aws marketplace

Kali Linux

Reviews, tips, and advice from real users

Powered by PeerSpot

Contents

Product Recap . . . . . 3 - 4

Valuable Features . . . . . 5 - 12

Other Solutions Considered . . . . . 13 - 15

ROI . . . . . 16 - 18

Use Case . . . . . 19 - 23

Setup . . . . . 24 - 27

Customer Service and Support . . . . . 28 - 30

Other Advice . . . . . 31 - 35

Trends . . . . . 36 - 37

About PeerSpot . . . . . 38 - 39

©2026 PeerSpot, All Rights Reserved

Product Recap

Kali Linux

Kali Linux Recap

Kali Linux is widely used by organizations for penetration testing, vulnerability assessments, web application security, network audits, ethical hacking, and open-source intelligence, providing extensive free features.

Organizations run Kali Linux in virtualized environments alongside other operating systems, employing tools for automated scans, malware identification, infrastructure testing, and application development or hosting. These users benefit from lower maintenance requirements and a smaller footprint. The toolset includes Nmap, SQLMap, Metasploit, and Hydra, ensuring effective security assessments. Its high scalability, performance, user-friendly interface, and extensive documentation enhance the platform's usability. Known for stability, flexibility, and virus resistance, Kali Linux supports web security, troubleshooting, and configuration tasks comprehensively.

What are the most important features of Kali Linux?

- Nmap: A network scanning tool for discovering hosts and services.
- SQLMap: An SQL injection and database takeover tool.
- Metasploit: A penetration testing platform with various exploit tools.
- Hydra: A network log-in cracker supporting numerous protocols.
- Documentation: Offers extensive resources for user guidance.
- Stability: Provides a reliable and consistent operating environment.
- Scalability: Adapts efficiently to growing security needs.
- Performance: Ensures fast and efficient operations.
- Virus Resistance: Enhances security through robust virus protection.

What benefits and ROI should users look for in reviews?

- Cost Efficiency: Free tools reduce operational expenses.
- Operational Efficiency: Lower maintenance needs and quick setup.
- Enhanced Security: Robust tools for comprehensive security measures.
- Flexibility: Adaptable to different environments and requirements.

Kali Linux can support industries in improving security through stable and flexible environments that resist viruses and provide extensive documentation. Users employ it for web security, troubleshooting, and configuring capabilities. Necessary improvements include automation, user-friendliness, and integrating AI and blockchain. Enhancements in security features, faster installations, and better learning tools are also essential. Machine learning integration and non-enterprise user functionalities can address current limitations.

©2026 PeerSpot, All Rights Reserved

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Kali Linux offers excellent features including being lightweight with low memory usage, easy installation, portability, and multiple architectures such as ARM architecture and server architecture."

Ciyagi Ciyagi

Senior Solution Architect & Delivery Lead at a tech services company with 10,001+ employees

- "Kali Linux has helped me significantly in simulating penetration testing and other activities, and since all the tools are open source, I can easily modify and customize them based on my needs."

Mathews Daniel

Cloud Security Architect at a tech services company with 10,001+ employees

- "Kali Linux stands out compared to other operating systems I have used for security work because it is a specific distribution of Linux that has all the required tools pre-loaded and configured."

Adarkum Kumar

Product security engineer at a tech vendor with 10,001+ employees

©2026 PeerSpot, All Rights Reserved

"Kali Linux is the only solution for cybersecurity if we are conducting pen testing or anything related to it."

M Pathak

Securuty solution architect at a tech services company with 11-50 employees

"Kali Linux has impacted my organization positively because it has allowed for the better security of my applications."

Validated user

Cloud Ops Lead at a tech vendor with 10,001+ employees

"Kali Linux positively impacts my organization by allowing us to monitor changes and security posture for the company."

Guillermo Buritica Tobon

Consultant at Cognizant

"Kali Linux is a very good tool and a good overall operating system to use when it comes to penetration testing, as it has a wonderful set of tools."

Validated user

Associate Cybersecurity Analyst at a university with 10,001+ employees

©2026 PeerSpot, All Rights Reserved

What users had to say about valuable features:

"Kali Linux is an operating system that has more than 30 plus tools that come as a package with Kali Linux. Those packages have their own purposes, such as Nmap, which is used for network testing. John the Ripper is used for passwords. Hydra is used for passwords and Wi-Fi. All tools have their own specific capabilities for the MITRE ATT&CK framework. Those are used for penetration, UABA analysis, and recent-related vulnerabilities. Most of the tools are a package with Linux and security-related tools, including those for spam and malicious emails.."

M Pathak

Securuty solution architect at a tech services company with 11-50 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"The best features Kali Linux offers, in my opinion, include being maintained by a reputable group, Offensive Security, and it is very much seen as the industry standard OS for ethical hacking. Because of a large user base, there have been many developments to make Kali Linux an all-in-one solution. I understand that Kali Linux is preloaded with maybe 500 security tools, so for anything from web security, such as using Burp Suite, to using Metasploit for exploit frameworks, I can use Kali Linux for anything ethical hacking based, making it really an all-in-one solution.

"Kali Linux has impacted my organization positively because it has allowed for the better security of my applications. The benefit here from security is multi-fold, including financial benefits because if the chance for exploitation is lower, then the chance to rack up server costs by being exploited is also lower, which is great, and also reputationally and from compliance perspectives, having that increased security benefits me.."

Validated user
Cloud Ops Lead at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

"Kali Linux comes with pre-installed ethical hacking tools in the terminal that you can use directly. You do not need to separately install each tool and its dependencies. All of them come with the same OS, which makes it very useful.

"The best features that Kali Linux offers are that it is faster, has a better response, and has fewer system requirements to utilize it. When I run a script on a GUI-based automation tool, it typically takes around ten to fifteen minutes. However, while using the CLI feature in Kali Linux, it gives me the output within one to two minutes. The performance is also better due to the ARM architecture that Kali comes with.

"Kali Linux has positively impacted my organization by providing all the tools and many methodologies we need for ethical hacking or VAPT requirements in a combined bundle in one OS. We do not need to go to other platforms to download separate tools and waste a lot of time doing that. It basically shortens that period of time.."

Validated user
Security Researcher at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

"The best features Kali Linux offers include the ability to customize everything and anything, from the terminal to the preferences to getting the environment set up and storing everything as I would want, and setting preferences accordingly.

"When I say customizing everything, I customize my tools that run using the CLI, such as the terminal itself. I usually write a script that would automate running four or five tools simultaneously. For example, I would provide input for a first tool, and the output from the first tool would be the input for the second tool, and so forth. The output from the second tool would be the input for the third tool, and similarly, I have a script written that combines three or four tools and gives me the end result exactly the way I want it or in the particular format that I need.

"A unique and really helpful feature of Kali Linux, compared to other operating systems, is that many of the offensive security tools are already pre-configured and pre-installed. I do not have to deal with a lot of hassle. I just boot up the operating system and I'm ready to go. The software is already loaded in the operating system.

"On a personal level, I have done a significant amount of learning, experimentation, and hands-on practice with Kali Linux.."

Adarkum Kumar
Product security engineer at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

"Kali Linux has positively impacted my organization significantly as it aids in red team work and penetration testing. It is not just red team work, as it also involves the blue team who defends and remediates issues, so having these tools available allows us to proactively identify issues rather than reactively, which is typically more difficult. Without these tools, the identification process is complicated and often only occurs after damage is done, making it critical that we utilize red team tools on a regular basis, allowing us to test, identify issues quickly, automate scans, and promptly notify teams to address fixes.

"The best features that Kali Linux offers stand out because it is built out of offensive security and blue team validation. It is not only about red team tools but also includes a massive security tool set, boasting over 600 plus tools available via Kali Linux, which we utilize for recon, scanning, exploitation, penetration testing, among others, with various tools such as clients that we can run, along with Metasploit, Burp Suite, SQLMap, Aircrack, Reaver, Hashcat, Hydra, and others to test different scenarios.

"Out of all those tools and capabilities, my favorite tools in Kali Linux that I find myself relying on the most are Burp Suite, which I frequently use, and based on Burp Suite issues, I can start the recon and then proceed to exploit using Metasploit or SQLMap, which are the second steps I take.."

Suresh A.
Senior AIML Engineer at a tech vendor with 1,001-5,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"I think the plethora of tools that come built-in with Kali Linux is really helpful. There are a lot of categories which it provides, starting from reconnaissance to exploit. Since all of them are already built-in, I don't have the necessity to go and install every single one of them. Kali Linux has a really good suite of tools already built-in, which is one of the best features that comes to my mind.

"I would definitely say the reconnaissance-based tools are my favorite in Kali Linux. There are a lot of reconnaissance tools available. Outside of that, I also use Metasploit and other exploitation tools. However, it predominantly lies with reconnaissance and exploitation.

"One feature I found cool was that you can disguise Kali Linux as just another operating system, such as Windows, when you are using it outside.

"A good amount of time is saved when it comes to scanning and reconnoitering infrastructure with Kali Linux.

"Kali Linux has a variety of tools and a variety of word lists present, which makes it a lot easier to choose between options. For example, for subdomains, there are a bunch of them. Particularly for finding the fields of requests, there are many options. All of this makes it easier rather than going to the web to search for a particular list and curating the list for a particular thing. In that case, I would say it is saving me a good amount of time.."

Validated user

Read full review

Associate Cybersecurity Analyst at a university with 10,001+ employees

©2026 PeerSpot, All Rights Reserved

Other Solutions Considered

"I previously used Linux, but the tools which I required for the VAPT part did not get pre-installed in that. I switched back to Kali Linux, as it was also suggested by my peers to use it.."

Validated user
Security Researcher at a tech vendor with 10,001+ employees

Read full review

"Before choosing Kali Linux, I evaluated other options such as Arch Linux and Parrot OS. I compared these three platforms and then chose Kali Linux. I think it is the best.."

Validated user
Security Researcher at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

"We evaluated alternatives to Kali Linux, including Parrot OS, BlackArch, BackBox, and the Network Security Toolkit (NST), but Kali Linux was chosen for its stability, open-source nature, and strong community support.."

Gaurav Pratap Singh
SWE-1 at a tech vendor with 10,001+ employees

Read full review

"Kali Linux is my first distribution for security in Linux. I tried other distributions, but I always stick with Kali Linux. It was the first that I knew and the one that I always use.

"I did not evaluate other options. I selected Kali Linux because it was the first one that showed me the right direction for security testing.."

Guillermo Buritica Tobon
Consultant at Cognizant

Read full review

©2026 PeerSpot, All Rights Reserved

"We use a variety of other tech products, including a bunch of AWS services, CrowdStrike, Rapid7, Trend Micro, Datadog, Axonius, Splunk, and several others.

"I am interested in analyst insights about other solutions.."

Suresh A.
Senior AIML Engineer at a tech vendor with 1,001-5,000 employees

Read full review

"Before Kali Linux, I was using a Debian operating system and I also tried Parrot OS. I found Parrot OS a little bit flashy. Kali Linux is more calm and composed. That is why I switched to Kali Linux. I still appreciate Debian, but it does not have the tools. If I'm getting a fresh operating system, I would still prefer Kali Linux.."

Adarkum Kumar
Product security engineer at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

ROI

Real user quotes about their ROI:

"I would say I have seen a return on investment in time saved, for sure. For metrics, I do not find any metrics apart from the learning that I have done.."

Adarkum Kumar
Product security engineer at a tech vendor with 10,001+ employees

Read full review

"I have seen a return on investment with Kali Linux, particularly in terms of needing fewer employees and the time saved, especially securing the business and protecting customer data.."

Suresh A.
Senior AIML Engineer at a tech vendor with 1,001-5,000 employees

Read full review

"There is no investment involved because I am using the product on my laptop, so there is no return on investment. The return on investment is having all the tools readily available without any cost.."

Guillermo Buritica Tobon
Consultant at Cognizant

Read full review

©2026 PeerSpot, All Rights Reserved

"I save around eight hundred to nine hundred dollars monthly by using Kali Linux. This is because the equivalent on-market tools have quite hefty charges. They are private and require a paid subscription to use. In Kali Linux, similar open-source tools are available for the same purpose.."

Validated user
Security Researcher at a tech vendor with 10,001+ employees

Read full review

"I have seen a return on investment with security improvements since using Kali Linux, and money saved because it is an open-source tool and free to use. There are no financial costs needed upfront, other than maybe if I am booting it from a USB, I might potentially need to buy that USB. The money saved from using Kali Linux means if I am able to make my applications more secure, I could easily see financial improvements.."

Validated user
Cloud Ops Lead at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

"Kali Linux has provided a very good return on investment. When we needed training for employees, we wanted 20 or 30 instances of Kali Linux. The availability on AWS Marketplace was helpful for us to spin up the VMs and deploy them readily. Once the need was over, we removed the instances, saving costs. If we had installed it on-premises or through other means, it would have incurred significant money and effort to create the VMs, deploy it on machines, and then delete and format it after use. The fact that it was available on public cloud helped us achieve about an 85% return on investment.."

Mathews Daniel

Cloud Security Architect at a tech services company with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

Use Case

"Kali Linux serves as the base OS across all my cloud environments. A typical task or project where Kali Linux plays a key role is that I have designated it as the base OS, which is the underlying operating system I use for all my cloud-native applications, with Kali Linux running across all the cloud nodes used for cloud-native products.."

Suresh A.
Senior AIML Engineer at a tech vendor with 1,001-5,000 employees

Read full review

"My main use case for Kali Linux is for reconnaissance and VAPT purposes like ethical hacking, and when I have to go through long scripts running to scan the targets. For reconnaissance or VAPT, a quick specific example is that for subdomain enumeration, I use tools such as Subdomainer and Sublist3r in Kali. Sometimes I also use Nuclei templates for the automation purpose of the VAPT process.."

Validated user
Security Researcher at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

“My main use case for Kali Linux is whenever there's an open-source or free tool to use with an API and Python that I need to utilize. I prefer Kali Linux because it has a Linux environment and numerous open-source tools that work and are compatible with Kali Linux.

“A specific example of how I've used Kali Linux in my work is that it has many offensive security tools. The last time I used it was when I was preparing for my OSWA exam, where I used the terminal extensively to probe the labs provided to me in the OSWA certification exam.

“I also use Kali Linux as my go-to operating system. My main operating system on my personal laptop is Kali Linux, and for my office use case, I have Kali Linux set up in a VM..”

Adarkum Kumar
Product security engineer at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

"I have been using Kali Linux for almost three to four years now.

"I use Kali Linux for penetration testing purposes as well as red teaming activity. I also use it for solving machines in Hack The Box or TryHackMe.

"There is a particular machine in Hack The Box which requires you to connect to their machines and perform reconnaissance as well as identify vulnerabilities in the system and exploit them in order to get the flags. That would be my recent use case.

"For my coursework, which was a long time ago, I used Kali Linux for vulnerability scanning.."

Validated user

Associate Cybersecurity Analyst at a university with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

"I use Kali Linux for vulnerability testing, sandbox analysis, red team penetration testing, and checking vulnerabilities in the network, checking vulnerabilities with users, and red teaming proactive penetration testing.

For penetration testing or vulnerability analysis, we have a website, and for conducting vulnerability analysis of the website, we use Metasploit and SQL injection to identify vulnerabilities. We also use Netmon and Nmap to see network-related vulnerabilities. Additionally, we use John the Ripper for password-related issues. There are different tools that we use for different purposes.

Kali Linux provides a secure environment for sandbox analysis and control testing, and most of the tools are free and open source, so we do not need to pay charges. It saves on costing, and because it is Linux-based, it provides a secure environment where we can conduct testing in our DMZ. If we are testing or analyzing malware, we need to use either Flare VM or Kali Linux. The testing is conducted in a controlled manner, and Kali Linux provides in-house tools for that. We do not need to go to the internet for the analysis.."

M Pathak

Securuty solution architect at a tech services company with 11-50 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"The main use case for Kali Linux is to test my own applications to ensure that they are secure, so I have pursued ethical hacking for my own applications.

"I typically set up tests by using tools which are out of the box in Kali Linux such as Nmap for port scanning, and for the applications that I build, I am trying to identify the underlying hardware that they are running on, checking for any open ports which could introduce security vulnerabilities into my application. I also have sent packets to my web applications that I built previously, such as a website that I self-host, and I use Wireshark for packet analysis to see if I can understand information about the request, such as where it is coming from.

"From using Nmap for port scanning, I have probably identified about 10% security improvements in my own applications just by closing ports which I did not realize were open but did not need to be.."

Validated user

Cloud Ops Lead at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

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.

"For licensing, we do not require any. For a small team, we do not need any licensing. We can directly install Kali Linux. It is open source. We can install it on our system and it is ready to use. All the tools come with it, so we do not need to do any complicated tasks. It is better.."

Validated user

Read full review

Security Researcher at a tech vendor with 10,001+ employees

"The product's initial setup phase was straightforward.

One just needs to create a bootable drive to install the product.

The solution is deployed on an on-premises model.."

Validated user

Read full review

Solutions Engineer at a tech services company with 1,001-5,000 employees

©2026 PeerSpot, All Rights Reserved

"I purchased Kali Linux through the AWS Marketplace. My experience with pricing, setup cost, and licensing for Kali Linux has been good. The pricing and the deployment, resource usage are all spot on and clearly defined, making it helpful and useful for me to deploy and calculate costs.."

Mathews Daniel

Cloud Security Architect at a tech services company with 10,001+ employees

Read full review

"The initial setup of Kali Linux is okay—not pretty complex or very simple.

"It could be simplified from Kali's side for a GUI user, but if we are doing it as command mode, it is okay. We don't find it very hard to install or pretty complex.

"For a regular user, they might find it complex. For the technical staff, it's not very complex.."

NilutpalDutta

Senior Technical Manager at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

“From my perspective, I can set up Kali Linux with information gathering, vulnerability analysis tools, and application analysis tools. I'm able to configure those.

However, now many people are interested in cybersecurity. So, I suggest that Kali Linux should improve things like the GUI interface, make it easier to use, and include a training portal that's easier for basic users to understand.

I use it sometimes on-premises and sometimes on the cloud.

Sometimes the setup takes only one hour, no more than that. But if we start getting errors, then it can take four to five hours to complete the setup of Kali Linux..”

Rohit Srivastava

IT Manager at PRATHAM SOFTWARE PRIVATE LIMITED

Read full review

©2026 PeerSpot, All Rights Reserved

"Most often, we use Hydra, Nmap, John the Ripper, Metasploit, and Wireshark. Those are the tools that we use most.

Among the 30 plus tools, the most that we use are Nmap, Wireshark, John the Ripper, Hydra, Metasploit, and a few more for SQL injection and sandbox analysis. Each tool has their own capabilities. We can install tools if we want. We can use the GitHub repo to install tools. There are a number of tools available.."

M Pathak

Securuty solution architect at a tech services company with 11-50 employees

Read full review

©2026 PeerSpot, All Rights Reserved

Customer Service and Support

"I have never interacted with customer support for Kali Linux before, but I imagine if support was needed, it would be very good because their documentation is good.."

Validated user
Cloud Ops Lead at a tech vendor with 10,001+ employees

Read full review

"The customer support for Kali Linux is good. Since most of the tools and other things are community-based, the documentation and other community support are very good.."

Mathews Daniel
Cloud Security Architect at a tech services company with 10,001+ employees

Read full review

"There is no customer support available for Kali Linux, so I have no comment on that aspect. However, I hope that customer support should be provided in the future, though I have never attempted to use it.."

Ciyagi Ciyagi
Senior Solution Architect & Delivery Lead at a tech services company with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

"It is an open-source tool, so we do not have the functionality to raise a case. However, it has a nice community. If we compare support from Microsoft, it is not the same because Kali Linux is open source and we are not paying any license cost. Customer support is there, but documentation and community have a strong base behind that.."

M Pathak
Securuty solution architect at a tech services company with 11-50 employees

Read full review

"I have not used the customer support for Kali Linux, but I have searched extensively on Stack Overflow and Kali forums. That was very helpful because most of the issues I faced were already mentioned in one of those forums, and I was able to solve the problems I was experiencing.."

Adarkum Kumar
Product security engineer at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

“I tried to connect to customer support through email, but I received responses very slowly. In those situations, I do my own research and development to fix those particular errors.

For their understanding of the errors and providing solutions, I'd give them a ten out of ten. But about response time, I'll give it a five because it's very slow..”

Rohit Srivastava
IT Manager at PRATHAM SOFTWARE PRIVATE LIMITED

Read full review

©2026 PeerSpot, All Rights Reserved

Other Advice

"If you want to use Kali Linux, my advice is to explore other options, compare them, and then know your needs before choosing Kali Linux. If you are looking for faster, better performance or scalability, then Kali Linux is the best. If you want a better GUI or something else, then you can go for Arch or Parrot OS. Those operating systems are also in the market. However, the benefit Kali Linux provides and its community is also good, so Kali Linux is far better than others. I have given this review a rating of eight point five out of ten.."

Validated user
Security Researcher at a tech vendor with 10,001+ employees

Read full review

"My advice to others looking into using Kali Linux is that it is a good security tool.

"I have shared all valuable information, so I have no additional thoughts about Kali Linux.

"I found this interview to be conducted well, and you are doing good.

"I would appreciate a short poem or haiku that summarizes my review. I give this review a rating of five out of five.."

Suresh A.
Senior AIML Engineer at a tech vendor with 1,001-5,000 employees

Read full review

"Kali Linux is the only solution for cybersecurity if we are conducting pen testing

©2026 PeerSpot, All Rights Reserved

or anything related to it. We cannot bypass Kali; we cannot ignore Kali. If we want a secure environment, we have to include Kali in our pen testing and all vulnerability analyses.

I give it a 10 because if we go in the market, we will not find any operating system with such a compact package. We will see Flare VM, but Flare VM is only for malware analysis. Every tool is based on the MITRE framework, and every tool is doing its own work. If we want to purchase something with the same functionality from other vendors which are not open source, we have to pay a high cost. It is cost-effective, highly secure, and it has proven its capabilities. I rate this product 10 out of 10 because it is the Bible for a cybersecurity expert. Without Kali Linux, we cannot do anything in cybersecurity. If we want to begin our career, Kali Linux is our first step.."

M Pathak
Securuty solution architect at a tech services company with 11-50 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"I cannot speak for the organization as a whole, but Kali Linux is used quite a lot in my team, and particularly by me. It does help me to increase my pace when it comes to the reconnaissance process and also while solving machines in Hack The Box.

"Kali Linux is a very good tool and a good overall operating system to use when it comes to penetration testing, as it has a wonderful set of tools. You just need to search for the right tools within it because it offers a plethora of tools. It might be a good way to start identifying what the tools are best suited for your environment and what your needs are.

"I have not had to get back to them anytime regarding support for Kali Linux. My overall rating for this product is nine out of ten.."

Validated user
Associate Cybersecurity Analyst at a university with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

"Out of all those built-in tools and features, I find myself using Wireshark quite a lot for packet analysis, and I have tried to bombard my web application with a large number of packets. I then use Wireshark to examine information regarding those packets, such as the geolocation of where they have come from and how many packets per second are trying to hit the application. I found that quite useful, especially when I am trying to understand the scalability and elasticity of my application. I also use cloud monitoring tools such as Grafana and built-in tools with Google Cloud in combination with Wireshark, which enables me to analyze packets and scalability from different angles.

"My advice to others looking into using Kali Linux is to go ahead and use it because it is free. I can download it and give it a try, and there is a lot of advice online about how to use it. I rate this product a 10 out of 10.."

Validated user
Cloud Ops Lead at a tech vendor with 10,001+ employees

Read full review

"Kali Linux has helped me with my learning and experimentation by allowing me to do many CTFs when I was learning to go into the offensive security side or doing penetration testing. There, I learned many probing attacks, such as HTTP probe, and then there is the Gitrob tool. Many of the offensive security tools that I used were in Kali Linux. The best part is automating it through the CLI. The CLI is the one feature that I have used the most in Kali Linux.

"The most significant benefits I have experienced since using Kali Linux for my personal or professional work are the hands-on capabilities that we use on the tools at every stage of probing a website. This includes everything from reconnaissance to active attacks, passive attacks, and then trying to use Burp Suite, which is a proxy tool. That is where I find it the most useful. Getting accustomed to the terminal gives you a different feeling than using the GUI.

"Kali Linux stands out compared to other operating systems I have used for

©2026 PeerSpot, All Rights Reserved

security work because it is a specific distribution of Linux that has all the required tools pre-loaded and configured. Python is already configured with the correct path variable, Java is installed already, and Go is pre-loaded. These are features that every offensive security software or operating system needs. If I'm using Windows and trying to attack a website, I have to manually install those programming languages that I will be writing scripts on, and then declare the path variables. That makes it more tedious than how Kali Linux works. Additionally, I can run multiple threads in Kali Linux, and the operating system is still able to support the performance, compared to Windows, which will lag or freeze if given multiple processes to run.

“My advice for others looking into using Kali Linux is to first understand the basics of Linux, then understand how the Linux terminal works, and only after that should you dive into Kali Linux. If Kali Linux is the first operating system you are using in a Linux environment, you might become confused. Many of the features do not have a graphical user interface, so you will need to be more accustomed to the terminal.

“Kali Linux is a great operating system. I appreciate it because it offers a diverse range of tools. I do not think I have ever used all the tools that are pre-provided in the operating system. An option to choose what different kinds of attacks you are using so you can streamline the software that you are downloading would be beneficial. If I need something for an active attack, that would be a different stream of tools that should be pre-loaded, compared to passive kinds of attacks. That could be a major upgrade or option for choosing at the time of download. You could get a lightweight operating system, and if needed, you can always download those tools later. Overall, I found this product to be valuable for my security work..”

Adarkum Kumar
Product security engineer at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

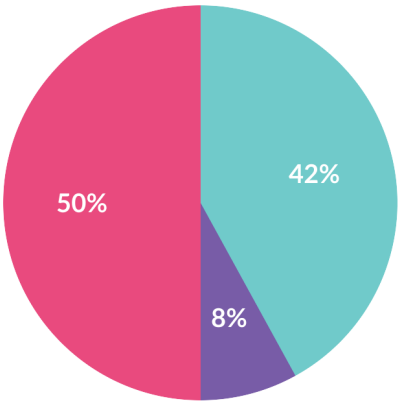
Top Industries

by visitors reading reviews

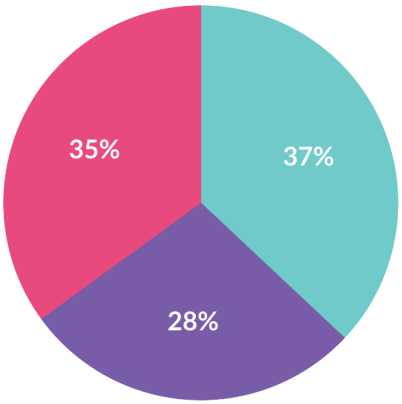
Comms Service Provider	12%
Construction Company	11%
University	10%
Educational Organization	7%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

©2026 PeerSpot, All Rights Reserved

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

©2026 PeerSpot, All Rights Reserved

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

©2026 PeerSpot, All Rights Reserved