SSH.COM

RFI Guide

5 must-have functions for every Privileged Access Management (PAM) solution

Make your trusted user management smooth, scalable and fast to deploy in multi-cloud & hybrid environments.

Premise

Permanent access credentials are dead!

Cloudification and digital transformation emphasize speed, agility and elasticity. Many of your privileged users (for example, developers, database admins, quality engineers, test engineers) are already using state of the art tools in their daily work but the tools that manage & control their access – like Privileged Access Management (PAM) solutions – are based on technology that was designed 15 years ago - when the world was more static and the change of pace more limited.

It is time to eliminate the words 'permanent' and 'static' from the administrative access management equation and think beyond traditional PAM paradigms. Often, they are based on permanent access credentials that work on the assumption that both the client, the server, the person and the level of privilege stay the same when the credentials are created. Nothing could be further from the truth in the era of digital transformation and cloudification.

Some of the reasons:

- **In a networked world, enterprises become decentralized**. Not everyone accessing your critical infrastructure is a permanent employee. Also affiliates, partners, 3rd parties, external contractors etc. are all a part of an enterprise ecosystem at one point or another.
- Also **permanent employees change roles** and levels of privilege constantly
- **Access needs are often short-lived and temporary** & need to be set up instantly
- **Cloud instances** are enrolled and decommissioned every day
- Your **managed host inventory is actually a multi-cloud, multi-vendor environment with a mix of on-prem** resources – with multiple access consoles and privileged user registries
- **Permanent access credentials are typically created manually** and are configured '**per-client-per-user-per server**'. This means agents need to be installed, configured and updated on the clients and the servers, creating a constant update cycle that in turn leads to operational friction.

Premise (cont.)

Permanent access credentials are dead!

As a result, permanent access credentials often:

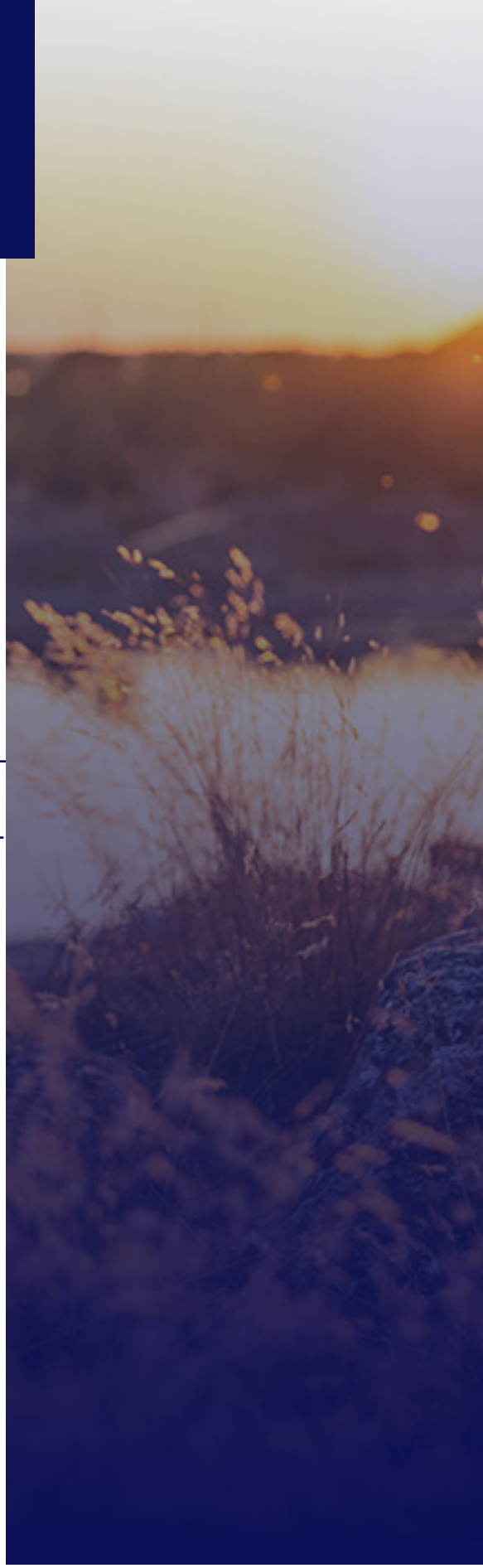
- are an **obstacle to attaining true cloud speed**
- are **shared with limited traceability**, because it is convenient
- provide **too much privilege** for the task at hand
- are **self-provisioned** without true individual accountability
- can be used to **move laterally inside the network**
- can be **forgotten, stolen, mismanaged, misconfigured & lost**

And the list goes on. We believe it is time to think beyond permanent access credentials and move towards a solution architecture where every authorization is short-lived and temporary and that allows you to stay on the pulse of the cloud.

1 Elastic, just-in-time access with the right amount of privilege for the right user

Go for a innovative & new architecture. Privileged users log in to the solution via their browser using Single Sign-on (SSO) and can see all their accessible hosts based on their current role(s). They can then access their user acounts with one click. It's "credentialess" because acess is not granted by user passwords.

This is possible because the solution validates each secure SSH/RDP/HTTPS connection in real time with unique, ephemeral certificates that are invisible to the user and automatically expire after authorization - even after a successful login. This is to ensure that there are no permanent credentials for anyone.



Benefits:

- **One trusted authority** between privileged users and their critical resources
- **Adhere to the principle of zero trust**: authenticate each user with just-in- time access with the just right amount of privilege to get the job done
- **No lateral movement in the network**, there is no unauthorized access as users can only see what they are allowed to access and nothing more
- **Easy Master Data Management (MDM)** of privileged users
- **No permanent credentials** to steal, forget, lose, mismanage or misconfigure to minimize risks and expedite access
- **No need to rotate passwords or to use traditional password vaults:** eliminates the single point of failure and the need for credentials management

2 Simple & instant on-boarding/ off-boarding 3rd parties, temps & employees

Automation is your friend. So is a solution that gets the user identities from your corporate directory (AD/LDAP/ OpenID) or identity management system (IAM/ IDM/IdaaS) automatically. Those identities are already defined into groups by job functions, so all your admin needs to do is to associate the groups with roles that entitle the right level of privilege per role (for example, developer, database admin, quality engineer, test engineer). Then, admin configures your (target) hosts to match the user accounts with roles defined in the solution to your multi-cloud & hybrid environment using automation and orchestration tools like Chef, Puppet, Ansible. This needs to be done only once.

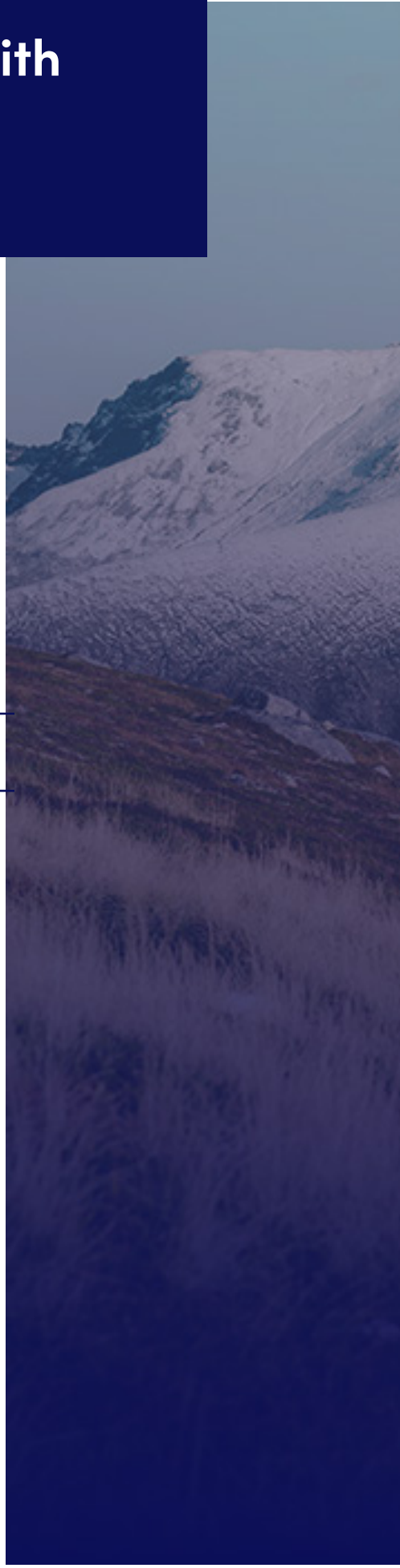
New users, any changes in user roles are discovered automatically after that. Your multi-cloud can change, you can scale your host needs up or down, and the users always have an up-to-date list of hosts and user accounts based on their current roles. If you remove a user from your AD or LDAP, the connection terminates automatically within 60 seconds. The same is true if the user logs out or if the user group changes in the directory service.

You can also define the allocated time for access in advance for external contractors (for example for 12 hours of allocated time) or provide ad-hoc access without any need to remember to revoke the access. All using simple workflows. Federated user authentication is also supported (Kerberos, OpenID).

Benefits:

- **Manage the entire access life-cycle of all job functions (the movers, joiners and leavers process)** in a mostly automated fashion and handle change in access needs instantly without delay
- **No duplicate user registries/directories (separate directory of privileged users in PAM)** – leverage the work that's been done already and link the HR process with the IT process
- **Deal with temporary access needs using simple workflows**: grant/ request elevated roles with automated access upon approval for the agreed period while following the principle of least privilege
- Multi-Factor Authentication (**MFA**) /Time-based One-Time Password (**TOTP**) /**Biometrics** Identity verification
- **Through OpenID Connect, integrates with IAM/IDaaS** service providers like Fujitsu, Okta, ForgeRock and Ubisecure

3 Centralized, browser- based UI with role-based access (RBAC) to all managed hosts



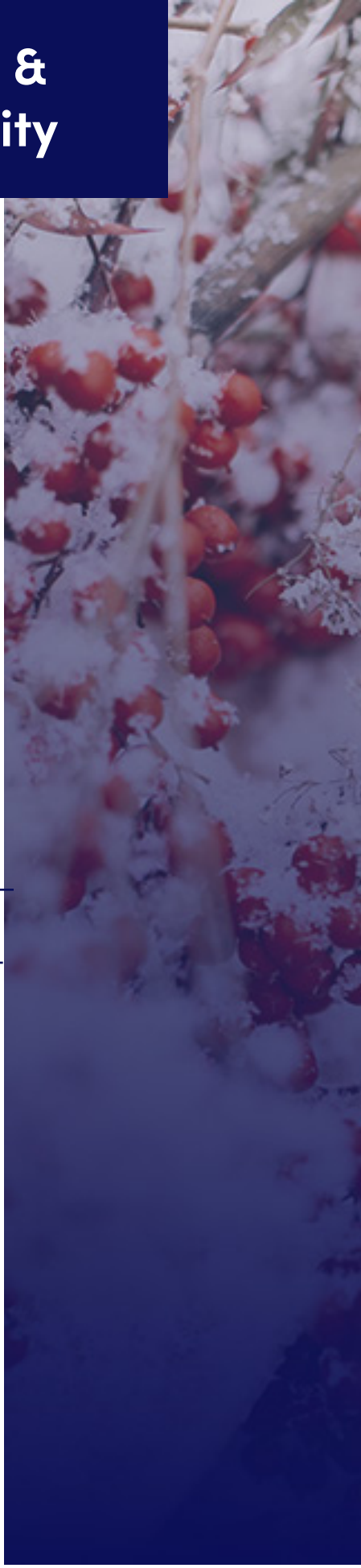
AWS, Google Cloud, Azure and OpenStack all have their access consoles to their respective proprietary cloud environment. The same is true for on-prem access.

Unfortunately, this means that your developers have to use multiple systems to access a resource and your IT manager needs to handle multiple user registries with duplicate information. This can be solved by using a browser-based trusted authority that links the privileged user ID with the right role that is needed to access a host and that then tracks that access.

Benefits:

- **Automatic discovery of your global multi-cloud (AWS, GCP, Azure, OpenStack) & on-prem estate 24/7**
- **No need to use multiple access consoles** per cloud service provider for access as a developer
- **Consolidated access administration** across the multi-cloud & on-prem inventory
- **Single source of truth**: role-based access with individual accountability
- **Get rid of password policies**. Shared accounts are safe to use, since the user's identity is always known to ensure individual accountability
- **Automatic audit trail** of all privileged access from inside and outside the company
- **Integration** with Security Information and Event Management (SIEM), ticketing systems, behavior analytics, AI with APIs
- **Compliance** with regulations and internal security polices for full accountability. Audit events can forwarded to external tools (SIEM, Azure Event Hub, AWS Cloud Watch, etc.) for further analysis.

4 Ease of use, great user experience & easy maintenance for better security



User experience matters. The more complicated the security software is to use, the more likely it is bypassed or it slows down the work of your engineers. Think about a solution, where the developer no longer logs in to the server using access credentials. Instead, she logs in to the solution using a browser with SSO and has an automatic view to all the servers and hosts she has access to. All it takes is one click and she's in.

Your admin has most of the work automated for him. After the initial setup, user group changes, the inventory of cloud assets and session logging are all automatically taken care of and updated.

Deployment and maintenance are also a big part of the experience. That is why a solution that can be deployed in a day and for all intents and purposes maintains itself is great. There is no need to install agents on the client or the server, so when the solution is up-to-date, your secure access is up-to-date.

Benefits:

- **Developers**: no need to look for access credentials or hosts to access, no complicated trainings, no configuring anything on the client: just 1-click to the right resources
- **Admins**: manage access with a dozen of access roles instead of hundreds of identities to save time and nerves
- **IT managers**: deploy in a day, walk away without massive IT projects or a team to maintain the solution: no agents to install or update on the clients or the servers
- **Devices**: no need to use VPNs that give access to the whole environment — stay safer with browser based sessions that limit the impact of untrusted devices/malware originating from physical hardware
- **3rd parties**: instant trusted access without training or installing anything on the client

5 Operational efficiency and cloud scalability to save on time & costs

To operate at the speed of cloud means matching the agility, flexibility and scalability of the cloud. Unlike traditional PAMs, look for a solution that is compact to ensure that your infrastructure stays lean and doesn't bloat into a monster that slows down your operations.

For high availability and load balancing, set up multiple servers as part of a single deployment. Ensure that the solution comes with a microservice architecture to support multiprocessing and benefit from using multiple CPUs or multiple CPU cores with minimal footprint.

Benefits:

- **Low Total Cost of Ownership (TCO)** with the fraction of the deployment time
- **Easy to take into use and maintain** compared to heavy fooprint solutions
- **Save valuable R&D time** for productive work with frictionless access
- Single access authority that **automatically updates itself and shields your environment** from changes in the user groups or the host environment
- **Unified view** into the global multi-cloud inventory – get rid of the ones you no longer need & **save money**
- **No duplicate privileged user registries/directories** – leverage the work that's been done already for better **ROI**
- **Best-of-breed access tool**: no multiple point solutions for cloud access
- **Scalable at cloud speed**: discovering user group changes and cloud hosts is **automated**, new instances are fast to deploy

Conclusion

Today's fast-paced and complex IT environment requires agile security solutions. SSH.COM delivers PrivX, a lean zero-trust access management solution, which offers a modern alternative to traditional PAM, and is ideally suited to today's rapid-fire DevOps applications and hybrid, multi-cloud environments.

Ephemeral certificate authentication avoids password and credentials management, adding convenience and security, while the agentless deployment scheme results in faster deployments. RBAC and simple integration with existing identity management systems further facilitate implementation, and deployment time is measured in days rather than months.

To learn more, visit us on SSH.com/products/privx.

SSH.COM

Finland

SSH Communication Security Oyj
Karvaamokuja 2 B 00380 Helsinki
www.ssh.com
+358 20 500 7000
info.fi@ssh.com

USA

SSH Communication Security, INC.
434 W 33rd Street, Suite 842
New York, NY, 10001, USA
www.ssh.com
+1 781 247 2100
info.fi@ssh.com

Hong Kong

SSH Communication Security LTD.
35/F Central Plaza, 18 Harbour Road
Wan Chai
Hong Kong
www.ssh.com
+852 2593 1182
info.fi@ssh.com