cloud environment using Generative AI took around one to two weeks. Once everything is set, it does not require much maintenance.

Shruthi R Varikoti

Senior ServiceNow Developer at Wells Fargo

[Read full review](#) 

“The product deployment can be complex, especially when migrating from on-premises to cloud environments like AWS. It involves reconfiguring settings and ensuring minimal downtime, which requires careful coordination..”

Lakshmi Kanth Muthyala

IAM lead at Tata Consultancy


[Read full review](#) 

“For PingFederate implementation, we have different options. We can have an on-premise implementation, meaning we install it on our own procured servers. Alternatively, we can use the cloud version of PingFederate.

The initial setup itself isn't overly complex. With the cloud version, it's primarily deploying WAR files.

While the full implementation takes time due to development and testing, the core installation process is relatively straightforward..”

Satish Shekhar Singh


[Read full review](#) 

IAM technical architect at Emprest Innovations Private Ltd

“The setup is generally straightforward, but it can depend on the environment. For example, in a previous organization, two companies merged, each with its own Active Directory and identity management instances. I had to build a new environment to match both the SSO-enabled applications. Although the process was straightforward, it depended highly on the organization’s architecture and requirements.

The deployment timeline depends on the availability of the application team. I aim to make SSO seamless between environments, avoiding multiple authentication logins for end users. Typically, the implementation takes about a month, considering network ACLs and other configurations. However, migrating applications can be challenging and may take months. My last project took almost one and a half to two years to complete the migration process..”

Verified user

[Read full review](#) 

Sr IAM Consultant at a healthcare company with 10,001+ employees

“Sometimes we need to configure PingFederate as an OAuth authorization server and OpenID Connect policy. We also configure SAML 2.0, register web applications and different applications, on-premises applications, and any cloud applications that integrate with PingFederate.

Sometimes we create data store connectors, password credential validators, and adapters to enable authentication, and we work with proxy servers. That kind of implementation with PingFederate.

Project-Specific Setup:

The complexity of the setup depends on the requirements of the project. Some architect teams and different customers have specific needs. If you want to deploy Ping on-premises, the team will handle that. We use the Ping Identity Portal and follow the core documents to integrate with any application.

We also create SOPs to enable authentication for different applications. We create high-level and low-level design documents and perform daily support activities for the PingFederate server..”

SandeepKumar30

Senior IAM Platform Enigeer at Loblaw Companies Limited

[Read full review](#) 

“The initial setup is difficult.

Integration process with the existing system:

Before creating user access, we first need to ensure the third-party application supports SSO protocols like SAML, ROA, or OpenID Connect. We gather necessary metadata files from the configuration information required by the PingFederate. Then, we select the application type based on the capabilities and requirements of the third-party application. Ping Identity Platform options may include SAML SP or Ping, OpenID Connect, and reliant party.

Next, we configure application settings, providing basic information such as the application name and description, along with relevant details.

Input the necessary URL, endpoint, and metadata provided by the third-party application. Configure authentication settings, including the signing certificates and encryption method. Then, proceed to attribute mapping, where we map attributes between PingFederate and the third-party application. This ensures user information is correctly extended during the SSO transaction. Define which attributes should be sent out and issued by the application.

Next, we define access policies to control which users or groups can access the third-party application, configuring authorization rules and permissions as needed. Use PingFederate's testing tools to ensure the SSO integration is functioning correctly, testing authentication, attribute mapping, and any other relevant features. Once the Ping integration is successful, deploy the configuration to make it live. Ensure any necessary firewall rules or network configurations are in place to allow communication between Ping and the third-party application..”

MAHESHKUMAR7

[Read full review](#) 

Cyber Security Engineer at TECHMINDZ DIGITAL CONSULTING PRIVATE LIMITED

Customer Service and Support

“The customer support team is quite responsive and knowledgeable. Whenever I encounter any issues or require assistance, they quickly provide solutions..”

Verified user

Sr IAM Consultant at a healthcare company with 10,001+ employees

[Read full review](#) 

In Ping, I have reached out to technical support for troubleshooting SAML certificate mismatches and federated errors between Ping and enterprise apps. They have helped support incident resolution for authentication failures using ServiceNow incident workflows and Generative AI summary.

Shruthi R Varikoti

Senior ServiceNow Developer at Wells Fargo

[Read full review](#) 

“They provide good technical support, but resource availability can be limited compared to larger providers like Azure AD. The self-help resources are useful, but response times for complex issues could be faster..”

Lakshmi Kanth Muthyala

IAM lead at Tata Consultancy

[Read full review](#) 

“If some access is denied to some users, then they can contact the support team for help you can help them fix everything. At times, users are not able to access the applications, but with features like SSO, we can have a single set of credentials. We can access and get a set of login credentials to access the application..”

Dilip Reddy

Ping Engineer at Equitable

[Read full review](#) 

“We have six to eight members who provide operational support for Ping Identity products. They perform day-to-day operational support, including root cause analysis, Ping server installation, server maintenance, troubleshooting data sources, and any issues related to stopping processes.

We create standard operating procedures for them to follow. If there's a high-priority incident that cannot be resolved by our SOPPO, CTP, IDaaS, and other support teams, we escalate the issue to the Ping Identity vendor team. We set up meetings to discuss the issue and find a solution.

I am also part of the support team as a senior consultant. Considering our daily activities and customer identity issue resolution, I would rate the operational support for Ping products at six to seven out of ten..”

SandeepKumar30

Senior IAM Platform Enigneer at Loblaw Companies Limited

[Read full review](#) 

“A lot of teams work with technical support, but I work with it for user issues only. You might need support with things like application swaps, application names, and application URLs.

I didn't know where to find those in Ping Identity, so I contacted technical support for those issues.

The support team is very clever and active. They provide end-to-end support once an issue is created. I have worked with most of the support team.

I also work with the support team because I work with the operations team. I provide 24/7 support to production and non-production environments.

I coordinate with application and network teams to troubleshoot critical tickets and issues related to Ping Identity solutions..”

MAHESHKUMAR7

Cyber Security Engineer at TECHMINDZ DIGITAL CONSULTING PRIVATE LIMITED

[Read full review](#) 

Other Advice

I would recommend PingFederate as an [IAM](#) solution for its no-code environment, single sign-on, multi-factor authentication, bidirectional services, and advanced features. On a scale of one to ten, I would rate the Ping Identity Platform as ten out of ten.

Shruthi R Varikoti

Senior ServiceNow Developer at Wells Fargo

[Read full review](#) 

“The tool is easy to use.

I would recommend the tool to others.

Ping Identity Platform can help identify and verify users. It is a really good platform to identify users, and give access to them.

I rate the tool a seven out of ten..”

Dilip Reddy

Ping Engineer at Equitable

[Read full review](#) 

“I haven't faced any debugging issues. It was only during the testing that I faced.

I advise you to be extremely careful when integrating Ping with any application, especially during authentication. If an intruder manages to get authorized, they're just one step away from accessing all your organization's data. With PingFederate, users only need to log in once, so if an attacker gains access, it becomes tough to

track and stop them. The critical takeaway is to be vigilant during integration and ensure that every security measure is thoroughly implemented.

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

Faiz Mohd

Sr. IAM Engineer at Southwest Airlines

[Read full review](#) 

“Ensure that the implementation of PingFederate aligns with your overall business goals and IT strategy. Identify key objectives such as improving security, enhancing user experience, or achieving regulatory compliance, and use these to guide the implementation process.

AI trends:

We have not used AI. We rely on shell scripting for automation processes, and there is no built-in AI in Ping products. We perform automation tasks through scripting and integrate various services, but no AI is involved.

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

SandeepKumar30

Senior IAM Platform Enigneer at Loblaw Companies Limited

[Read full review](#) 

“Overall, I would rate it a seven out of ten. Ping Identity is a multinational company, and many MNCs and small-scale industries approach them to implement SSO or MFA. Basic information like data users and data centers are all in the Ping Gateway.

I would recommend it to others. I love Ping Identity products. We use PingFederate, PingAccess, PingOne, and PingID for authentication and authorization. I use PingID on my mobile phone for MFA. It safely and securely accesses my applications without any interruption.

PingID and PingOne are used for authentication and authorization. When MFA is used, you're using PingID on your mobile phone. But PingOne securely accesses my applications without interruption. Within a fraction of a second, I can log in and access any application.

Ping Identity products like PingFederate are safe. They help cybersecurity teams prevent ransomware, any interruption data theft, and money theft for banking products. They offer 24/7 support and monitoring. Ping Identity products are 100% safe and secure..”

MAHESHKUMAR7

Cyber Security Engineer at TECHMINDZ DIGITAL CONSULTING PRIVATE LIMITED

[Read full review](#) 

“I use Ping Identity Platform as the Multi-Factor Authentication solution. Once the first level of authentication is completed with a user ID, password, or card authentication, the request is directed to PingID. I have configured profiles that allow the use of devices like the mobile Ping app. I also use email in some scenarios, although I prefer FIDO authentication methods like YubiKey or FaceID for enhanced security.

I have integrated the platform into all environments using an adaptive clustering model that operates in an active-active configuration. Two regions are active-active, while the third serves as a passive disaster recovery region. When integrating new applications, I follow a structured process, beginning with intake forms to determine whether OAuth or SAML is required, depending on whether the application is accessing internal or external systems. ServiceNow tickets are used

for configuration. This adaptive clustering ensures that the requests are automatically routed to the disaster recovery center if two data centers are down.

It includes a centralized tool where users can create their OAuth client IDs. However, I do not recommend this practice as it can lead to unnecessary client IDs and access tokens, increasing system load. Instead, I have developed a controlled process where users can request what they need, and the request is then sent to me for approval. This approach ensures that the process is managed effectively.

Overall, my experience with the solution has been very positive. It has played a crucial role in enhancing the security and efficiency of our access management processes. While there are always areas for improvement, particularly in terms of scalability and phishing resistance, it has consistently met our expectations. I would highly recommend it to organizations looking for a reliable and secure access management solution.

I rate it an eight. .”

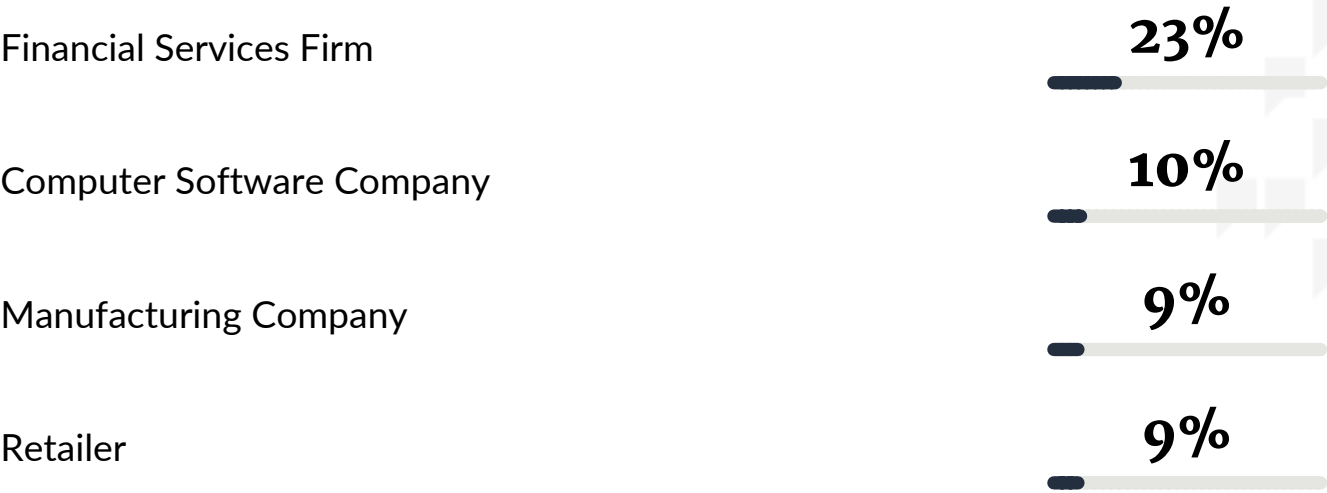
Verified user

Sr IAM Consultant at a healthcare company with 10,001+ employees

[Read full review](#) 

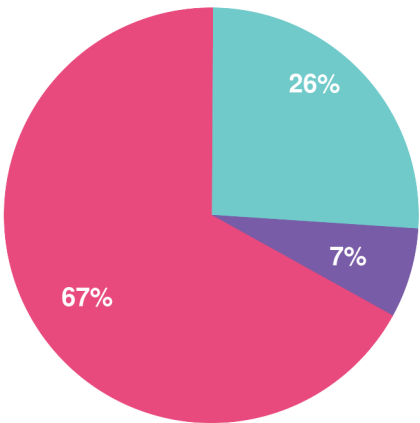
Top Industries

by visitors reading reviews

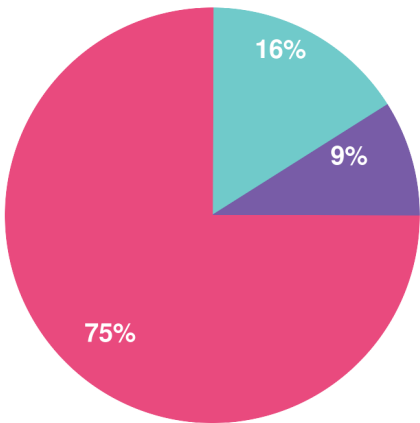




Company Size

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