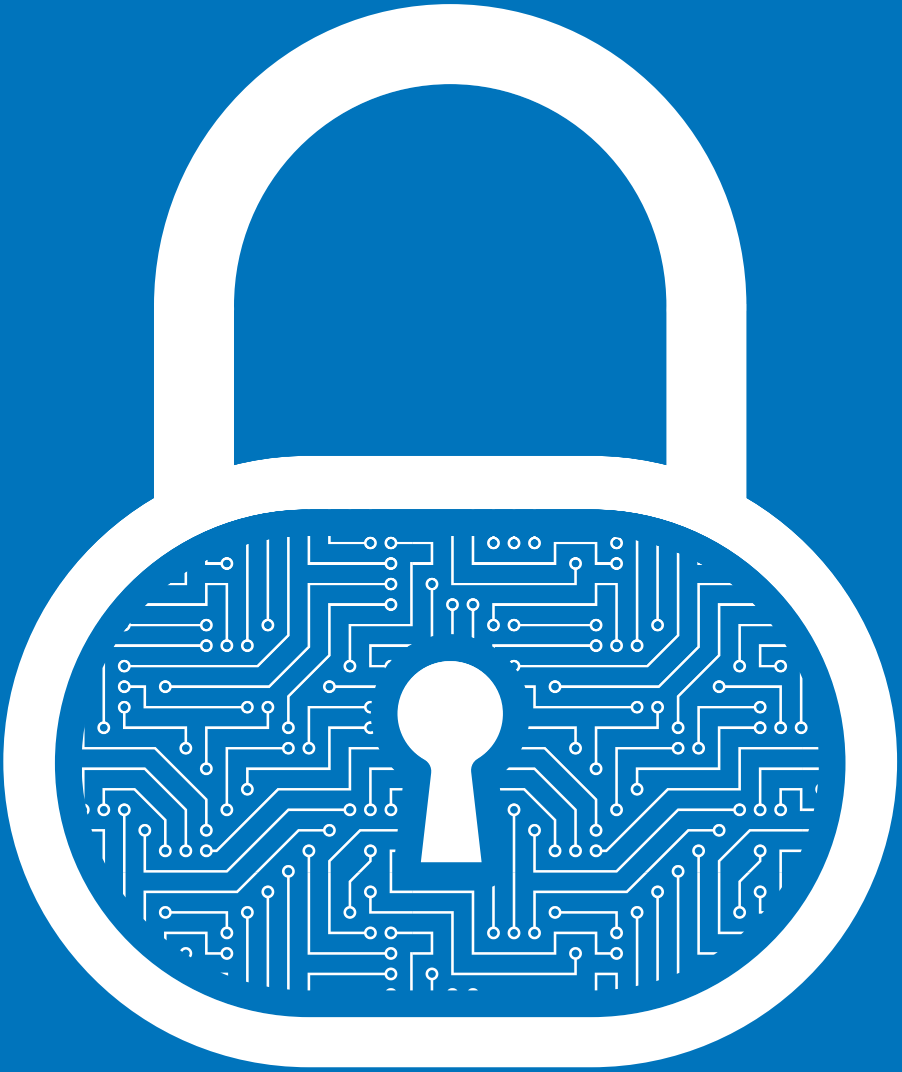
PeerPaper Report

Best Practices: Selecting a Privileged Access Management (PAM) Solution

Based on Real User Reviews of One Identity Safeguard

2020



IT Central Station
Unbiased reviews from the tech community

CSO
FROM IDG

ABSTRACT

Privileged Access Management (PAM) solutions have become essential for compliance and security. They have moved way beyond the realm of “nice to have.” A wide range of PAM solution choices is available, with the new generation offering the best functionality with the least friction. This paper examines the factors that go into selecting a PAM solution. It’s based on insights shared by users of One Identity Safeguard on IT Central Station. Based on their experiences, they recommend assessing a potential PAM solution for its ease of deployment and use, its transparency, scalability, and ability to work with existing IT and business operations.

CONTENTS

INTRODUCTION

Privileged Access Management (PAM) is an established security countermeasure, but the current threat environment and compliance burdens render manual approaches to PAM inadequate.
A PAM solution is now essential.
A range of choices is available, with the next generation offering the best functionality with the least friction. This paper examines the factors that go into selecting a PAM solution, based on experiences described by One Identity Safeguard users on IT Central Station. They recommend assessing a potential PAM solution for its ease of deployment and use, its transparency, scalability, and ability to work with existing IT and business operations.

The Current Mandate for PAM

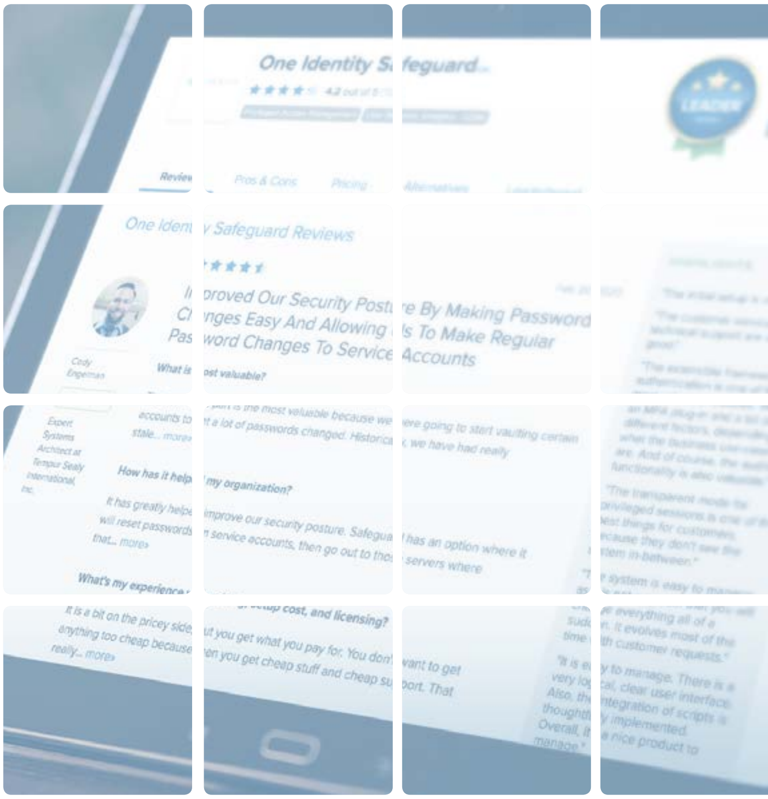
PAM is more than a technology. Rather, it's a collection of practices, policies, and tools that establish controls over administrative "privileged" access to critical systems. PAM is far from a new idea, yet the quality and consistency of PAM practices vary widely. This reality is increasingly concerning as the overlapping fields of compliance and cybersecurity become more demanding.

Security and compliance managers are under pressure to define and enforce PAM policies. Control over privileged users is a fundamental aspect of the major standard industry security and compliance requirements. Achieving these requirements invariably involves the use of a PAM solution. While it is possible to perform PAM manually, this is not optimal. PAM solutions are required for sound monitoring and control over privileged access.

PAM solutions are also essential for effective security incident response and forensics. Without knowing who did what — and when — it is quite difficult to handle a security event or understand what went wrong. Auditing of privileged user activity before and after a breach is also useful in preventing similar events from recurring in the future.

Selection Factors for a PAM Solution

IT Central Station members shared their insights regarding what to look for in a PAM solution. They stressed basic efficacy along with ease of deployment. Transparency, scalability, and ease of use also factored into selection. These qualities are essential for the success of your PAM program. They also underscore a potential risk with the technology. If a PAM solution is too difficult to use, it can end up on the shelf. The right solution can avoid this unfortunate scenario.



Basic Effectiveness

Being able to deliver core PAM functions is a selection factor for PAM solutions, e.g., password and session management, monitoring, privilege delegation, session recording and analytics. This may seem obvious, but the history of overly-complicated systems makes it compelling nonetheless. An Identity & Access Manager at Reist Telecom GmbH, a small tech services company, for example, acknowledged the benefits of his solution by saying, “We are able to demonstrate what has happened on the systems and who did what, when we have to investigate, in regards to audits using evidence.”

An IT Security Consultant at a small tech services company similarly remarked that his solution “gave much more visibility over who is doing what and more granular control over external support engineers.”

An Expert Systems Architect at Tempur Sealy International, a manufacturing company with more than 5,000 employees, shared, “It has greatly helped improve our security posture. Safeguard has an option where it will reset passwords on service accounts, then go out to those servers where that service account is running as a service and update the password on it. That makes password changes very easy.

We can regularly change passwords now and are planning on making it an annual activity, where all the people who own service accounts will go in and make sure all their passwords get changed, updated, and reset." Figure 1 captures the basic functions of a PAM solution.

"We went from a state where privileged accounts were being used and not being monitored or even audited to our situation now where we are starting to monitor these privileged accounts more closely," said an Information Security Manager at a financial services firm with over 1,000 employees. He added, "That's where we show value in the product. Whenever a change is happening, we know because we find it in the logs. Our reporting and monitoring team is looking at it, and they are now starting to question changes that are associated with some kind of ticket or some kind CAB (change advisory board) request. It has improved our visibility for privileged access."

Ease of Deployment

PAM solutions need to be easy to set up. If PAM is overly time-consuming or requires excessive external consulting to set up, it may fail to launch. No IT department volunteers for long, costly, and frustrating projects. Praise for ease of deployment thus comes through in many reviews.

> "
> **... the way the solution is installed and deployed is very valuable. They make it very easy.**

For example, a Security Consultant at Controlware GmbH, a tech services company with more than 200 employees, praised Safeguard because, "the install and deployment are quite rapid." As he said, "For a smaller project, sometimes it only takes us about two to three days to implement and get the policies inline. For larger projects, it's actually also not that long for the appliance itself." A System Consultant at a tech services company with over 1,000 employees simply said, "The initial setup is very easy."

"The initial setup is quite simple, not complex. The installation documentation is good, so the installation is okay," said the Identity & Access Manager at Reist. For a VP of Risk Management

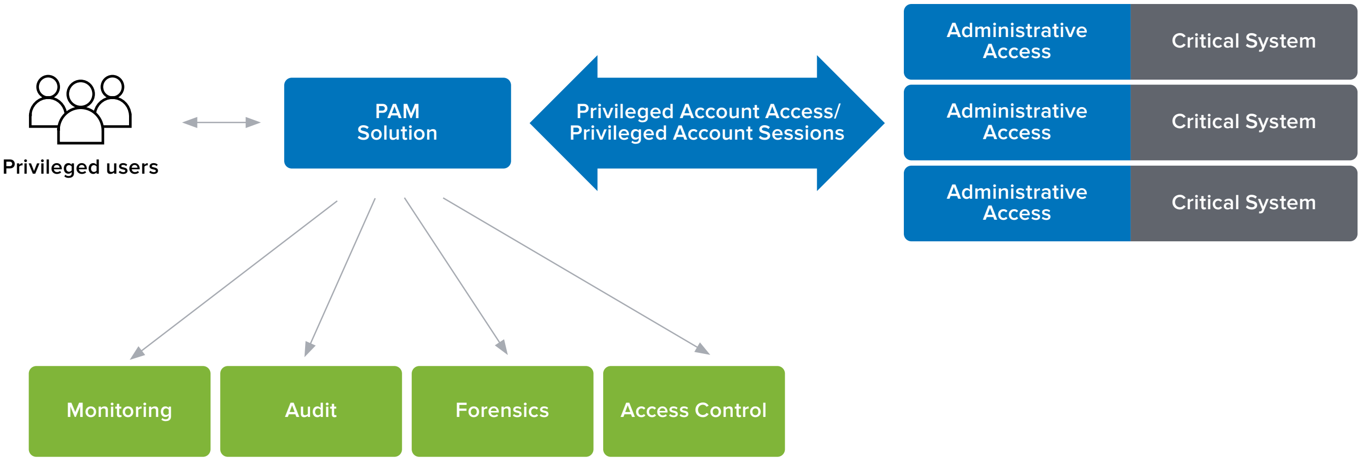


Figure 1 - The basic functions of a PAM solution, including privileged account monitoring, audit, forensics, and access control.

at a Financial Services firm with over 1,000 employees, "The deployment took no more time from when we got the servers brought in to when got the software installed. This took a few weeks to get it up, configured, and customized for our needs." A Security Engineer at a tech services company with more than 200 employees shared that "the way the solution is installed and deployed is very valuable. They make it very easy." They had previously used CyberArk, which they described as being "a much more difficult solution to work with and deploy."

> "The initial setup is quite simple, not complex. The installation documentation is good...

Transparency

Further to the point of avoiding "shelfware" and the circumvention of PAM by users, IT Central Station members expressed the view that transparency should be a factor in selecting a PAM solution. As the Controlware Security Consultant put it, "The transparent mode for privileged sessions is really nice because it keeps the integration quite smooth. Also, users don't have to change the way that they currently are used to working." The Identity & Access Manager at Reist also remarked, "The transparent mode for privileged sessions is one of the best things for customers, because they don't see the system in-between. Thus, it is transparent for them."

"The transparent proxy is the most valuable feature," said a Chief Information Security Officer at Outscale, a small tech services company. He added, "When you are connecting to a server inside the platform, the user doesn't need to change their habit. They just have to make small configurations to their workstation, then it is transparent for them. Our users like the solution because it's transparent. It's interesting for the users because they don't have to think, 'I have to note all what I've done during the incident to remember it.'" This user also shared that his team had evaluated CyberArk. He noted, "CyberArk's login was not so transparent. We chose One Identity because it has a transparent login."

Operations and Automation Ready

By its very nature, a PAM solution must interact with a wide range of IT systems. Users thus prefer solutions that can be automated and be made ready to work with IT operations. Making this happen today invariably requires a standards-based Application Programming Interface (API). One Identity has a RESTful API for this purpose, enabling it to integrate with Security Incident and Event Management (SIEM) ticketing systems, DevOps, and so forth. Figure 2 provides a simple reference architecture for PAM integration with operational systems.

> "The transparent mode for privileged sessions is really nice because it keeps the integration quite smooth.

For instance, a VP Risk Management at a financial services firm with over 1,000 employees shared that the Safeguard solution is part of his company's identity and access management product. He said, "We use Saviynt as our identity, governance, and administrative tool. We certify all privilege accounts on a schedule basis. There is some integration with our identity and access management platform/program at the bank." The value of this integration came from being in a position where they can identify and detect as well as prevent any type of privilege act that's being used as a threat at the bank.

"It has reduced operational costs as well as providing services 24/7 with a platform that can be used anytime and anywhere for investigation in case we have a requirement," explained a Chief Information Security Officer at a small financial services firm. He then commented, "We integrated One Identity with our ERP system (Oracle) and also with our security operations center (Splunk). The integration went perfectly. It was an easy connection. We built the connectivity directly through the API. All the logs in the system are recorded and sent to our security operations center (SOC) for analysis."

> **It has reduced operational costs as well as providing services 24/7...**

The financial services Information Security Manager uses Safeguard to manage the account for his IIGA identity governance solution. He noted, "When it creates new users or transfers or terminates users, it's using a privileged account that is being handled by Safeguard." In this use case, PAM is the primary control on all user identities in the organization.

Scalability

IT Central Station members preferred PAM solutions that can scale easily. In this context, a PAM user at a company with over 10,000 employees said, "No problem to scale. It's always a good option to use a load balancer in front of the solution to handle the traffic." The financial services Information Security Manager similarly noted, "It's very scalable. It doesn't matter what size of organization you have. If you have an organization of 1,000 or 100,000, the product is going to be scalable to your needs."

Flexibility in deployment also emerged as a selection factor. "We have also found the solution to be extensible through cloud-delivered services," said an IDM Architect at a tech company with over 10,000 employees. He then commented, "It's worked out well. The SPS instances we use are located on-premise,

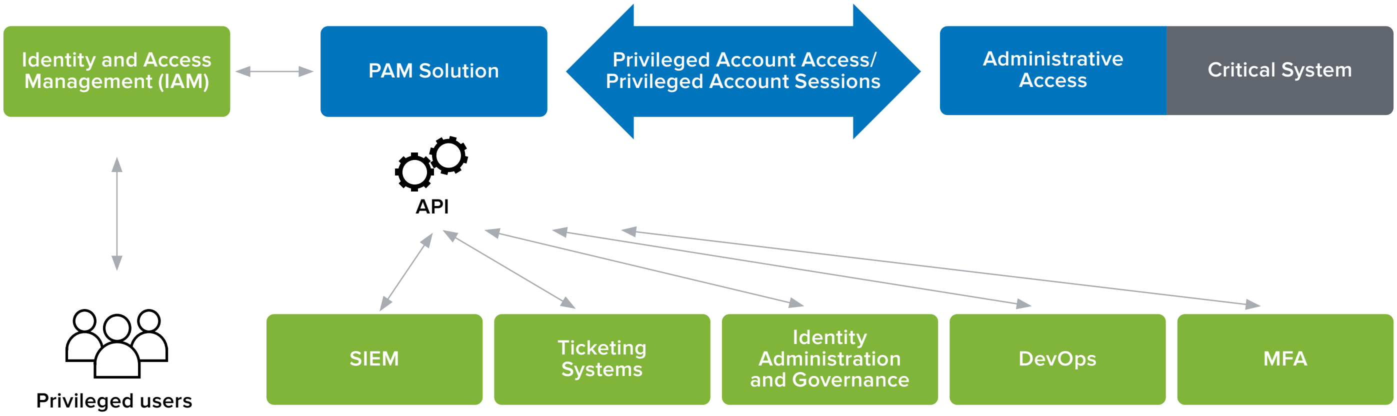

Identity and Access Management (IAM)
PAM Solution
Privileged Account Access/ Privileged Account Sessions
Administrative Access
Critical System
API
Privileged users
SIEM
Ticketing Systems
Identity Administration and Governance
DevOps
MFA

Figure 2 – PAM integration with operational systems.

but we can still utilize them to access resources in the cloud." This capability mattered to the financial services Information Security Manager because, as he said, "We definitely have plans to expand the usage of the product. Any area that's going to require some kind of privileged account, especially as we go through a digital transformation in deploying cloud services, Safeguard is going to be right there with us and will give us that flexibility to manage those kinds of accounts."

> **It's very scalable. It doesn't matter what size of organization you have. If you have an organization of 1,000 or 100,000, the product is going to be scalable to your needs.**

Other notable comments about PAM scalability included:

- "It is very scalable. If we want to add another site or stand up another data center, we just buy a couple more appliances. Then, we set up a couple more session boxes and everything is covered." - Expert Systems Architect at Tempur Sealy International
- "Because of the nature of the connections being monitored, you can load balance it quite well. It is easy to shift the load from one appliance to another." - Security Consultant at Controlware GmbH
- "The solution is scalable. You can place it on another virtual machine to extend it. Right now, we only have three users on the solution as we are in a pre-production environment." - Security Engineer at a tech services company with more than 200 employees

Ease of Use/Management

PAM solutions have to be easy to manage. If it takes too many person-hours to support, the IT team will not be happy. They also have to be simple — or even totally invisible — to end users. Given the usual budget and personnel constraints, the less effort it requires, the better off everyone is. The Controlware Security Consultant spoke to this issue when he said, "It is easy to manage. There is a very logical, clear user interface. Also, the integration of scripts is thoughtfully implemented. Overall, it's a nice product to manage."

The Identity & Access Manager at Reist echoed this sentiment, saying, "The system is easy to manage, as it is not a system that you will change everything all of a sudden. It evolves most of the time with customer requests." The IDM Architect liked that his solution enabled his team to take an environment where they had several hosts managed by different people and consolidate them into a single, centrally managed solution.

> **It is easy to manage. There is a very logical, clear user interface.**

For the financial services Information Security Manager, the solution's functionality, use cases, and usability were straightforward. He said, "They designed this product with the end-user in mind, and they also had the sysadmin who is supporting the product in mind." Tempur Sealy's Expert Systems Architect likewise added, "It's really easy to use. Security guys are able to identify, 'Why is this person logging into spots on the weekend when historically they've never accessed it on the weekend whatsoever?' We're able to keep watch as there is a lot better visibility of our environment."

Flexible, Consistent Approvals

IT Central Station members expressed the view that a PAM solution should support flexibility in granting privileged access requests. This is because approvals of access need to be universal in order for PAM to work as a security countermeasure. If users can get privileged access without a knowledgeable person in a position of authority saying yes, there will be serious risk exposure. The admins who approve such requests may be out of the office, however, so an effective PAM solution offers approvals from anywhere.

To this point, the financial services Information Security Manager said, “We use the Approval Anywhere feature and, through an app, it allows us to approve or deny requests. It adds an extra layer of security for critical passwords without adding time-consuming approval processes.”

> “
> **It adds an extra layer of security for critical passwords without adding time-consuming approval processes.**

CONCLUSION

PAM is an increasingly important mandate for security managers. The right PAM solution, as exemplified by One Identity, will enable security and compliance teams to define and enforce robust privileged account policies. This means being easy to deploy and use. As One Identity user reviews reveal, the right PAM solution will also provide transparency for users. The less evident the solution is, the more effective it will be, according to IT Central Station members. It should integrate with other security and operational systems. Scalability is important as well, as corporate organizations grow and evolve over time. An appropriate PAM solution is able to keep up and not stand in the way of change.

ABOUT IT CENTRAL STATION

User reviews, candid discussions, and more for enterprise technology professionals.

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors. What you really want is objective information from other users. IT Central Station provides technology professionals with a community platform to share information about enterprise solutions.

IT Central Station is committed to offering user-contributed information that is valuable, objective, and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

www.itcentralstation.com

IT Central Station does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, IT Central Station websites, and IT Central Station materials do not reflect the opinions of IT Central Station.

ABOUT ONE IDENTITY

One Identity, a Quest Software business, lets organizations implement an identity-centricsecurity strategy, whether on-prem, in the cloud or in a hybrid environment. With our uniquely broad and integrated portfolio of identity management offerings including account management, identity governance and administration and privileged access management, organizations are empowered to reach their full potential where security is achieved by placing identities at the core of a program, enabling proper access across all user types, systems and data. Learn more at OneIdentity.com.