aws marketplace

One Identity Safeguard

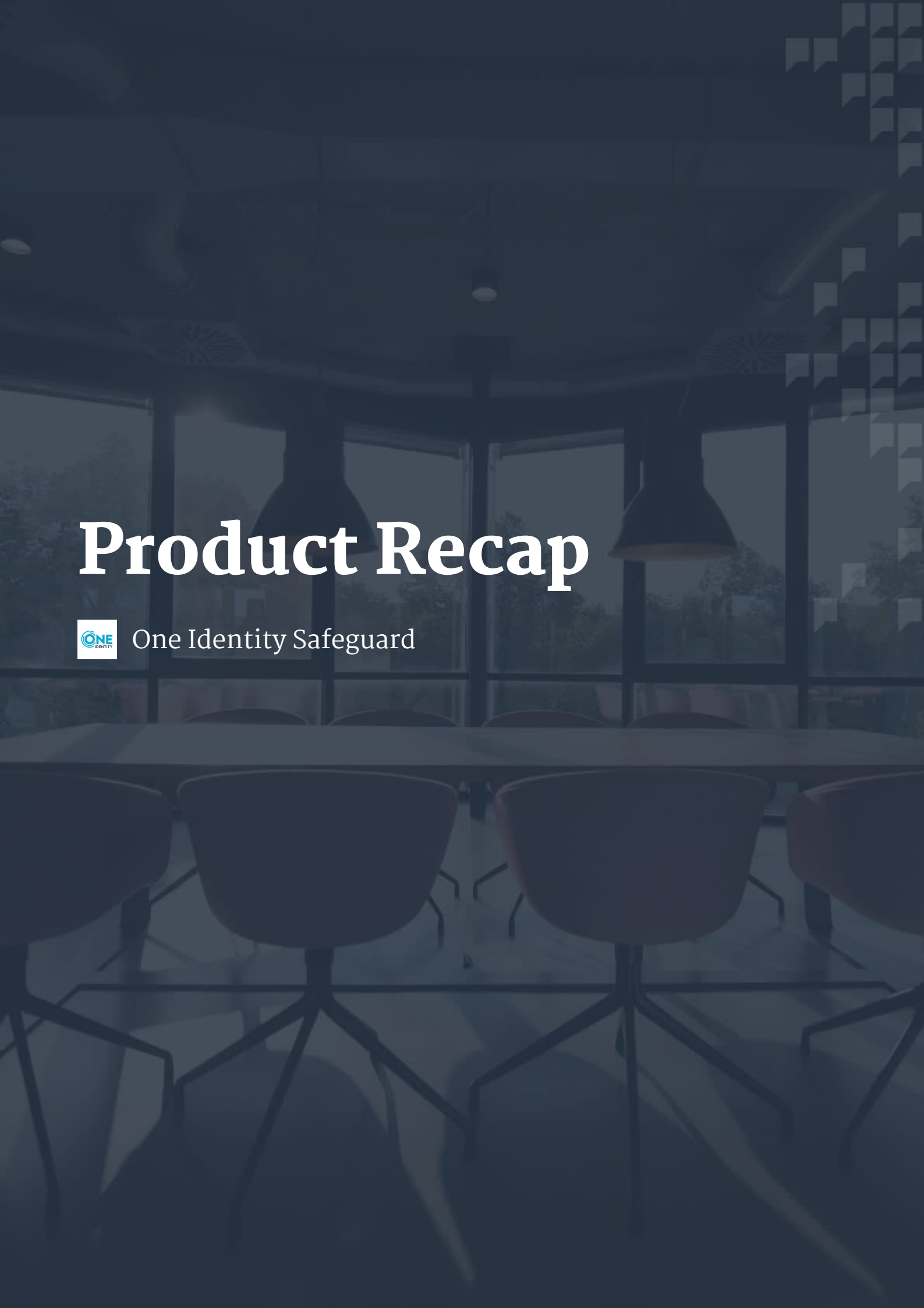
Reviews, tips, and advice from real users






Powered by PeerSpot

Contents



Product Recap

One Identity Safeguard

One Identity Safeguard Recap

One Identity Safeguard manages and monitors privileged access, enhancing security with features like automatic session recording, real-time monitoring, and credential rotation. It integrates seamlessly, supports compliance with audit trails, and improves operational efficiency across organizations. This robust platform significantly bolsters security protocols while controlling sensitive operations.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "With One Identity Safeguard, we have seen clear, measurable improvements across security, operations, and compliance."

Mahesh Malve

Senior business development executive at DigitalTrack solution ind pvt ltd

- "The integration of One Identity Safeguard has had a clear positive impact on both security and operational efficiency, with earlier estimates showing thirty to forty percent fewer password-related tickets and fifty percent faster audit preparation, along with reducing risk and eliminating shared credentials."

Prithviraj kallurkar

Business Development Executive at Digitaltrack solutions

- "One Identity Safeguard, in my experience, has had a significant positive impact on our organization, especially in terms of security, efficiency, and compliance."

Nikita Bhojwani

Senior Business Development Executive at Digitaltrack Solutions Private Limited

"Since using One Identity Safeguard, we have more control over who accesses what, especially regarding vendors, and we have seen billing actually go down because we now know how long vendors have been on the server and how long they have worked on it."

Sindre Toft

Senior Information Technology Consultant at Helse Nord IKT

"I have seen a clear return on investment with One Identity Safeguard, reducing manual effort for access management by around thirty to forty percent, decreasing audit preparation time by nearly fifty percent, and lowering the risks of costly incidents through improved security controls."

Ahitesh Anumala

Business Development Manager at Digitaltrack Solutions Private Limited

"Overall, my experience with One Identity Safeguard has been very positive, as it is a reliable and secure privilege access management solution that effectively protects sensitive accounts and provides full visibility into administrator activity, with minor improvements needed in terms of UI and reporting enhancements."

Prathamesh Pawar

Technical Support Engineer at Digitaltrack

"I give it an eight because of its robust security features, its splendid automated password management, and real-time activity monitoring that stood out to me."

Aryan Priyanish D.

Developer Intern at Stealth

What users had to say about valuable features:

“One key benefit of my main use case with One Identity Safeguard is that it helped me eliminate shared admin credentials, which was a major security risk earlier. Now, every access request is tracked and tied to an individual user, improving accountability. It also simplified audits by providing clear session records, which solved a big challenge I previously faced with compliance visibility.

“The best features One Identity Safeguard offers include credential injection, session monitoring, and role-based access control. Credential injection ensures passwords are never exposed to users, improving security, while session monitoring and recording provide full visibility and an audit trail of activity. Role-based access helps enforce a least privilege policy, and additional features such as real-time alerts, reporting, and integration with other systems make it a comprehensive solution for managing and securing privilege..”

Ahitesh Anumala
Business Development Manager at Digitaltrack Solutions Private Limited

Read full review

The best features One Identity Safeguard offers are out-of-box templates, which simplify password rotation workflows and have a nice interface. It is also pretty stable.

The out-of-box templates from One Identity Safeguard make onboarding much easier for my team in day-to-day work.

“One Identity Safeguard's automation of password management and incident investigations has cut manual efforts significantly.

“One Identity Safeguard has positively impacted my organization by improving compliance, posture, and audit capabilities. It has cut manual efforts by 30 to 40% via automation and also decreased privileged account incidents by up to 40%. .”

Swapnil Karkala
Senior Frontend Developer at HCl

Read full review

"The best features One Identity Safeguard offers include secure and controlled access along with real-time session controlling.

"The real-time session control feature helps me in my daily tasks by providing session controlling and monitoring in user sessions that occur, allowing proactive management across web and platform access instead of reacting after something goes wrong.

"Session monitoring and recording are also crucial parts of the features.

"One Identity Safeguard has a noticeable positive impact around security and operational efficiency, providing secure, strong security, real-time monitoring, and full visibility.

"Operational efficiency has improved as it requires less manual effort for the IT team and makes troubleshooting easier.."

Nitin Yadav
Network & Security Engineer at Arrow PC Network Pvt Ltd

Read full review

"The best features of One Identity Safeguard mainly revolve around strong security, visibility, and control over privileged access. One of the most valuable features is its password management, where sensitive credentials are securely stored, automatically rotated, and accessed only through a controlled workflow, reducing the risk of misuse. Another standout feature is session monitoring and recording, which captures every action taken during privileged sessions.

"The session monitoring and recording feature in One Identity Safeguard has been extremely valuable for our team, especially from a security and compliance perspective. We use it quite regularly whenever an administrator accesses critical systems. Every privileged session is recorded in detail, covering screen activity, commands executed, and user behavior, so we have a complete audit trail. This has helped us quickly investigate incidents, verify actions taken on sensitive systems, and ensure that all activities follow internal policies.

"One Identity Safeguard has had a very positive impact on our organization, especially in terms of security, efficiency, and visibility. It has helped us centralize and control privileged access and provided a structured secure approach. As a result, we now have much better visibility into accessing credentialed systems and the actions performed, which has improved accountability and compliance.

"One Identity Safeguard has significantly improved accountability and compliance by giving us complete visibility of all privileged activities. Every access requires approval, and a session is logged and recorded, which means we always have a great audit trail of who accessed what and when. This has made internal and external audits much smoother, as we can quickly provide evidence without manually tracking.."

Twinkle
Business Development Executive at Digital Track Solution pvt ltd

Read full review

"The best features of One Identity Safeguard revolve around password security, session control, and governance. Some of the features I can mention are privileged password vault and automatic rotation, session recording and playback, real-time monitoring and threat blocking, just-in-time privileged access, and privileged session search.

"The session recording feature is straightforward in day-to-day use. When an admin launches the RDP session or SSH session through One Identity Safeguard, the system automatically records everything in the background with no extra steps needed. It captures screen activity, commands executed, keystrokes, login-logout times, and target systems accessed. After the session, I can search by username, server name, date, time, and request ID. Real-time monitoring is also useful, especially for high-risk systems. Security or privileged access administrators can watch the session live and receive alerts on suspicious activity to determine if the session should be terminated if needed. I do not use live monitoring constantly, but it is very valuable for domain controller access, production database access, and emergency admin access. Overall, these features are valuable because they provide full visibility into privileged activity without slowing down the administrator.

"One Identity Safeguard has improved privileged access security and accountability. I have eliminated shared admin passwords, implemented time-bound access with approvals, and gained session recording for audits. This has led to better visibility, faster investigation, and reduced standing privilege access. Investigations are much faster and more accurate, and audits are quicker with fewer findings, thanks to full session visibility and traceability. Regarding relevant metrics for any IAM solution or monitoring solution like One Identity Safeguard, previously it took two to three days to complete investigations. Now, after recording the session, investigations can be completed in under an hour.."

Antara R Deolekar
Business Development Executive at Digitaltrack

Read full review

"In my opinion, the best features of One Identity Safeguard are the ones that directly improve both security and operational control. First, privileged session monitoring and recording stand out. One Identity Safeguard can capture and replay entire sessions with searchable logs, even down to the commands and screen activity. This is extremely useful for audits and incident investigations. Second would be secure password vaulting with automated rotation, which is a big advantage. It eliminates manual credential handling and reduces the risk of password exposure while enforcing strong security policies. Another key feature is real-time monitoring and threat detection. One Identity Safeguard can detect suspicious behavior during a session and even block unsafe actions, which adds a proactive security layer rather than just reactive logging. Finally, centralized privileged access governance is an essential feature. Bringing password management, session control, and analytics into a single platform makes it much easier to manage hybrid environments effectively.

Session monitoring and recording, even from demos and industry feedback, has the biggest impact on audits in terms of clarity and speed. Instead of relying only on logs or user statements, with One Identity Safeguard, I can actually replay a full session, see exactly what commands were run, what changes were made, and in what sequence. During an audit or investigation, instead of spending hours correlating logs, my team can directly pull the session recording as evidence. It reduces ambiguity, speeds up root cause analysis, and makes compliance reporting much stronger and more defensible. For example, if there is any suspected misconfiguration or data change, I do not have to guess; I can literally watch what happened.

For day-to-day operations, automated password rotation in One Identity Safeguard shifts us from a manual, reactive process to a fully automated, policy-driven approach. Today, IT teams often spend time resetting privileged passwords, handling access requests, and responding to potential credential exposure. With automation in place, most of the effort is eliminated. Passwords are rotated automatically after each use or on a scheduled basis, so there is no need for frequent manual resets. In fact, it does not just reduce how often we reset passwords; it removes the need for manual resets almost entirely. In terms of

workload, this means fewer support tickets related to password issues, less coordination between teams for credential sharing, and reduced human error. The IT team can shift focus from routine tasks to more strategic work like security improvements and system optimization. One important operational change is that users no longer handle actual credentials. They request access, get approved, and One Identity Safeguard manages everything in the background. That is a big shift in thinking, but it slightly improves security..”

Prithviraj kallurkar
Business Development Executive at Digitaltrack solutions

Read full review

Other Solutions Considered

"We evaluated a few other privileged access management (PAM) solutions before implementing One Identity Safeguard, including CyberArk and other enterprise PAM tools in the same space.."

Twinkle
Business Development Executive at Digital Track Solution pvt ltd

Read full review

"I was previously using a basic in-house solution for managing privileged credentials, but it lacked advanced features such as session monitoring and automated password management. I switched to One Identity Safeguard for better security, centralized control, and improved compliance capability.."

Ahitesh Anumala
Business Development Manager at Digitaltrack Solutions Private Limited

Read full review

"Previously, we used a more basic PAM approach built around a legacy vaulting solution combined with manual approval workflows, ticket-based access, and shared admin controls. We switched mainly because of limited access visibility and auditing, too much manual effort, weak hybrid or cloud integration, especially as we moved more workloads to Azure, and scaling challenges that arose as the number of privileged accounts and systems increased.."

Prithviraj kallurkar
Business Development Executive at Digitaltrack solutions

Read full review

"Before choosing One Identity Safeguard, I evaluated a few other privileged access management solutions, such as CyberArk Privileged Access Manager, Delinea Secret Server, and BeyondTrust Privileged Access Management. These are well-known options in the market and commonly compared during the evaluation.."

Ahitesh Anumala
Business Development Manager at Digitaltrack Solutions Private Limited

Read full review

"Before finalizing on One Identity Safeguard, we evaluated other privilege access management solutions, such as CyberArk and BeyondTrust. CyberArk is a strong market leader with advanced features, but it can be complex to implement and manage. BeyondTrust also offers good capabilities, especially for endpoint privilege management and remote access, but we found One Identity Safeguard to be more aligned with our requirements in terms of ease of use and deployment flexibility. We chose One Identity Safeguard because it provides a good balance between security, usability, and integration capabilities, particularly with Active Directory.."

Prathamesh Pawar
Technical Support Engineer at Digitaltrack

Read full review

"Before choosing One Identity Safeguard, we did evaluate a few other enterprise PAM solutions. The main ones were CyberArk Privileged Access Manager and BeyondTrust Privileged Access Manager. We compared them mainly on session recording and monitoring capabilities, ease of deployment in hybrid environments, and integration with Active Directory. One Identity Safeguard stood out because it offered a strong balance of deep session monitoring and solid integration with our identity stack, along with easier appliance-based development. It aligned well with our internal compliance and auditing requirements without adding too much operational complexity. Overall, the decision came down to fit with our hybrid infrastructure, ease of control, scalability, and compliance readiness rather than just feature comparison.."

Prithviraj kallurkar
Business Development Executive at Digitaltrack solutions

Read full review

ROI

Real user quotes about their ROI:

I have seen a return on investment with One Identity Safeguard, leading to efficient management and lower upfront cost. It has reduced inside and external threats, which is essential for preventing privileged user damage, and decreased privileged account incidents by 40%.

Swapnil Karkala
Senior Frontend Developer at HCl

Read full review

"Time is definitely saved. Regarding money, money is also saved because I maintain the compliance part. However, fewer employees are not needed; I need to hire more employees to monitor these things.."

Antara R Deolekar
Business Development Executive at Digitaltrack

Read full review

"We have seen a clear return on investment with One Identity Safeguard, mainly driven by time savings, reduced manual effort, and fewer security-related incidents. One of the biggest measurable improvements has been in IT workload reduction. After implementing One Identity Safeguard, we saw a significant drop in manual tasks including password handling, privileged access approvals, and incident troubleshooting.."

Twinkle
Business Development Executive at Digital Track Solution pvt ltd

Read full review

"I have seen a clear return on investment with One Identity Safeguard. I have reduced manual effort for access management by around thirty to forty percent, which has saved significant staff hours. Audit preparation time has decreased by nearly fifty percent, and improved security controls have helped lower the risks of costly incidents. Overall, the efficiency gains and risk reduction have justified the investment.."

Ahitesh Anumala
Business Development Manager at Digitaltrack Solutions Private Limited

Read full review

"I have seen a return on investment in both money saved and time saved.

"I have experienced noticeable time savings and some indirect cost benefits, specifically in that access provision has reduced from hours to minutes, requiring less manual effort, and the cost impact has been mitigated due to fewer security incidents and audit issues.."

Nitin Yadav
Network & Security Engineer at Arrow PC Network Pvt Ltd

Read full review

"Overall, we have seen a clear ROI from One Identity Safeguard, mostly in the form of time savings, reduced manual effort, and improved audit efficiency rather than just direct headcount reduction. In terms of time saved, one of the biggest gains is the privileged access workflow, such as password rotation and session approvals. What used to require manual coordination or admin intervention is now largely automated. This has noticeably reduced day-to-day operational overhead for the infrastructure team, amounting to multiple FTE days per week after deployment. From a security and compliance standpoint, the ROI is more evident. Session recording and audit trails have reduced the time spent preparing for audits and investigating incidents. Instead of manually reconstructing activity, everything is already logged and searchable, which has improved response time during internal reviews.."

Prithviraj kallurkar
Business Development Executive at Digitaltrack solutions

Read full review

Use Case

"My main use case for One Identity Safeguard includes privilege access, session recording, and real-time monitoring.

"In daily work, I use session recording and real-time monitoring as part of my workflow.

"My main use case is privilege access.."

Nitin Yadav
Network & Security Engineer at Arrow PC Network Pvt Ltd

Read full review

"I mainly use One Identity Safeguard to secure and control privileged access by managing admin credentials, granting time-based access, and monitoring sessions to ensure security and compliance.

"For example, when an admin needs access to a production server, they request it through One Identity Safeguard, which grants time-limited access after approval. The system automatically injects the credentials, so the password is never exposed, and the entire session is monitored and recorded. This helps my team maintain security and quickly review activity during an audit.."

Ahitesh Anumala
Business Development Manager at Digitaltrack Solutions Private Limited

Read full review

Our primary use case for One Identity Safeguard includes privileged password management, where it includes vaulting, rotating, and checking in and checking out privileged credentials. Secure remote access helps to grant access to Windows/Linux servers based on group membership. We also use it for session monitoring and recording, where it helps to monitor, record, and audit privileged sessions for compliance. Access request simplification plus threat detection helps to streamline requests and quickly detect threats seamlessly.

In my day-to-day work, One Identity Safeguard helps to identify anomalous behavior, a deal breaker feature for some customers. It also helps to detect threats and streamline requests and quickly detect threats. .”

Swapnil Karkala
Senior Frontend Developer at HCl

Read full review

"I have been using One Identity Safeguard for almost a year. The main use case of One Identity Safeguard is privileged access management, specifically controlling and monitoring administrator access. In my organization, I typically use it for privileged password management, secure admin access, session recording and monitoring, approval workflows, and privileged account discovery.

"A common day-to-day example involves accessing a production server. An admin needs to troubleshoot a service issue. Instead of sharing the local administrative password, they submit an access request in One Identity Safeguard, provide a reason, and select a time duration, for example, one hour. A manager or security team approves the request. The admin launches the RDP session directly from One Identity Safeguard. One Identity Safeguard injects the credential automatically. The password is not visible. The entire session is recorded for audit purposes. When the session ends, access expires, and the password is automatically rotated. This makes a difference because there is no shared admin password, temporary least privileged access is implemented, full session recording is available for audits, and automatic password rotation occurs after use.."

Antara R Deolekar
Business Development Executive at Digitaltrack

Read full review

"In our organization, the primary use of One Identity Safeguard is managing and securing privileged access, and we mainly use it to store and protect sensitive credentials like admin passwords, ensuring that they are not exposed or misused. It also helps in monitoring privileged sessions, allowing us to track and audit activities performed by administrators or high-level users. This adds a stronger layer of security and compliance, as all credential access is controlled, recorded, and reviewed when needed. Overall, it plays a key role in protecting sensitive systems and reducing the risk of insider or outsider threats.

"A common example of how we use One Identity Safeguard to secure privileged access is when a system administrator needs access to a production server. Instead of sharing or knowing the actual admin password, they request access through One Identity Safeguard, which securely provides a temporary credential for a session without exposing the password. This system automatically records an entire session, including actions performed on the server. If anything unusual happens, such as an unauthorized change or risky commands, the session logs and recording can be viewed by a security team, ensuring that privileged access is tightly controlled, fully monitored, and auditable at all times.

"One additional point about our main use case is that we use One Identity Safeguard not just for securing access but also for enforcing strict governance and accountability across teams. For example, we apply role-based access control and approval workflows, so any privileged access request must be approved before it is granted.."

Twinkle
Business Development Executive at Digital Track Solution pvt ltd

Read full review

"I am familiar with One Identity Safeguard and am also evaluating it for the organization.

For our primary use case for evaluating One Identity Safeguard, we aim to strengthen privileged access management across our environment. Currently, we are looking to improve how we control, monitor, and secure access to critical systems, especially for admin and high-privilege accounts. Additionally, as our infrastructure is a mix of on-premises and cloud, we need a solution that can provide centralized visibility and control across the environment. One Identity Safeguard aligns well with that need while also helping us streamline access workflows and improve audit readiness.

A good example of a scenario where One Identity Safeguard would really help my team is managing third-party vendor access. When external vendors need access to our critical servers for maintenance or troubleshooting, it often involves sharing credentials or giving standing access, which increases risk. With One Identity Safeguard, we could provide temporary, just-in-time access without exposing actual passwords. The vendor would request access, get approval, and then log in through One Identity Safeguard. Their entire session would be monitored and recorded. This helps us in multiple ways: no credential sharing, full visibility of what actions were performed, and an audit trail for compliance. Once the task is done, access is also automatically revoked. In this scenario, One Identity Safeguard directly reduces security risk while also making the process more controlled and compliant.

There is one important scenario related to internal privileged user management that I would like to add about my use case for One Identity Safeguard. For example, our system administrators currently have standing access to central servers. With One Identity Safeguard, we can shift to a just-in-time access model where admin rights are granted only when needed and for a limited time. This significantly reduces the risk of misuse or accidental changes. Another scenario would be audit and compliance. During audits, it is often challenging to provide clear evidence of who accessed what and what actions were performed. One Identity Safeguard helps by maintaining session recordings and detailed logs, making audits much

smoother and faster..”

Prithviraj kallurkar
Business Development Executive at Digitaltrack solutions

Read full review

Setup

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

"The deployment of One Identity Safeguard was relatively quick compared to many other IAM and PAM solutions because it is delivered as a pre-configured appliance, either physical or virtual. The initial setup can be done quite fast, which helps to reduce the time to value.."

Twinkle

Business Development Executive at Digital Track Solution pvt ltd

Read full review

"The initial setup typically took four weeks and sometimes more than four weeks as well, depending on the customer's environment and production environment. The setup was fairly minimal for end-users, but for an administrator, it requires a lot of work. The process is very straightforward and negotiable as well.."

Antara R Deolekar

Business Development Executive at Digitaltrack

Read full review

"The deployment of the solution took around two to four weeks due to initial setups, integrations, and policy configurations.

"End users need a minimum of two to three weeks to understand the solutions.."

Nitin Yadav

Network & Security Engineer at Arrow PC Network Pvt Ltd

Read full review

"The integration of One Identity Safeguard with my DevOps environment and cloud applications was generally smooth, especially with standard systems, but it required some initial configuration and fine-tuning to align with my DevOps workflow and core cloud applications. I did face minor challenges around setup and policy configuration, but once implemented, it worked reliably and integrated well with my environment.."

Ahitesh Anumala

Business Development Manager at Digitaltrack Solutions Private Limited

Read full review

The deployment of One Identity Safeguard took two to three weeks.

The deployment of One Identity Safeguard did not affect my privileged users; it was not disruptive to them.

“Not much training was required to start using One Identity Safeguard, both for those who manage it and for end users. It is self-service, and it is very easy to learn how to use it. The learning curve is smooth. .”

Swapnil Karkala

Read full review

Senior Frontend Developer at HCl

“The initial deployment of One Identity Safeguard on virtual appliances took roughly six to eight weeks end-to-end, including planning, setup, integration, and user rollout. The process was done in phases. First, we set up the core One Identity Safeguard appliance in a controlled environment and integrated it with our identity sources such as Active Directory. After that, we configured privileged accounts, session policies, and audit requirements. We also ran a pilot with a small group of administrators to validate session recording, access workflows, and reporting before going wider. In terms of disruption, it was minimal for most privileged users, but not completely zero. During the pilot phase, there were some adjustments needed because users had to get used to logging in through One Identity Safeguard gateways instead of directly accessing the system. Overall, the phased rollout approach helped reduce disruption significantly, and most users adapted quickly after the initial onboarding period..”

Prithviraj kallurkar

Read full review

Business Development Executive at Digitaltrack solutions

Customer Service and Support

"Customer support for One Identity Safeguard is generally good and knowledgeable, especially when it comes to technical issues and enterprise deployments.."

Verified user
Network Engineer at a outsourcing company with 1,001-5,000 employees

Read full review

"Customer support for One Identity Safeguard was generally good, with a knowledgeable and helpful team assisting during the setup and troubleshooting. In most cases, issues were resolved efficiently, but response times can sometimes be slower for more complex problems.."

Ahitesh Anumala
Business Development Manager at Digitaltrack Solutions Private Limited

Read full review

"Our experience with customer support has been quite positive. The support team is generally responsive and knowledgeable, especially for standard use configurations, and we have mainly expressed satisfaction in this area because we have solved almost all problems using One Identity Safeguard.."

Nikita Bhojwani
Senior Business Development Executive at Digitaltrack Solutions Private Limited

Read full review

"Customer support for One Identity Safeguard has been generally reliable based on our experience. On the positive side, the customer team is knowledgeable and technically strong, especially when dealing with configuration issues, session monitoring, or password-related queries. For standard or well-defined issues, responses are usually helpful and resolve problems efficiently.."

Twinkle
Business Development Executive at Digital Track Solution pvt ltd

Read full review

"One Identity's customer support is knowledgeable and provides helpful guidance for troubleshooting and configuration-related issues. For standard issues, the response time is responsive and the resolutions are effective. For more complex or critical issues, response time can sometimes vary, but overall, my support experience has been satisfactory. Documentation and knowledge base resources are also useful for resolving common issues and understanding product features, making customer support reliable and meeting enterprise expectations.."

Prathamesh Pawar
Technical Support Engineer at Digitaltrack

Read full review

"I have had to reach out to One Identity customer support a few times, mainly during the initial development phase or for a couple of integration-related queries. Overall, the experience has been decent to good, but it varies depending on the type of issue. For critical or well-defined technical issues, especially around configuration or known product behavior, the support team has been quite effective. They have provided clear guidance and documentation references, and in some cases, helped us resolve issues within a reasonable timeframe. Overall, the responsiveness from the technical side has been generally good, and the knowledge of the support team has been useful. Resolution time has been good for common use issues but slow for complex or custom scenarios, and handling escalations has been manageable.."

Prithviraj kallurkar
Business Development Executive at Digitaltrack solutions

Read full review

Other Advice

"My advice for others considering One Identity Safeguard would be to plan and execute the deployment properly during the implementation phase.

"I have given this review a rating of 8.."

Nitin Yadav
Network & Security Engineer at Arrow PC Network Pvt Ltd

Read full review

"I am currently happy with One Identity Safeguard, so there is no point to implement changes. I gave this solution a rating of eight. There was a short learning curve, but overall adoption was smooth and users now find it very easy and more secure to use. I recommend this solution if you want proper security for your infrastructure and want to improve your budget. If you have a limited budget, then please do not go for this solution. I am asking for better security.."

Antara R Deolekar
Business Development Executive at Digitaltrack

Read full review

"My advice for others looking into using One Identity Safeguard would be to plan the implementation carefully and invest time in understanding your access policies and workflow before deployment. One Identity Safeguard is a powerful tool, but it is not plug and play. It requires proper configuration and tuning to get the best results. Start with a phased rollout, focus on high-risk privileged accounts first, and ensure your team is trained properly. Once properly implemented, it can significantly improve security, visibility, and compliance across the organization. I would rate this product nine out of ten.."

Ahitesh Anumala
Business Development Manager at Digitaltrack Solutions Private Limited

Read full review

"My advice to others looking into using One Identity Safeguard is that we have seen a clear return on investment, mainly derived from saved operational efficiency and reduced security overhead. A simple way to explain it is time saved, faster administration, fewer security incidents, and efficiency gained.

"Overall, One Identity Safeguard stands out as a strong and well-built privileged access management solution, especially for organizations that want tighter control over admin activity without slowing down operations. I would rate this product a nine out of ten.."

Twinkle
Business Development Executive at Digital Track Solution pvt ltd

Read full review

I chose eight out of 10 for One Identity Safeguard because the pricing is very competitive. It is a nice tool that helps to identify anomalous behavior, a deal breaker feature for some customers. It also helps with access request

simplification plus threat detection, where it streamlines requests and quickly detects threats.

My advice for others looking into using One Identity Safeguard is that it is a serious, enterprise-grade identity safeguard. It excels at security, monitoring, and compliance, but trades off simplicity and ease of use.

“One Identity Safeguard has been a cost-effective tool that has prevented major security breaches, avoided insider threats and misuse of admin privileges, and reduced audit and compliance costs. However, the initial cost plus setup effort is a bit high.

“I gave this review a rating of 8 out of 10. .”

Swapnil Karkala
Senior Frontend Developer at HCl

Read full review

“Even during the evaluation phase, One Identity Safeguard has shown clear positive impacts across key areas in my organization. From a security posture perspective, the biggest improvement is the elimination of direct credential exposure. Instead of sharing admin passwords, access is brokered through One Identity Safeguard, which significantly reduces the risk of credential misuse or leakage. In terms of audit readiness, we have seen a big improvement in visibility. The ability to track sessions and maintain detailed logs means we can quickly answer questions such as who accessed what, when, and what actions were performed. Even in a pilot, this level of transparency makes audits much more straightforward. On the operational efficiency side, processes such as access requests and approvals have become more structured instead of informal or manual coordination. Everything follows a defined workflow, which reduces delays and confusion.

Since we are still in the evaluating or pilot phase of One Identity Safeguard, we do

not have long-term production metrics yet, but we have observed some early indicators and rough estimates. For example, in terms of operational efficiency, we have seen a noticeable drop of roughly thirty to forty percent in password-related support requests within the pilot group, mainly because users no longer need to request or manage credentials manually. From an audit perspective, the time required to gather access logs and evidence has reduced significantly. Tasks that earlier took hours, such as correlating logs, can now be done in minutes using session recordings. We estimate around fifty to sixty percent reduction in audit preparation time for privileged access reviews. On the security side, while it is early to quantify incidents, we have effectively reduced the risk surface by eliminating shared credentials in the pilot scope. That alone is a major improvement, even if it is not directly measurable yet. Earlier estimates show thirty to forty percent fewer password-related tickets and fifty percent faster audit preparation, along with reducing risk and eliminating shared credentials.

The integration of One Identity Safeguard has had a clear positive impact on both security and operational efficiency. From a security perspective, the most noticeable improvement is tighter controls over privileged access across systems. For example, before One Identity Safeguard, some privileged accounts, especially service accounts used in automation, had unrestricted access. Just-in-time access and session recording have significantly improved visibility. Now, even when an automation job or admin session runs, we can trace exactly what was accessed and when.

My advice for others looking into using One Identity Safeguard is that it offers a positive ROI overall, but it is mostly reflected in time savings, operational efficiency, and risk reduction rather than a single direct cost metric. In practical terms, the biggest measurable benefit has been time saved for IT and security teams. Tasks such as privileged access approvals, password rotation, and session audits are now largely automated or centralized. Another key area is auditing and compliance efficiency. Before One Identity Safeguard, preparing for audits required collecting logs from multiple systems and manually correlating activity. Now, session records and searchable audit trails make this process faster, saving a significant amount of effort during compliance cycles. Overall, the ROI is very real,

but it shows more in time saved, reduced risk, and smoother operation rather than a direct headcount or cost-cutting figure.

Before wrapping up, I would say that my overall experience with One Identity Safeguard has been strong and reliable for our needs, especially for privileged access control in a hybrid environment. What stands out most is the visibility and control it brings to privileged activity, having full session recording and centralized access workflows. It has also helped us move away from fragmented manual processes towards a more structured and governed access model, which becomes very important as the environment scales. Overall, it has been a solid investment from both a security and operational standpoint. I would rate my overall experience with One Identity Safeguard as a nine out of ten.."

Prithviraj kallurkar
Business Development Executive at Digitaltrack solutions

Read full review

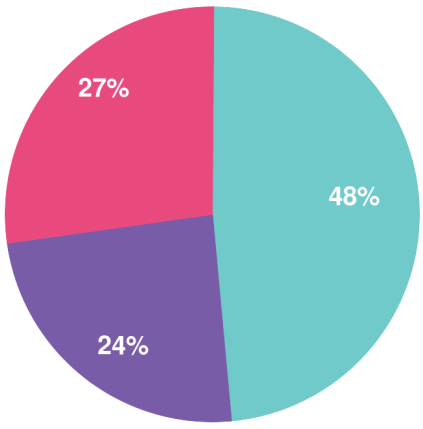
Top Industries

by visitors reading reviews

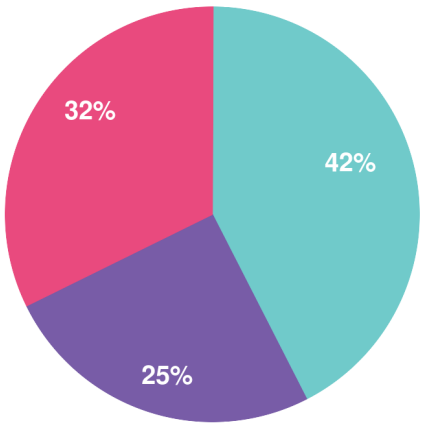
University	11%
Computer Software Company	9%
Outsourcing Company	9%
Financial Services Firm	7%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

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

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

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

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

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

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

About PeerSpot

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

PeerSpot helps tech professionals by providing:

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

Use PeerSpot to:

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

Join PeerSpot to connect with peers to help you:

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

Visit PeerSpot: www.peerspot.com

PeerSpot

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

reports@peerspot.com

+1 646.328.1944