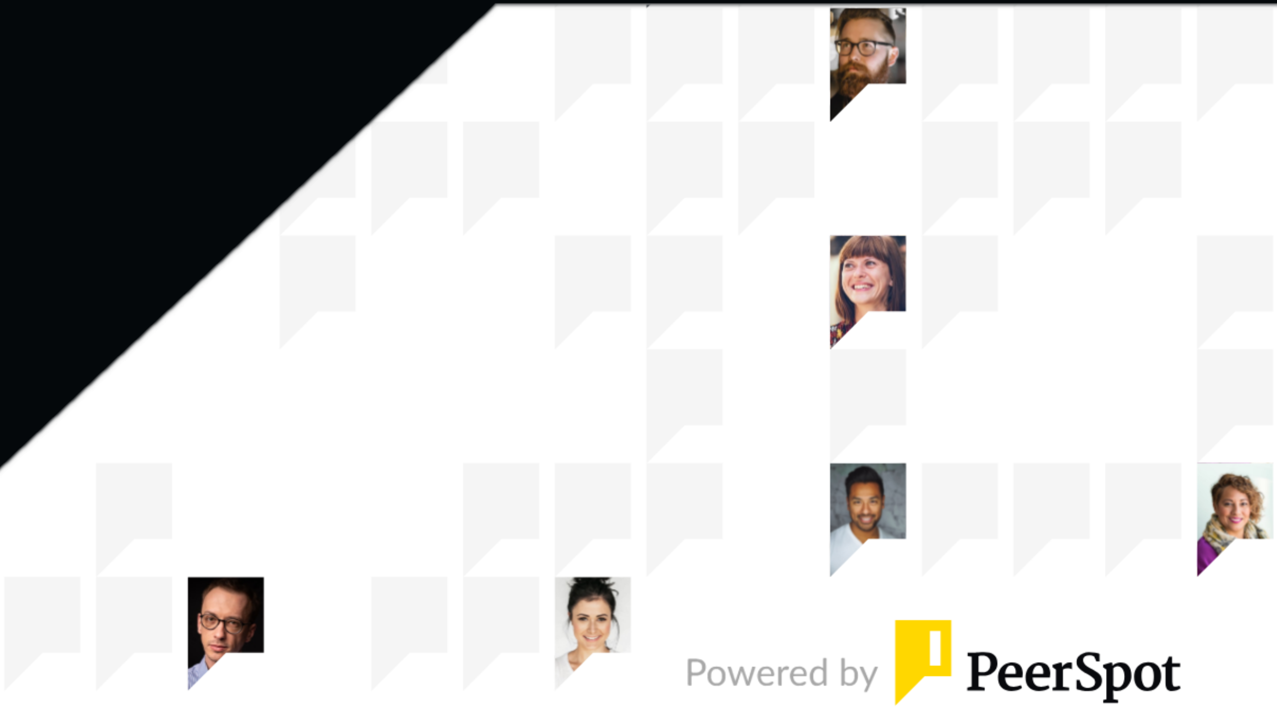
aws marketplace

OpenText Core Application Security

Reviews, tips, and advice from real users



Powered by PeerSpot

Contents

Product Recap

OpenText Core Application Security

OpenText Core Application Security Recap

OpenText Core Application Security offers robust features like static and dynamic scanning, real-time vulnerability tracking, and seamless integration with development platforms, designed to enhance code security and reduce operational costs.

OpenText Core Application Security is a cloud-based, on-demand service providing accurate and deep scanning capabilities with detailed reporting. Its integrations with development platforms ensure an enhanced security layer in the development lifecycle, benefiting users by lowering operational costs and facilitating efficient remediation. The platform addresses needs for intuitive interfaces, API support, and comprehensive vulnerability assessments, helping improve code security and accelerate time-to-market. Despite its strengths, challenges exist around false positives, report clarity, and language support, alongside confusing pricing and package options. Enhancements are sought in areas like CI/CD pipeline configuration, report visualization, scan times, and integration with third-party tools such as GitLab, container scanning, and software composition analysis.

What features define OpenText Core Application Security?

- Static and Dynamic Scanning: Offers thorough analysis to identify vulnerabilities during development.
- Real-time Vulnerability Tracking: Continuously updates and monitors potential security threats.
- Seamless Development Platform Integration: Enhances security processes without disrupting workflows.
- Cloud-Based Service: Provides flexible, on-demand security capabilities with accurate results.
- API Support: Allows smooth integration and automation within existing systems.

What benefits should users look for in reviews?

- Reduced Operational Costs: Optimizes resources by lowering costs associated with security management.
- Efficient Remediation: Speeds up the process of identifying and resolving vulnerabilities.
- Enhanced Code Security: Strengthens overall application security during the development lifecycle.
- Accelerated Time-to-Market: Streamlines development stages by integrating essential security tools.

Industries like mobile applications, e-commerce, and banking leverage OpenText Core Application Security for its ability to identify vulnerabilities such as SQL injections. Integrating seamlessly with DevSecOps and security auditing processes, this tool supports developers in writing safer code, ensuring secure application deployment and enhancing software assurance.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

✓ “It is valuable in improving our overall security posture by catching significant errors.”

Verified user

Lead Developer at a legal firm with 1,001-5,000 employees

✓ “The source code analyzer is the most effective for identifying security vulnerabilities.”

Jonathan Steyn

Principal Technical Consultant at EOH

✓ “The scanning capabilities, particularly for our repositories, have been invaluable.”

Javad_Talebi

Cloud architect at Vodafone

✓ “It helps deploy and track changes easily as per time-to-time market upgrades.”

AhmedElkholy

Pre-Sales Manager at Ejada Company Limited

✓ “Each bank may have its own core banking applications with proprietary support for different programming languages. This makes Fortify particularly relevant and advantageous in those cases.”

AbbasiPoonawala

Architecture Manager at Alinma Bank

✓ “What stands out to me is the user-friendliness of each feature.”

Verified user

Test Lead at a financial services firm with 10,001+ employees

✓ “I use the solution in my company for security code scans.”

Verified user

Director at a healthcare company with 10,001+ employees

What users had to say about valuable features:

“Fortify helps me find serious issues, such as developers inadvertently leaving access tokens, including API access tokens, in the source code. Fortify is effective in identifying such oversights, making it a really helpful tool despite its problems. It is valuable in improving our overall security posture by catching significant errors..”

Verified user

Lead Developer at a legal firm with 1,001-5,000 employees

Read full review

“I appreciate all the features, with a particular emphasis on their vulnerability scanner. For instance, in our environment where two-factor authentication is prevalent across many of our sites, the scanner efficiently identifies vulnerabilities, including those related to second-factor methods or mobile codes. What stands out to me is the user-friendliness of each feature. Given that we're a bank with multiple applications, having the flexibility to customize solutions according to the unique needs of each application is crucial..”

Verified user

Test Lead at a financial services firm with 10,001+ employees

Read full review

“The solution is user-friendly. One feature I find very effective is the tool's automatic scanning capability. It scans replicas of the code developers write and automatically detects any vulnerabilities. The integration with CI/CD tools is also useful for plugins.

The tool's AI feature analyzes security threats and recommends updating the code accordingly. One major issue that AI detected for us was logging issues and hardware vulnerabilities. Fortify On Demand identified these, allowing our developers to address and fix the issues..”

Manikantha Nagireddy
Security Tester at Ray Business Technologies Private Limited

Read full review

“Our CSD team used multiple tools for different scenarios. When dealing with sophisticated threats or vulnerabilities, manual analysis was necessary alongside Fortify's machine-based analysis. So, in handling complicated vulnerabilities, we couldn't rely on just one tool. Multiple tools were required. One such tool was OS Zap Proxy. We integrated Zap Proxy with Fortify, and this integration proved quite useful. Instead of relying solely on Fortify's dashboard, we integrated it with other tools, which made more sense. The security analysts, up to the level of the CSO, wouldn't rely only on a single dashboard. They used multiple tools to detect and work on vulnerabilities across various platforms and products. Fortify seamlessly integrates all these aspects..”

AbbasiPoonawala
Architecture Manager at Alinma Bank

Read full review

“One of the most valuable features of Fortify On Demand is its ability to integrate seamlessly with the DevOps lifecycle, particularly in terms of security testing. Injecting security testing into the DevOps process ensures that security measures are incorporated from the development stage onwards. It aligns with the main objective of DevOps, which is to automate and streamline the software development lifecycle, from code commit to deployment. With automation tools orchestrating the pipeline, tasks such as code compilation, testing, and deployment can be carried out rapidly and efficiently. This results in faster time-to-market for features, reducing deployment times from hours to minutes. It enhances trust from customers and cybersecurity teams, as security measures are built into the software from the outset, increasing confidence in the security..”

AhmedElkholy
Pre-Sales Manager at Ejada Company Limited

Read full review

“The source code analyzer is the most effective for identifying security vulnerabilities. It is the engine or the artificial intelligence behind the scanning engine that does the actual analysis of the data, and they then create an FPR file. This FPR file can then be further analyzed and tested at ScanCentral, which is your centralized dashboard for security auditing and remediation.

So from there, once you've got the artifact or this file, which is created from scanning all of your applications, it gives you a comprehensive overview of the vulnerability scores or the bug densities of your code, and then you can further analyze and test those codes and draw reports from ScanCentral.

So, these reports are against the OWASP Top ten. So you've got different reports that will give you a detailed analysis of your scan data, and it also does it in a dashboard format. So you then get a comprehensive report, and you can also draw a developer's workbook report, which you can send to developers where they actually have a bird's eye view or code-level view of the vulnerabilities and the recommendations are made by Fortify on how you can remediate those threats or vulnerabilities.

And you can then improve your bug density and scores, and you can also do that from the dashboard interface. You can also remediate and within the dashboard, change your score. So you have the dashboard, which gives you a comprehensive overview across all the applications. Also, as you remediate and fix your code, the dashboards update your scores, and then you have a view, and you can control your bug densities across all of the applications once you've onboarded each and every application. And that's across all your DAST and SAST applications. And this is on a centralized dashboard.

Fortify is constantly improving. Their tools and their interfaces are modernized with every new feature or every new version. I constantly see improvements by OpenText. OpenText is very intuitive. They're also implementing a lot of new AI capabilities with the NerdTools, which I think is remarkable..”

Jonathan Steyn
Principal Technical Consultant at EOH

Read full review

Other Solutions Considered

“We did not use a different solution previously. Before we had this solution, we were just evaluating other solutions and looking at the costs, and trying to bring in something newer, like an integrated automated secure stack, or something like that..”

Fernando Carlos
Project Manager at Everis

Read full review

“We use SonarQube alongside Micro Focus Fortify on Demand.

The difference between the two is Micro Focus Fortify on Demand handles the security testing and SonarQube does more in-depth level code testing..”

Jayashree Acharyya
Director at PepsiCo

Read full review

“We didn't evaluate any other solution. I was trying to find out which solution should I use, and I just saw good reviews of this solution. This was the first solution that we tried out, and we liked it. We started with a trial, and it was doing good. Our necessities were met, so we didn't try to figure out any other competitive tool in the market. .”

Mamta Jha
Co-Founder at TechScalable

Read full review

“We've been working with SonarQube for five years. SonarQube can show us the initial test and how your code is developed over time. It gives us insight into how a specific project is progressing. That's the great thing about SonarQube. Once the code goes into the Fortify or Nexus, it's mostly a safety check. SonarQube catches most of the vulnerabilities in Python at the development stage..”

Yash Brahmani
Devops Engineer at BNP Paribas

Read full review

“We were considering upgrading to the enterprise level, given the need for a robust solution in the banking environment. During this evaluation, we compared Netsparker, Burp Suite, and Fortify. After conducting a proof of concept (POC) that involved testing APIs, websites, and infrastructure arrangements, we presented our analysis to management. Ultimately, Fortify was selected as the preferred choice..”

Verified user

Test Lead at a financial services firm with 10,001+ employees

Read full review ↗

“We are already decommissioning Fortify and have already implemented SonarQube. We are currently using SonarQube Enterprise.

Fortify on Demand was utilized for a considerable period. However, we have now transitioned away from Fortify on Demand. It was primarily used by our CSD team, the cybersecurity defense team at the bank.

Initially, we performed penetration testing and vulnerability assessments within the Fortify platform. However, we have since implemented a DevSecOps pipeline in partnership with Red Hat. Currently, all testing, including penetration testing and vulnerability assessments, is automated within the pipeline. The pipeline runs on Tecton, enabled on the OpenShift site.

Therefore, any tool we use, be it Fortify or SonarQube, must be integrated into that pipeline. This approach has addressed most of the pain points we faced previously. Consequently, we are satisfied with SonarQube's performance now.

Fortify on Demand only offers static analysis and lacks dynamic security testing capabilities. However, if it's integrated into the pipeline, we can incorporate another tool for dynamic security testing. This was not possible with Fortify alone.

Additionally, Fortify has limited programming language support compared to SonarQube. The recent global launch of SonarQube in the GA version expanded its support for various programming platforms, such as CSM and .NET on the Java side, among others.

In our bank, we use T24 as our core banking system, which relies on a proprietary programming language called Infobasic. SonarQube also supports this language. When we place the code into the pipeline and perform builds, including the repository, we scan the entire codebase, including Infobasic code for the banking application. In summary, SonarQube offers broader programming language support. Previously, we only scanned other business-critical applications, but now we can scan our most critical banking application, T24, using SonarQube..”

AbbasiPoonawala

Architecture Manager at Alinma Bank

Read full review

ROI

Real user quotes about their ROI:

“Fortify On Demand is not highly expensive. It provides options for the number of scans and tests for the on-premise version. The customers utilizing hardware must install the tool for cost-effectiveness and high availability..”

AhmedElkholy
Pre-Sales Manager at Ejada Company Limited

Read full review ↗

“At this time, I don't have an answer on the return of investment. As far as I can see, it's necessary. If we got exposed or had a data leak it would cost the company dearly. With that in mind, while I can see there's an ROI, I can't provide an exact number..”

Fernando Carlos
Project Manager at Everis

Read full review ↗

“Quality vs quantity: You pay more for a higher-quality product and meets your needs, compared to others that might be cheaper, but you have to crawl to get what you are looking for..”

Verified user
Specialist Master/Manager at a consultancy with 10,001+ employees

Read full review

“Micro Focus Fortify on Demand has saved our company money from the use of automation features. We are able to run the scans automatically from the pipeline saving us a lot of time and communication. Previously it would have taken a few days whereas now it can be completed in 10 minutes..”

Jayashree Acharyya
Director at PepsiCo

Read full review

“Fortify on Demand improved the overall security posture our customers. Fortify on Demand has reduced not only bug densities but also their attack surface quite drastically. And it's in real-time because it's got real-time dashboards, and their security teams are more proactive. It's a lot easier for them to implement their security mechanisms and gateways because Fortify allows that. I have seen a dramatic reduction in bug densities and incidents. So, a major reduction in security incidents as a result of using Fortify..”

Jonathan Steyn
Principal Technical Consultant at EOH

Read full review

“Looking for a return on investment on security is a little challenging. Some CIOs might argue one way or another. Some look at it as a cost, and some look at it as cost avoidance. I'm a security professional, and I look at it as cost avoidance. So, we're avoiding breaches, people being able to manipulate the code or cause any issues, and downtime. I always look at the positives of the product. If we eliminate any of the security risks or attack factors on these products before they go live, we're doing due diligence in making sure that the product stays up and running, especially for something like e-commerce..”

Verified user

Security Systems Analyst at a retailer with 5,001-10,000 employees

Read full review

Use Case

“I primarily use Fortify to check for sensitive information disclosure in the source code and for identifying security vulnerabilities. These types of issues are scanned by Fortify..”

Verified user

Lead Developer at a legal firm with 1,001-5,000 employees

Read full review

“We use it to scan the bank's applications systematically. This process aims to identify and address security vulnerabilities within the applications, ensuring the robustness of our security measures..”

Verified user

Test Lead at a financial services firm with 10,001+ employees

Read full review

“I use the solution to check the software, as the development is done internally, to detect any security breaches. If there is something in the code that could lead to SQL injections or other vulnerabilities, it will be detected..”

Robertino Catalin Ionescu

Department Manager of Testing Automation Centre at a energy/utilities company with 10,001+ employees

Read full review

“The primary use case for Fortify On Demand in our environment revolves around its critical role in sales and desk operations. It helps identify application vulnerabilities from both a source code and web perspective. It directly detects issues such as SQL injection in the source code. It conducts website scans with customizable configurations to examine potential risks and vulnerabilities, which is crucial during software development. We can avoid risks before moving to the production stage..”

AhmedElkholy
Pre-Sales Manager at Ejada Company Limited

Read full review

“I have used Fortify on Demand for security scanning, along with outsourcing to companies that scan our systems and report vulnerabilities. My work has involved securing our APIs and systems.

We use Fortify across all stages of the environment: development, test, and production. We even use it for disaster recovery.

Whenever we deploy our Jenkins pipelines, the system automatically scans our Git repository to fix security vulnerabilities. All the security vulnerabilities are then created as tasks in Jira, so we can fix them as quickly as possible..”

Javad_Talebi
Cloud architect at Vodafone

Read full review

“Fortify On Demand is a cloud-based service/software-as-a-service model. Fortify On-Prem, which I have implemented, is an on-prem service where the customer provides the server infrastructure, and then Fortify On Demand comes fully implemented out of the box.

But you're still able to connect all of your Git repositories and your build environments like Maven and Gradle and all these different build environments, even like Jenkins that customers are using. It's fully connected either whether it's on-prem or cloud, and then you can do a full scan analysis of your security posture.

SAST and DAST scanning. Dynamic application scanning as well as static application scanning. So that would be websites, and you can do an audit and crawl scan of your web-based or web-facing applications, and then also scan your source code of your static application code..”

Jonathan Steyn
Principal Technical Consultant at EOH

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.

“We have a dedicated Fortify team, along with service teams with developers involved in the deployment process. It does not take longer than thirty minutes to deploy..”

Verified user

Lead Developer at a legal firm with 1,001-5,000 employees

Read full review

“The initial setup is complicated. It takes around four to five hours to complete, including installation and scanning. I rate the process a seven out of ten..”

AhmedElkholy

Pre-Sales Manager at Ejada Company Limited

Read full review

“It was straightforward. It took us two or three months because we had to integrate with our DevOps and pipeline solutions. It took a bit of extra time.

In terms of maintenance, we need to update the version. Micro Focus releases new versions every two months or so..”

Jaime Baracaldo

Chief Information Officer at Location world

Read full review

“The initial setup experience with Fortify On Demand was straightforward for us. We installed the plugin and integrated it with our existing tools and logins. There was no need for configuration or setup—it was quite simple. The deployment time varies based on the code complexity. Once vulnerabilities are identified, the support team provides the necessary fixes. .”

Manikantha Nagireddy

Security Tester at Ray Business Technologies Private Limited

Read full review

“I am the architecture manager, and my team evaluated and onboarded Fortify based on reviews and evaluations from GQ, Peerspot, Gartner, and even Forrester.

During the setup process, we had concerns regarding the cost. From the CSD perspective, Fortify was not very cost-friendly. The CSD has a separate budget and reports directly to the CEO and CIO. We had to consider our budget limitations because we have been leveraging Fortify since the bank's inception in 2008. Although we have utilized it extensively, the cost appeared higher compared to SonarQube. Hence, we decided to go with SonarQube. However, I must say that Fortify offered a lot of value.

It was quite manageable to maintain. We have a dedicated team that supports Fortify in production. So, it was quite manageable. .”

AbbasiPoonawala

Architecture Manager at Alinma Bank

Read full review

“Fortify on Demand is fully functional and fully integrated with an open-source analysis tool that's fully integrated with Fortify on Demand. So, Fortify on Demand is easy to use. It's intuitive. No implementation or training is required.

Fortify on-prem requires a bit of work, but I was able to set up, in a lab environment, the controllers, the scanners, the architecture, and all of the different servers in a virtualized environment. You could set it up quite relatively easily without requiring major training because the user guides are very easy to follow. I've set up lab environments within an hour.

So you could literally set up your entire on-prem Fortify solution within an hour because it is a very simple process to follow. The setup, installation, and configuration of the files are not that difficult to do. So you could effectively do it within an hour. You could set up the entire environment.

I would rate my experience with the initial setup an eight out of ten, where ten being easy and one being difficult.

Cloud and on-prem. So that it's hybrid. There's three tiers for deployment model. You can do Fortify on Demand, which is a fully functional system on the cloud. Fortify On Prem, which is a system where your Fortify system is installed on client servers or on-premises. And then hybrid would be a combination of both services where you have some implementation with the client and some in the cloud..”

Jonathan Steyn

Principal Technical Consultant at EOH

Read full review

Customer Service and Support

“Customer support is amazing. They've got community forums, customer resources, a lot of free resources, and their premium support is very effective. So they have proper support internationally. They've been very good..”

Jonathan Steyn
Principal Technical Consultant at EOH

Read full review

“Whenever we have any issues, Micro Focus support has been helpful. They have lots of products, and they're established in the market. When you open a ticket, you get an immediate response by phone..”

S S RAMA KRISHNA MURTHY SURI
Senior Manager at valuelabs LLP

Read full review

“The support from Micro Focus Fortify on Demand is great. They have been very good to answer our questions. They have their own Fortify on Demand team and they will help you resolve your problems..”

Harkamal-Singh
Solution architect at NTT

Read full review

“The support is good. Their support is in the Netherlands, sometimes it takes some time for the time zone difference between Latin America and the Netherlands but overall the support is good..”

Verified user

R&D at a tech services company with 51-200 employees

Read full review

“I used technical support during the integration between Fortify and ALM, but the support staff was not adequately prepared to assist me. I identified that there is a need for development between Fortify on Demand and ALM.net. They initially said that it was working with ALM, but after reading the documentation, I discovered that it only works with Octane, not with ALM.net..”

Robertino Catalin Ionescu

Department Manager of Testing Automation Centre at a energy/utilities company with 10,001+ employees

Read full review

“Whenever required, we have reached out to the technical support team. Our architecture team thoroughly evaluated Fortify along with our stakeholders. We always prioritize leveraging our existing applications from an inventory of over 340 applications, rather than opting for new ones.

When we onboarded Fortify in 2008, we had other choices for tools and products as well, but we didn't choose them. This decision was made by the cybersecurity defense team, who are the primary users of the product.

They were satisfied with Fortify, and we didn't require extensive support. However, whenever needed, we can rely on the support included with the license..”

AbbasiPoonawala
Architecture Manager at Alinma Bank

Read full review

Other Advice

“Based on the experience of our company, I would recommend Fortify. It is helpful despite its problems, and I rate it as a seven out of ten.

It effectively detects serious security issues, adding to our confidence in using it as a vital tool in our processes..”

Verified user
Lead Developer at a legal firm with 1,001-5,000 employees

Read full review

“I rate the platform's accuracy for detecting vulnerabilities an eight and a half out of ten. By utilizing Fortify as a comprehensive security testing tool, financial institutions operating at high-security levels gain confidence in the security posture of their applications. It helps deploy and track changes easily as per time-to-time market upgrades.

I advise new users to learn about new features introduced in the last two years. I rate it a nine out of ten..”

AhmedElkholy
Pre-Sales Manager at Ejada Company Limited

Read full review

“With over 12 years in application security, I've consistently observed the adoption of Fortify in major organizations like Cognizant, Barclays, and Credit Suisse. Across large banks in Europe, Fortify has established a reputation for reliability and effectiveness. Drawing on my experience, I am confident that organizations with clear problem statements and no budget constraints will find Fortify to be a comprehensive solution. Its technical capabilities and features align well with the diverse needs of large organizations in the banking sector. Overall, I would rate it ten out of ten..”

Verified user
Test Lead at a financial services firm with 10,001+ employees

Read full review

“My organization has been using the solution for at least four years. I don’t deal with technical support directly. I would recommend the solution to others. We are dealing with some issues with the report.

The reports might be meaningful, but they sometimes do not match the situation. We cannot really deal with them. We don't know if they are false positives or if they're simply not relevant because they concern vulnerabilities in the development cycle and not in the production operations. It is sort of a mystery. Overall, I rate the tool an eight out of ten..”

Angelo Quaglia
Independent Professional at Studio Dott. Ing. Angelo Quaglia

Read full review

“Fortify has excellent support for various programming languages. Each bank may have its own core banking applications with proprietary support for different programming languages. This makes Fortify particularly relevant and advantageous in those cases. This advantage may not be present in SonarQube.

Additionally, if a feature is not offered out of the box, Fortify allows customization, providing flexibility. Apart from dynamic security testing, Fortify is reliable for generating and distributing v-scan reports to multiple stakeholders, making it less of a hassle for the CAC team as most tasks are automated.

I would rate Fortify on Demand as an eight..”

AbbasiPoonawala
Architecture Manager at Alinma Bank

Read full review

“As an expert, a lot of what I've seen in the tool is to use the principle of defense in-depth. Because that is the objective of Application Security, Fortify. Customers often need to look at their current security architecture, security gateways, rules, and policies.

To best utilize Fortify is to shift left, to use all of the tools and plugins that Fortify has throughout the SDLC process, to use the IDE tools, including the board tools, to use all of these respective tools together. And to shift left, to start from the IDE perspective, before source code even goes into production, before it even reaches a build environment. It is to reduce bug densities by shifting left. Use Fortify to get your bug densities and your security or your attack surfaces to reduce it by shifting left from inception, before the code is even written. They can scrutinize, go into Fortify tools, analyze them, and progressively test your code using all the tools that Fortify provides.

A lot of customers already use their own tools and their own third-party tools. It's best to use one security architecture. So for instance, rather use Fortify with Brakeman and RASP, use the Fortify suite of tools as your one architecture instead of using several third-party tools. It's always good to**centralize your security architecture and use one architecture for your entire security posture** instead of using different tools. Fortify has all the capabilities to centralize your security attack methodology.

So, your attack surface comes from different perspectives. It comes from an open-source code perspective. So you've got open-source code. You have proprietary code. You have repositories. You have different places where your code is, even in Azure. We even have a plugin for Azure. The point is to use all of the capabilities of Fortify as your central tool instead of using disparate tools that do not integrate with Fortify, that do not work with Fortify. It's always good to have one solid architecture as opposed to multiple disjointed tools.

Overall, I would rate it a ten out of ten. I've used several technologies and tools, even open-source or free tools, over the last fifteen years. In my opinion, from the perspective of the many tools used and other competitors, I have found Fortify to be the most reliable. They kind of align with my principles and the principles of cybersecurity specialists with defense-in-depth and shifting left. Because those are very important principles to me. And also confidentiality, integrity, and availability. They align with all of those pillars and building blocks of cybersecurity..”

Jonathan Steyn
Principal Technical Consultant at EOH

Read full review

Top Industries

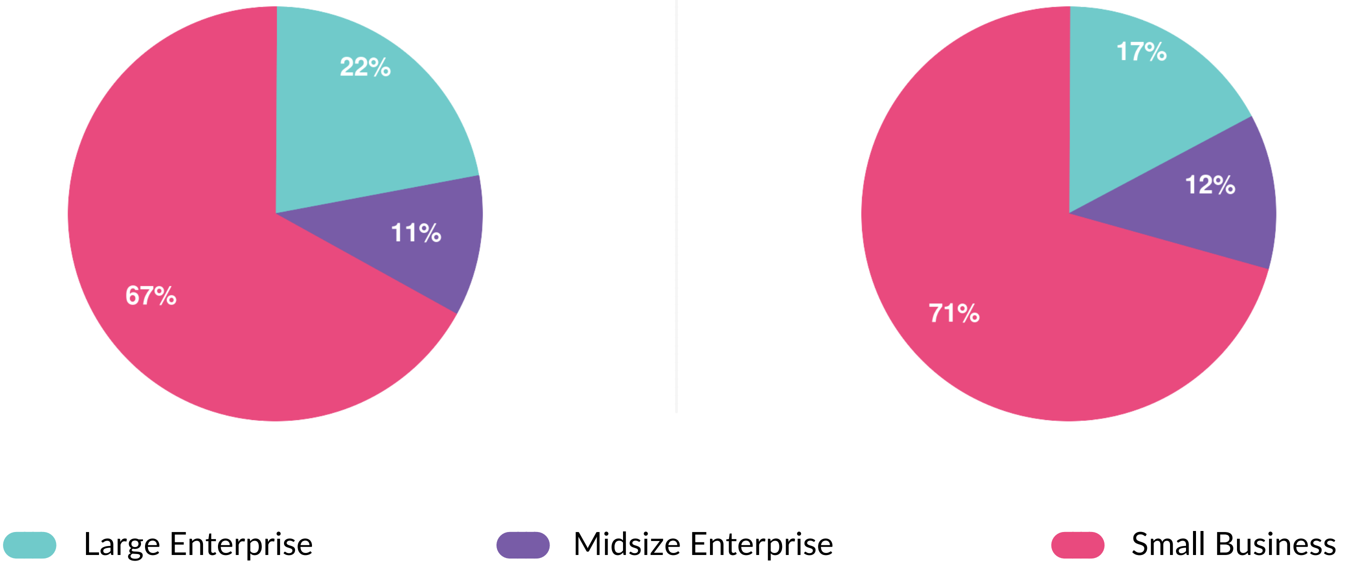
by visitors reading reviews

Financial Services Firm	18%
Manufacturing Company	15%
Computer Software Company	10%
Government	8%

Company Size

by reviewers

by visitors reading reviews



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