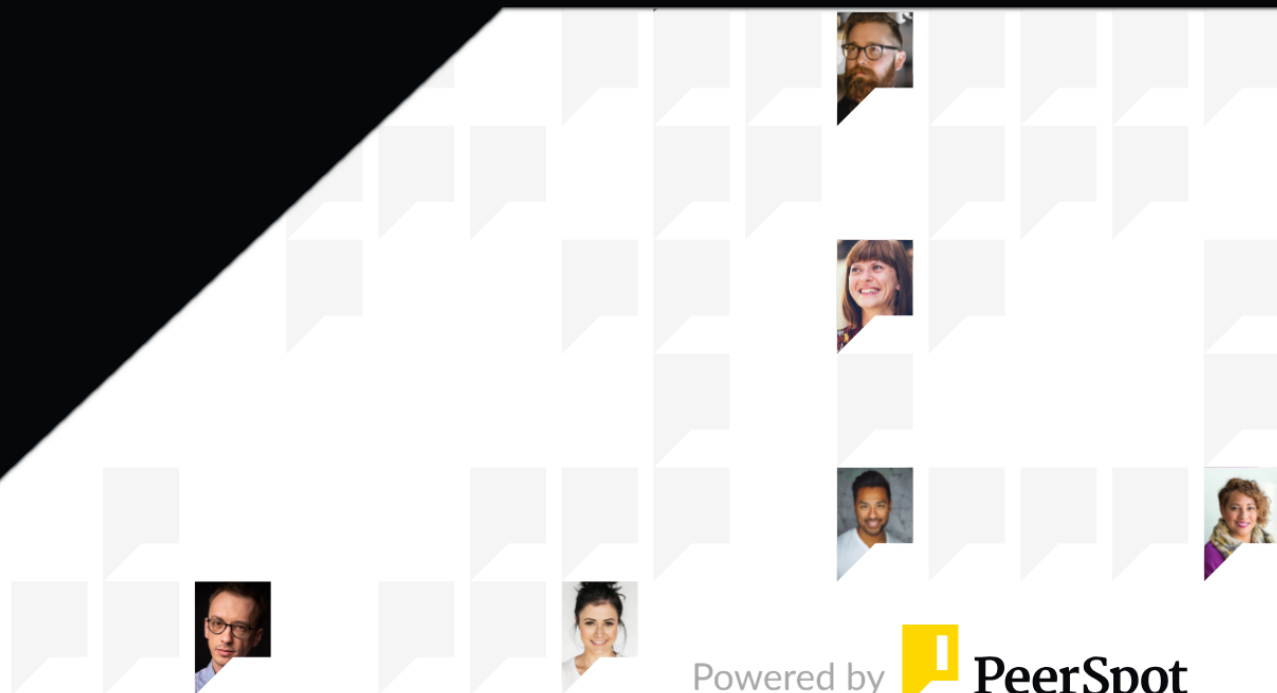




OpenText Core Application Security

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 5

Valuable Features..... 6 - 12

Other Solutions Considered..... 13 - 16

ROI..... 17 - 19

Use Case..... 20 - 24

Setup..... 25 - 28

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

Other Advice..... 32 - 36

Trends..... 37 - 38

About PeerSpot..... 39 - 40

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:



“Fortify on Demand is a very good service which can be used by any organization when they are building a team because it identifies security vulnerabilities early in the software development life cycle and provides good visibility into issues in cloud-hosted applications.”



Himanshu_Tyagi

Lead Cybersecurity at TBO



“The biggest advantage of this tool, Fortify on Demand, is that it is very scalable; it provides all the features just in time, and you do not need to have massive deployment or a lot of compute capabilities to use the product—that's the beauty of it.”



ShitanshuKumar

Co-Founder at Insecsys Technologies Private Limited



“The best features with Fortify on Demand include having analysis for any product based on analysis points.”



Diego Caicedo Lescano

Chief Innovation Officer at SAGGA

- ✓ “OpenText Core Application Security helps maintain compliance standards with a faster remediation cycle, as we know the vulnerabilities, and everybody knows that the developers can perform fixes more quickly.”



Wagner Azevedo

Cloud Security Manager at T-Systems International GmbH

- ✓ “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

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](#) 

“The best features with Fortify on Demand include having analysis for any product based on analysis points. With on-premise, you have to buy the license for each application. The licensing model is better on demand than on-premises. Another feature is that on demand you have two levels of reports: the first from the tool, which is the same as we can get from Fortify on-premises, and a next level reporting made by experts from OpenText, leading to a more condensed and precise report as level three..”

Diego Caicedo Lescano

Chief Innovation Officer at SAGGA

[Read full review](#) 

“Fortify on Demand is a good service. Since it is fully being managed by OpenText, after Micro Focus acquired Fortify, all services are managed by the Fortify team when a customer is using Fortify on Demand. When you are seeing the application and the vulnerabilities which have been identified by their tool, you can see the issues. However, the visibility of the actual work being done is by the Fortify team. If you want to fully outsource your services, then it's a very good solution.

“The best feature is that it supports many language frameworks. VB.NET was not available previously, but later they onboarded VB.NET as well, which is a legacy-based application, but some organizations still use VB.NET, so they have onboarded it, which is a good thing. Another aspect I appreciated about Fortify is that it gives a good understanding of the issues. The false positive rate is less, and they give valid issues. The invalid issues identified by Fortify are fewer. That is a good aspect. Additionally, you can integrate Fortify in CICD pipeline, so you get real-time updates about the security issues in your pipeline..”

Himanshu_Tyagi

Lead Cybersecurity at TBO

[Read full review](#) 

“The dynamic application security testing feature is the most valuable and useful for me so far, because the synapse does not have that—it has only FCA or CBON. The best application security tools support this testing, and usually, the customer wants to do tests while running, simulating real-world attacks. This is why OpenText Core Application Security is important, as it enables the customer to do that. The second is the SCA; I also support the customer in managing vulnerabilities for free open-source libraries and components. We can perform vulnerability management and handle the CVEs and licenses, of course, when we are talking about intellectual property.

The integration of OpenText Core Application Security with existing systems for security operations benefits us by providing vulnerability management and quality gates; without both, we will always have vulnerable applications running for our customers. This is the main benefit. The other benefit is related to the infrastructure; we leverage OpenText Core Application Security using the SaaS model, so we do not have to deploy any applications inside the customer environment. We can reduce the false positives and have a better approach to handle vulnerability management, making it the best tool for continuous integration with DevOps pipelines such as GitHub, Jenkins, and Azure DevOps..”

Wagner Azevedo

Cloud Security Manager at T-Systems International GmbH

[Read full review](#) 

“The biggest advantage of this tool, Fortify on Demand, is that it is very scalable; it provides all the features just in time, and you do not need to have massive deployment or a lot of compute capabilities to use the product—that's the beauty of it. It is supporting a few of the largest deployment web applications globally.

Fortify on Demand supports most of the major integrations and gives an opportunity to integrate custom-built solutions. For enterprise licenses, if you consume more than a couple of custom integrations, each would be a separate cost, allowing integration with any solution.

Automated risk assessment helps ensure that continuous risk analysis is happening; you get automated reports through a set of rules, batch scripts, and relating to different logs and events—that's how continuous assessment occurs.

Our solutions like SAST and DAST are compliant, allowing compliance with CMMI levels. Additionally, integration with ArcSight provides various compliance reporting for PCI, HI-TRUST, HIPAA, FCC, ISO 27001, 22301, and 27701. .”

ShitanshuKumar

Co-Founder at Insecsys Technologies Private 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

“As a vendor, I was part of Micro Focus while I was taking care of OpenText Core Application Security.

Before Micro Focus OpenText, I used multiple solutions like Synopsys, which offers very promising competition. .”

ShitanshuKumar

Co-Founder at Insecsys Technologies Private Limited

[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 switched to Checkmarx.

“When you talk about the key differences between Fortify and Checkmarx, we migrated from Fortify to Checkmarx because at that time, Fortify was not supporting VB.NET application, and our main application was using VB.NET. We raised the case with Fortify team about any plan in their future release to onboard VB.NET, but they didn't give us a good answer because they were saying they would try to onboard VB.NET into their platform in a year. A customer won't wait for one year to assess their application..”

Himanshu_Tyagi

Lead Cybersecurity at TBO

[Read full review](#) 

“SonarQube is used as a different solution for SAST.

“The main difference between Fortify and SonarQube is that SonarQube is a complete solution for SAST plus quality code analysis, focusing on five pillars, which according to ISO 25000 includes security as one pillar.

“Q1 from Idera is another solution that covers five pillars and is great compared to Fortify, which only addresses the security pillar. There are significant differences in findings, as each solution has different findings, but SonarQube is the best for SAST findings..”

Diego Caicedo Lescano

Chief Innovation Officer at SAGGA

[Read full review](#) 

“When you talk about the key differences between Fortify and Checkmarx, we migrated from Fortify to Checkmarx because at that time, Fortify was not supporting VB.NET application, and our main application was using VB.NET. We raised the case with Fortify team about any plan in their future release to onboard VB.NET, but they didn't give us a good answer because they were saying they would try to onboard VB.NET into their platform in a year. A customer won't wait for one year to assess their application.

“The pros of Fortify include that you get a good understanding of the issues identified by the application. They continuously send notifications that the scan is being paused and the customer has to initiate the scan because the application scan has failed for some reason. The timely notification and visibility of issues identified is good, and the false positive aspect is also good.

“Coming to Checkmarx, when we onboarded it, our primary reason was the VB.NET issue, and Checkmarx also has very good coverage on Java-based applications. The majority of our applications were on Java, and Checkmarx did a great job on the coverage of assessing our applications. Regarding the accuracy of issues, I find it almost the same for Fortify and Checkmarx. I didn't find much difference on the false positive side either..”

Himanshu_Tyagi

Lead Cybersecurity at TBO

[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..”

Abbasi Poonawala

Chief Enterprise Architect 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](#) 

“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

[Read full review](#) 

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

“There are indeed savings with OpenText Core Application Security because when investing in a security solution, the efficacy depends on the orchestration and the layers in place. Many failures in achieving ROI stem from configurations, not deployments. A notable example is securing an important transportation application for a different country—a situation demanding stringent security measures.

There is definitive ROI if OpenText Core Application Security is deployed properly; it substantially reduces efforts in securing the solution while averting various application-related risks. .”

ShitanshuKumar

[Read full review](#) 

Co-Founder at Insecsys Technologies Private Limited

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](#) 

“I am familiar with all of the ADM portfolio, Application Delivery Management, including UFT, Unified Functional Testing, and we are building LoadRunner for security, specifically for the Cyber Res portfolio, which is Fortify, and for the other portfolio, SMAX for Service Desk and monitoring..”

Diego Caicedo Lescano

Chief Innovation Officer at SAGGA

[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](#) 

“For OpenText Core Application Security, I currently support a couple of my clients who are using Fortify on Demand for their web application, CRM, and sales platform.

Many good features of Fortify on Demand include SAST and DAST capabilities, and you can do sandboxing of a few features when you're testing web applications. You can create environments and recreate scenarios. I can walk you through the platform itself, taking about six to eight hours, because I have been working on the product as a product specialist and product manager, so I know the ins and outs of it.

Before Micro Focus OpenText, I used multiple solutions like Synopsys, which offers very promising competition. .”

ShitanshuKumar

Co-Founder at Insecsys Technologies Private Limited

[Read full review](#) 

“My usual use cases for OpenText Core Application Security include SAST and static testing, which covers the majority of the CVAs or CVSS that we have in the deployments.

The dynamic application security testing feature is the most valuable and useful for me so far, because the synapse does not have that—it has only FCA or CBON. The best application security tools support this testing, and usually, the customer wants to do tests while running, simulating real-world attacks. This is why OpenText Core Application Security is important, as it enables the customer to do that. The second is the SCA; I also support the customer in managing vulnerabilities for free open-source libraries and components. We can perform vulnerability management and handle the CVEs and licenses, of course, when we are talking about intellectual property.

The integration of OpenText Core Application Security with existing systems for security operations benefits us by providing vulnerability management and quality gates; without both, we will always have vulnerable applications running for our customers. This is the main benefit. The other benefit is related to the infrastructure; we leverage OpenText Core Application Security using the SaaS model, so we do not have to deploy any applications inside the customer environment. We can reduce the false positives and have a better approach to handle vulnerability management, making it the best tool for continuous integration with DevOps pipelines such as GitHub, Jenkins, and Azure DevOps..”

Wagner Azevedo

Cloud Security Manager at T-Systems International GmbH

[Read full review](#) 

“I have been working with AWS cloud for the past six to seven years, and in my current role, I am working on AWS cloud.

“Fortify was used for scanning applications to identify dynamic security vulnerabilities. Another solution from Fortify named Fortify Source Code Analyzer, basically SCA, scans lines of code for different technologies, such as ASP.NET, VB.NET, and Java-based applications. It scans different lines of code for an application and flags vulnerabilities, and on the basis of that vulnerability, a security professional has to identify false positives and then report it to the internal application team.

“When security issues are identified in the early stage of the software development life cycle, it really helps because if threats are identified early, the product being developed by the application development team has fewer security issues. There is no product that doesn't have any issues. Obviously, the team tries to build a solution that has zero issues, but that is hypothetical. When threats are identified in the early software development life cycle, it gives confidence among the team and provides a fair idea that the application being developed will be a viable solution for the customer.

“Whenever any security vulnerability is identified by Fortify or OpenText, it gives information about whether that particular security issue is non-compliant related to PCI, ISO 27001, or SOC 2. It provides a fair understanding that this security vulnerability should be prioritized because if you don't fix this vulnerability, your application will be non-compliant and your compliance goal will ultimately fail. So it helps a lot..”

Himanshu_Tyagi

Lead Cybersecurity at TBO

[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

[Read full review](#) 

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

“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

[Read full review](#) 

Pre-Sales Manager at Ejada Company Limited

“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

[Read full review](#) 

Security Tester at Ray Business Technologies Private Limited

“When you talk about static application source code testing, we had to involve the Fortify team to create an LDAP role for us. Regarding Fortify on Demand, it was pretty much straightforward because we just needed to configure our application in their platform. We had to enter the information for our application, and the rest was done by the Fortify team. Fortify on Demand was very simple. Regarding the SAST part, I won't say it was hard, but it was a little bit complicated, and when we raised cases with their technical support team, they resolved our queries and we onboarded the tool into our environment..”

Himanshu_Tyagi

[Read full review](#) 

Lead Cybersecurity at TBO

“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. .”

Abbasi Poonawala

Chief Enterprise Architect 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](#) 

“I have not needed to communicate with the technical support of OpenText Core Application Security or OpenText support.

For me, the documentation is adequate; I do not feel they need to add more information or use cases to what is available..”

Wagner Azevedo

Cloud Security Manager at T-Systems International GmbH

[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](#) 

“My experience with the technical support customer service team of Fortify was pretty good; I would rate it four out of five.

“I had direct contact with Fortify team and the sales director. I had direct interaction with them, which facilitated how we onboarded Fortify..”

Himanshu_Tyagi

Lead Cybersecurity at TBO

[Read full review](#) 

“I would rate the support for OpenText at no more than three out of ten; it is really bad, and we encounter a lot of problems when getting support.

“Support tickets often stay open for one month to three months, which leads to customer frustration. The wait time for a customer is too much. We understand the technology, but customers do not like paying for that kind of support..”

Diego Caicedo Lescano

Chief Innovation Officer at SAGGA

[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..”

Abbasi Poonawala

Chief Enterprise Architect 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 use Fortify on Demand for monitoring up to a certain extent; it provides monitoring and helps analyze and identify issues that could propagate in the application. When used in conjunction with ArcSight and other solutions, it gives a lot of analytics which allows you to make predictions and be proactive rather than reactive in security.

When it comes to custom integration, it usually takes about seven to ten days. This does improve threat response time in general..”

ShitanshuKumar

Co-Founder at Insecsys Technologies Private Limited

[Read full review](#) 

“I have been working with OpenText Core Application Security for code security and AppSec, GitHub advanced security, and the hyperscaler tools such as Azure Defender, AWS Security Hub, and WiredDaddy, covering all the AWS ecosystem

tools. I am quite familiar with the Google Security Center, and I come from Palo Alto.

OpenText Core Application Security helps maintain compliance standards with a faster remediation cycle, as we know the vulnerabilities, and everybody knows that the developers can perform fixes more quickly. This is important for compliance. The second point relates to PCI DSS, the framework for security concerning payment methods. I know that OpenText Core Application Security also provides access to OpenText trainings, enabling us to check all the requirements for PCI DSS. .”

Wagner Azevedo

Cloud Security Manager at T-Systems International GmbH

[Read full review](#) 

“If you want to onboard a solution for your application security side, I will definitely recommend Fortify because for your application, when you get a fair understanding of the security issues in the early stage of the software development life cycle, it's a very good thing.

“I have worked on Fortify on Demand. I have used it six months ago.

“Our applications were hosted on AWS cloud, and Fortify identified security vulnerabilities on our cloud platform. Our application which was hosted in AWS cloud showed that they provide good visibility. However, every tool has some pros and cons. If you ask me that if I want to recommend Fortify on Demand, it's obviously a good service which can be used by any organization when they are building a team. But if you have an in-house team which is working on many solutions, then it won't fit into their umbrella.

“Fortify on Demand was the on-demand service provided by Fortify that was assessing all our applications. When applications hosted on AWS cloud were being assessed, Fortify was identifying issues for the application which was hosted on AWS cloud.

“My experience with the technical support customer service team of Fortify was pretty good; I would rate it four out of five. Overall, I would rate this review a seven..”

Himanshu_Tyagi

Lead Cybersecurity at TBO

[Read full review](#) 

“I do have experience with OpenText.

“I would be willing to provide a review for an OpenText product, and we are partners from OpenText, selling a lot of products since UFT, functional testing, performance testing, and some of those products.

“Andres has experience with [LoadRunner Cloud](#), so Andres is the person to contact.

“I do have experience with Fortify on Demand as well as Fortify on-premises, but I am the general manager, not the technician. Andres is the technician, and you can have a call with Andres, Alex, or Henry to get any review or feedback on the products.

“For Fortify on Demand, the experience is less than three years—around two years, not more than that.

“I am familiar with Fortify and Real User Monitoring.

“The pricing is better for the customer, but it is not easy to understand the new pricing points. For us as partners, it is cheaper than the other licensing models, but for the customer, understanding how many points apply to each application can be confusing.

“The overall review rating for this product is 7 out of 10..”

Diego Caicedo Lescano

Chief Innovation Officer at SAGGA

[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](#) 

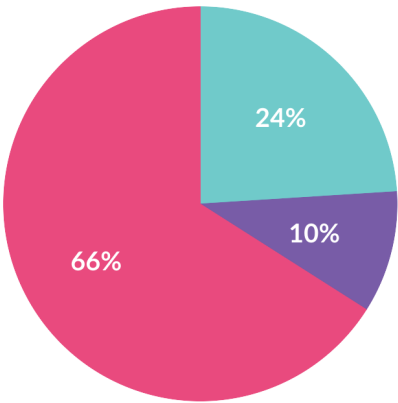
Top Industries

by visitors reading reviews

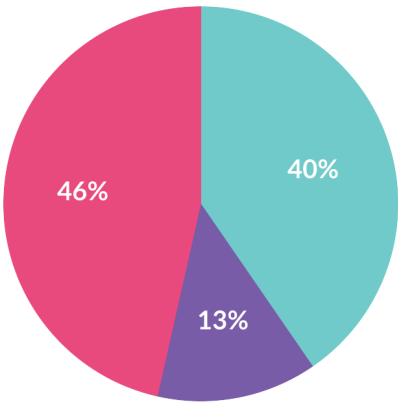


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsized Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

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

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

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

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

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

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

[Get your personalized report here](#)

About PeerSpot

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

PeerSpot helps tech professionals by providing:

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

Use PeerSpot to:

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

Join PeerSpot to connect with peers to help you:

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

Visit PeerSpot: www.peerspot.com

PeerSpot

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

reports@peerspot.com

+1 646.328.1944