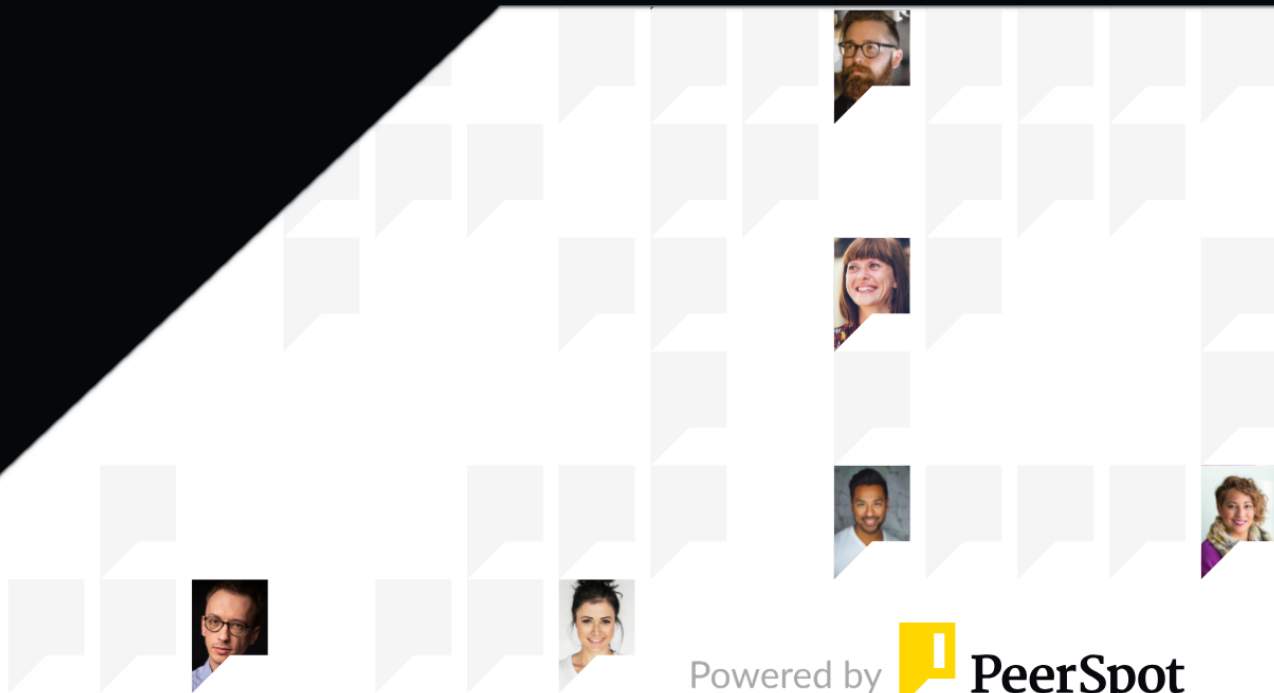


aws marketplace

Picus Security

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 8

Other Solutions Considered..... 9

Use Case..... 10 - 11

Setup..... 12 - 13

Customer Service and Support..... 14 - 15

Other Advice..... 16 - 18

Trends..... 19 - 20

About PeerSpot..... 21 - 22

Product Recap



Picus Security

Picus Security Recap

Picus Security runs the Picus Autonomous Exposure Validation Platform, which proves what attackers can actually exploit across your hybrid and cloud environments and what your security controls stop. Picus unifies breach and attack simulation, automated penetration testing, and exposure validation into one continuous loop, so teams act on real exploitation risk instead of severity scores.

As adversaries weaponize new CVEs in hours, Picus validates your attack surface, exposures, and security controls together, then re-validates after every change. It works across on-premises, cloud, and hybrid infrastructure and connects to the tools you already run through an open ecosystem of 75+ integrations, including EDR, SIEM, firewall, SOAR, and ticketing systems.

What are the key capabilities of Picus Security?

- **Breach and Attack Simulation:** Continuously test EDR, SIEM, and firewall controls against the latest adversary techniques to see what they block, detect, and miss.
- **Automated Penetration Testing:** Execute real exploit chains to prove which vulnerabilities an attacker could actually reach and exploit.
- **Exposure Validation:** Determine whether a CVE is exploitable in your environment, including on business-critical or restricted systems a live exploit cannot safely touch.
- **Security Control Optimization:** Close gaps with ready-to-deploy signatures and rules, then re-validate that the gap is closed.
- **MITRE ATT&CK coverage:** 25,000+ TTPs and 5,700+ threat scenarios mapped to MITRE ATT&CK.

What outcomes can users expect?

- Prioritize remediation by real exploitation risk, and deprioritize what controls already block.
- Prove control effectiveness and report measurable risk reduction to leadership with evidence.
- Raise the return on the security tools you already own before buying more.

Organizations in financial services, healthcare, energy, and technology use Picus to validate security continuously across hybrid and cloud environments.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“The most valuable feature of the solution is its integration capabilities with the other security tools.”



Kateryna Andrushchenko

Information Security System Manager at CS-Consulting



“It provides good reports and offers signature-based solutions.”



AkashDeshpandey

Cyber Security Consultant at GBS IT Services



“One of the most valuable features would be the detection capability, specifically the ability to detect alarms and logs collected from SIEM tools.”



Mauro Restante

Cybersecurity Customer Service Manager and Technical Account Manager at Cybersel



“It's very useful software because the customer mostly configures their IPS and manages their firewalls, WAF, and the DBS according to the latest update, latest news, or according to the situation.”



erdemerdag

Cybersecurity Operations Engineer at a tech services company with 201-500 employees



“You have the liberty of physically executing a specific set of rules in your environment.”



Taha Hussain

Solutions Architect Cybersecurity at a tech vendor with 11-50 employees



“The most valuable feature of Picus Security is its threat intelligence, providing suggestions to block and prevent attacks by identifying malicious files and providing threat IDs.”



Verified user

Security Engineer at a tech services company with 201-500 employees

What users had to say about valuable features:

“One valuable feature of Picus Security is security control validation. It provides good reports and offers signature-based solutions. I can simulate an attack into a live environment, testing whether my controls are operational and able to stop or mitigate attacks..”

AkashDeshpandey

Cyber Security Consultant at GBS IT Services

[Read full review](#) 

“It's very useful software because the customer mostly configures their IPS and manages their firewalls, WAF, and the DBS according to the latest update, latest news, or according to the situation. Sometimes they miss a configuration, but they aren't aware of it. Picus gives the wheel to the customer because they are using the real payloads, real attack, and real simulation, but not to the production servers or simulation servers. That's why it's not damaging the customer's reports. But they can see the current situation of their product.

It's a complete solution, so they have network vectors, endpoint vectors, and email vectors. They provide almost a complete solution..”

erdemerdag

Cybersecurity Operations Engineer at a tech services company with 201-500 employees

[Read full review](#) 

“The list of vulnerabilities that get detected is the most valuable feature. The list of injections, basically that we identify within the infrastructure is the most valuable one, as they can see which attack has actually been successfully executed in their environment. You can navigate through different options on the product and you can do exercises. One of the beneficial features is that if you do not want to perform a specific set of attacks, you can uncheck them. Alternatively, if there are certain attacks that you want to execute, you can do that as well. You have the liberty of physically executing a specific set of rules in your environment. For example, let's say the customers don't have Apache servers. If there are any vulnerabilities or injections that are performed on Apache servers, a lot of tools rely on those rules. Customers can basically uncheck those injections that are performed on servers that do not exist in their environment..”

Taha Hussain

Solutions Architect Cybersecurity at a tech vendor with 11-50 employees

[Read full review](#) 

Other Solutions Considered

“We chose this solution because there are not many options for a Turkish company.

We are very familiar with the dashboards, managers, and salespeople. We have a very close relationship with them..”

erdemerdag

Cybersecurity Operations Engineer at a tech services company with 201-500 employees

[Read full review](#) 

“If you're opting for cloud services, you are exposing your results to the internet. It's of paramount importance that customers, especially government organizations protect the data of their consumers and their own employees. They end up using the services, and we know there have been a lot of breaches in the major cloud providers as well. There have been breaches at Amazon, Oracle, and Microsoft previously. For this type of activity, I would personally recommend an on-premise solution where you would have entire control of the attacks, as well as the results that you see. If you are testing your infrastructure where you want to develop something, or there are some financial and transition servers, which store your critical data, and you are assessing that network, I wouldn't recommend using a cloud-based SaaS offering from Picus. However, let's say you have a non-critical or a non-confidential network, where you want to assess those servers, applications and network, then, in that case, I would definitely recommend that you use a cloud SaaS offering also..”

Taha Hussain

Solutions Architect Cybersecurity at a tech vendor with 11-50 employees

[Read full review](#) 

Use Case

“I can simulate an attack into a live environment and test whether my controls are working properly. It checks if the controls can stop and mitigate the attacks..”

AkashDeshpandey

Cyber Security Consultant at GBS IT Services

[Read full review](#) 

“Picus Security is used for BAS, helping companies test their network security layers by simulating attacks from the cloud. It installs an agent behind the firewall to assess security configurations and policies, enabling both blue teaming and red teaming scenarios. Additionally, it provides prevention measures like URL bypass blocking to enhance firewall security..”

Verified user

Security Engineer at a tech services company with 201-500 employees

[Read full review](#) 

“We engage with customers in the Middle East to check the visibility of the use cases that we create, using the Picus solution. We want to check the strength of their infrastructure, their application servers. This is the type of integration exercise we do for our customers. We check if there are any loopholes or weak links that can be hardened using a visibility tool, of course like Picus Security. Customers in the Middle East are concerned about cloud solutions, the data or software component has to reside within their premise or at least inside the boundaries of this country. The majority of them prefer the on-premise solution, and sometimes we use cloud-based solutions as well. When using the cloud they have a SaaS service available and it's hosted on Amazon cloud. .”

Taha Hussain

[Read full review](#) 

Solutions Architect Cybersecurity at a tech vendor with 11-50 employees

“Picus Security is a breach and attack simulation software. It has a dictionary attack. According to your peers and attack vectors, it's trying to attack with the files. It also has some lateral movement attacks. They need to install or configure the peers or attack vectors so we can support it.

The solution updates almost daily because the dictionary updates. The latest version is 4273. We have some customers using the on cloud platform. We also have some military customers who are using the on-prem solution.

The system managers or administrators are managing this product, so I don't have a specific number of clients that are using the solution..”

erdemerdag

[Read full review](#) 

Cybersecurity Operations Engineer at a tech services company with 201-500 employees

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

“The initial setup is very simple. I would rate my experience with the initial setup a nine out of ten, with one being difficult and ten being easy.

With the next generation platform, the setup was quite straightforward..”

Mauro Restante

[Read full review](#) 

Cybersecurity Customer Service Manager and Technical Account Manager
at Cybersel

“Installing and deploying Picus Security is relatively straightforward, with a simple process outlined in the documentation. It involves adding process names to run the agent and allowing domain features on the firewall to stimulate attacks, but overall, there are no significant challenges..”

Verified user

[Read full review](#) 

Security Engineer at a tech services company with 201-500 employees

“The installation is straightforward, but the configuration is sometimes complicated because it's up to the customer. They have to decide the scenario or the vectors because they have some different segments in their network. They have the cloud site, they have the MV site, and they have some segmentations on the internal networks. They have to decide how to design the infrastructure, so it takes some time and extra effort to deploy..”

erdemerdag

[Read full review](#) 

Cybersecurity Operations Engineer at a tech services company with 201-500 employees

“It was straightforward, It's not complex. There is good documentation and they provide immense support from the company. A lot of customers find it easier if you demonstrate to them what needs to be done. If you point the customer to the correct part of the documentation, the majority of the customers would be able to take care of the solution themselves. They would be able to do the initial setup as well..”

Taha Hussain

[Read full review](#) 

Solutions Architect Cybersecurity at a tech vendor with 11-50 employees

Customer Service and Support

“I had to contact the technical support team of the product once, but the problem was in our company's environment. The response from the support team was nice.

I rate the technical support a ten out of ten..”

Kateryna Andrushchenko

Information Security System Manager at CS-Consulting

[Read full review](#) 

“It can be challenging to reach Picus Security's support team due to time differences, as support mainly comes from the US and UK, even though deployment support is provided locally in India. Improving the support team presence could enhance customer satisfaction and impressions..”

Verified user

Security Engineer at a tech services company with 201-500 employees

[Read full review](#) 

“Picus Security is aggressively trying to acquire at least one customer so that it becomes a reference for the other customers. We haven't had any issues with support, whether it is a presale, sales or technical support. Every time we reached out to them, a resource was quickly assigned to us..”

Taha Hussain

Solutions Architect Cybersecurity at a tech vendor with 11-50 employees

[Read full review](#) 

Other Advice

“On a scale of one to ten, I would rate the solution ten out of ten. However, the only area that would need improvement is the response time from customer support..”

AkashDeshpandey

Cyber Security Consultant at GBS IT Services

[Read full review](#) 

“I recommend starting with a few risk factors and gradually expanding the platform's usage. Begin with evaluating risks from different perspectives, like from the firewall to data loss prevention. Starting small allows for better management of data and a smoother experience.

Considering what I know about other platforms in the market, I'd give Picus Security an eight..”

Mauro Restante

Cybersecurity Customer Service Manager and Technical Account Manager
at Cybersel

[Read full review](#) 

“As far as the implementation is concerned, you definitely need to evaluate our own infrastructure first. I see a lot of customers installing the agents at an inappropriate place. For example, let's say we want to initiate an attack from the Picus cloud to somewhere inside your own network. You need to access and ensure that the traffic is going through every security device you're evaluating. Customers frequently install agents at a place which doesn't cover all the security devices. There is a need to ensure that traffic is going through all the security devices..”

Taha Hussain

Solutions Architect Cybersecurity at a tech vendor with 11-50 employees

[Read full review](#) 

“Picus Security has been implemented in our organization to enhance threat detection by allowing us to test some of the other security tools in our company.

I recommend the product to others who plan to use it.

The tool has not had an impact on our company's overall security posture since the time of implementation since we just used it for some testing purposes, during which it did show some interesting results.

I rate the overall tool a nine out of ten..”

Kateryna Andrushchenko

Information Security System Manager at CS-Consulting

[Read full review](#) 

“Picus Security's continuous validation feature offers predefined attack templates and over ten thousand simulations. Users can see how well their security solutions prevent attacks on endpoints and receive suggestions for improvement. This helps

enhance overall security measures.

Integrating Picus Security with existing security tools and workflows isn't straightforward as it requires manual installation of the agent, rather than seamless integration with other products.

For new users, my advice is to leverage Picus Security for simulation and prevention purposes, as it is considered one of the best options in both European and Asian countries.

Overall, I would rate Picus Security as a nine out of ten..”

Verified user

Security Engineer at a tech services company with 201-500 employees

[Read full review](#) 

Top Industries

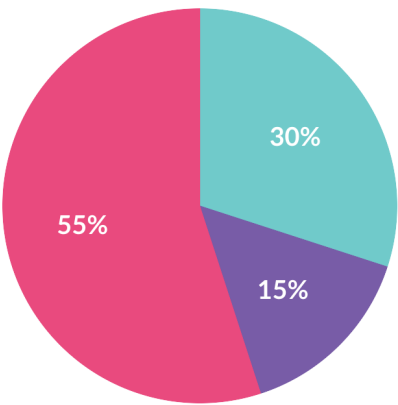
by visitors reading reviews



Company Size

by reviewers

by visitors reading reviews



Large Enterprise Midsized Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

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

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

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

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

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

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

[Get your personalized report here](#)

About PeerSpot

PeerSpot is the leading review site for 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