SiTS

Your Trusted
Cyber Security Partner

Privileged Access Management as a Service

Introduction by Brian de Vries, teamlead PAM as a Service

SITS announces the introduction of Privileged Access Management as a Service (PAM as a Service). This PAM as a Service offer is built upon SITS's long-standing and successful best practices foundation together with CyberArk, named a Leader in the latest “Gartner® Magic Quadrant™ for Privileged Access Management” (PAM).

In today’s digital landscape, privileged access accounts are the “keys to the kingdom” for cybercriminals, providing unrestricted access to systems and data. Consequently, cybercriminals target these high-value accounts, with most of breaches involving privileged accounts, highlighting the need for robust PAM solutions . Cyberattacks, including ransomware, have become increasingly problematic, partly due to attackers exploiting vulnerabilities in unmanaged privileged identities.

SITS's PAM as a Service leverages CyberArk’s advanced technologies to deliver a comprehensive solution that secures, manages, and monitors privileged access. By offering PAM as a service, SITS ensures that all organizations can benefit from cutting-edge security measures without the complexities of managing and maintaining the infrastructure and configuration themselves.

“This is truly a game-changer in IAM managed services. It addresses the major risks of privileged access that is involved in most cyberattacks. Our customers can now benefit from best in class PAM managed services, with unparalleled scalability, speed, and affordability. I am proud of the team that made this possible.”

“I hope you learn more about privileged access management. Please feel free to contact me in case you have questions.”

Brian de Vries, Teamlead PAMaaS

Do you have oversight of your privileged accounts?

Any organization can experience attacks and data breaches – if not from within the organization by the unsuspecting or disgruntled employee, then from outside the organization. Or even through cooperating organizations. It is by no means just about unknown perpetrators who happen to find a vulnerability in your IT system any longer. Increasingly, the goal is to take advantage of your information or IT systems.

Hacks regularly appear in the news with far-reaching consequences, such as data being lost or becoming public. Or having to pay a ransom to access your data again. Failure to pay usually means loss of data. Enterprises legally obliged to report it, resulting in fines and possible compensation. Not to mention the (potential) clients and customers who will do business elsewhere.

How much insight do you have into access to your and your customers' information and IT systems?

According to the Identity Security Threat Landscape 2024 report , 93% of organizations suffered two or more identity-related breaches in the last 12 months. Studies show that many companies do not have an overview of all their login data. IT auditors regularly observe risks in the secure (or insecure) use of login data.

1. https://www.cyberark.com/resources/ebooks/identity-security-threat-landscape-2024-report

What are your privileged accounts?

If you and your colleagues work with IT systems, you deal with login accounts and access rights. These login details are needed to use applications and communication tools like personal email. These are the regular business accounts managed by Identity and Access Management solutions. However, employees who manage IT systems or corporate communications use other special accounts, called privileged accounts. These accounts are used for tasks like setting up and maintaining IT systems, networks, servers, workstations, and mobile devices, or sharing information on social media for your organization.

Privileged accounts have more rights than regular accounts and are considered critical accounts. Users of the privileged accounts have the option to change the access to confidential information or make business critical applications unavailable. Examples of privileged accounts are:

- Administrator and root accounts to maintain IT systems;
- Accounts to post/edit information on your corporate social media account;
- Accounts to adjust a power supply (for example, wind turbines, smart meters, and other IoT devices);
- Accounts to carry out (payment) transactions;
- Accounts used within applications or Robotic Process Automation (RPA) software to establish connections to other applications.

Privileged accounts provide access to your organization's crown jewels: the information your organization cannot do without.
To regulate the use, management and access to privileged accounts, there are specific solutions under the collective name of Privileged Access Management (PAM).

Problems with privileged accounts

Privileged accounts are sought after by hackers because they provide access to important systems and information. Without the help of a PAM solution, users of privileged accounts must set their own hard-to-guess passwords for those privileged accounts and change them regularly so that unauthorized persons cannot discover them or once discovered, cannot abuse them for long. These passwords for shared privileged accounts must be shared securely and records must be kept of who used which privileged account and when to ensure traceability to the user.

To keep an overview of the number of accounts and passwords, the number of privileged accounts will be limited. This does not benefit the meshing of the system. The rights granted to privileged accounts are then more expansive than necessary. Users can carry out tasks that go beyond what is intended. The principle of least privileges is therefore abandoned; grant only those rights that are necessary for the task for which the privileged account is intended. We also see that privileged accounts are more often shared, while the password must be known or accessible to multiple employees. But who is responsible for regularly changing the password of the privileged account? And who used a privileged account at what time, for what purpose and what was actually done with it? How strong is the discipline to keep it up? And what about the passwords used in applications and services? Is there any monitoring of usage and whether passwords are changed? It is precisely in the latter category – in addition to the abuse of domain admin accounts – that the greatest risks lie, and hackers know it!

PAM as Man-In-The-Middle (MITM)

Access in PAM is provided by session management. Session management makes it possible to establish a secure connection to a target system, creating **insulation** between the administrator's workstation and the target system. In fact, the user connects to a hardened PAM session proxy component, also known as a steppingstone, step-up server or jump host. The session proxy then initiates a second session to the relevant target system. The user will therefore not have a direct connection to a target system, thus preventing "eavesdropping" on a possibly compromised workstation.

In addition to insulation, the session proxy can also be used to record what activities are carried out on a target system by means of **recording**. In this way, from an auditor's perspective or a problem solver's perspective, specifically authorized persons can review what has been done. The option is also offered to watch during a live session. This can be useful, for example, if an external supplier needs to carry out work.

When using session management, it is important to investigate whether there is a breach of **privacy**. It will first be necessary to establish what the policy is on the possible monitoring of employees. It is also possible that confidential information is in view during a session. It is therefore important to establish who is permitted to view any recordings within the organization. Finally, a determination must be made about how long recordings can be retained. If recordings can or must be saved for a long time, it is also important to provide sufficient storage space for the PAM solution.

Privileged Access Management or Privileged Account Management?

A PAM solution offers various options that can help protect and provide traceability in the use of privileged accounts. For example, your privileged accounts will be safely stored in a digital vault that is protected by a number of security layers such as strong encryption, application of granular PAM access rights, extensive and non-customizable logging, isolation and hardening.

PAM supports password management of privileged accounts and in that way relieves the burden on users of the account. It can periodically change passwords in an automated way, including the enforcement of required complexity. Periodically changing passwords reduces the risk of using an old, well-known password. It will also be possible to apply the principle of least privileges, based on which more specific accounts are used with only the minimum required rights. The secure storage and automatic management of passwords is Privileged Account Management.

Administrators can also gain access to target systems or information without knowing the password. That is known as Privileged Access Management. The access will then be set up entirely through PAM, with the password being automatically entered into the target system invisible to the user. This functionality can be used for both internal employees of an organization and external suppliers. Providing secure access for external suppliers through PAM is also called remote access.

Which target systems an administrator is permitted to access and which corresponding privileged accounts can be used is defined with set authorizations in PAM. An alternative is approval process can also be set up before a privileged account can actually be used. The use of a privileged account is recorded in logging and is therefore traceable. It is even possible to make recordings of all activities during the work. A recording such as that can then be viewed from an auditor's perspective to see exactly what has been done on a target system in response to an incident. Recording is part of PAM session management. See the box for more information on PAM session management.

With PAM, you can therefore:

- Save passwords of privileged accounts centrally and securely;
- Automated and periodic password changes of privileged accounts based on policy;
- Central management of access to various target systems and associated privileged accounts;
- Granting users only management access to systems for which they are authorized;
- Giving users management access when necessary;
- Recording all actions of privileged accounts unalterably in an audit trail.

From standing privileges to zero standing privileges

Traditionally privileged accounts are often created on a permanent basis, also called “standing access”. The risk with standing (privileged) access is that these accounts can be harvested by attackers and misused, because these accounts remain in existence. Modern PAM solutions can now also operate under what is known as the “zero standing privileges” principle, which is in line with the principle of least privilege.

With zero standing privileges, tasks are assigned based on just-in-time and just-enough privileges. In other words, the privileges are only valid for a set time and only with the rights that are strictly necessary for a specific asset. When an administrator needs to carry out operational work and requires appropriate rights, then he or she submits a request through the PAM system. If the requester meets the requirements to obtain access to the necessary admin rights for the asset, then this is defined according to attribute-based access control (ABAC). As soon as the request is (automatically) approved, the PAM system creates a temporary privileged account. This is valid only for the asset and for the period specified in the request. Zero standing privileges are granted through ephemeral access. As soon as the period has elapsed, the user is logged off and the privileged account is automatically removed. The PAM system automatically records who had access to which asset and when in a full audit log. The absence of zero standing privileges prevents misuse. After all, there is no account present that can be hacked. The ephemeral privileged account is created in such a way that it can be recognized in log files and the SIEM system.

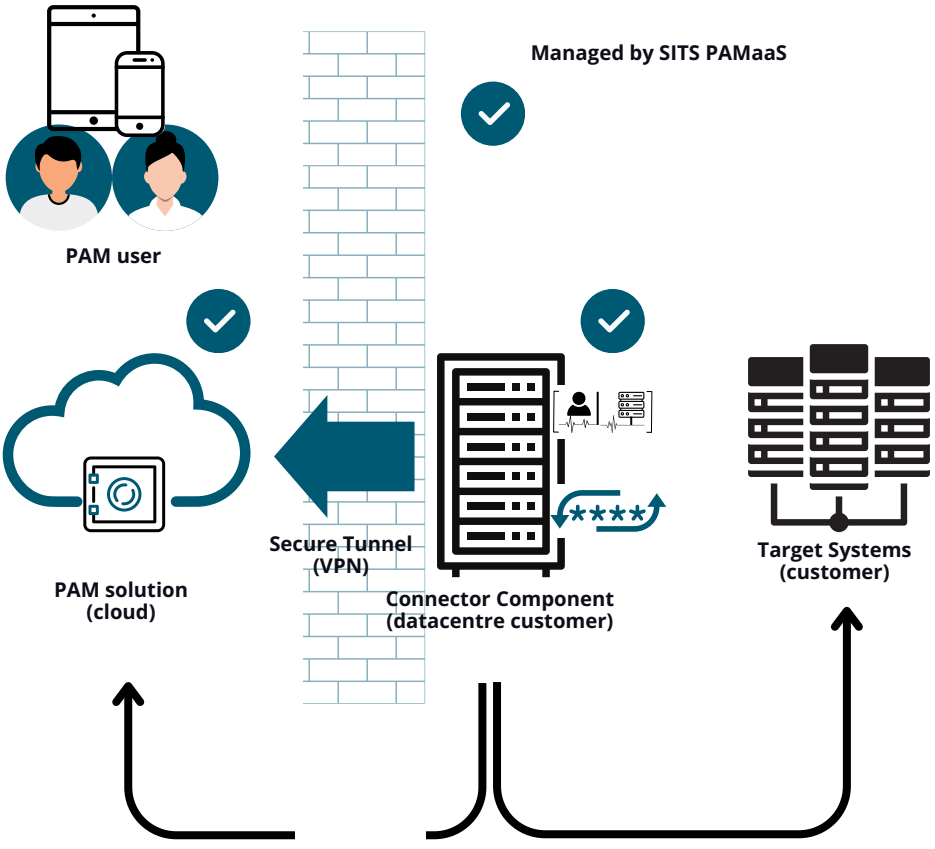
Applying zero standing privileges to operational accounts through ephemeral access is the new standard in privileged access management. More and more PAM solutions also offer this feature, allowing you to protect your organization even more effectively against cyber-attacks. And for the types of privileged accounts, such as application accounts or built-in accounts, that persist through standing privileged the PAM digital vault can be utilized to centrally protect and manage these privileged accounts.

Zero standing privileges are granted through ephemeral access. As soon as the period has elapsed, the user is logged off and the privileged account is automatically removed.

PAM as a secure remote access solution

In today's world, more and more work is carried out remotely, by internal employees, external employees, and suppliers. Offering the right capabilities for remote security and management access to target systems can be challenging and expensive. These include, for example, providing laptops, VPN solutions or remote desktop solutions such as Citrix. And don't forget the activities involved in managing it and keeping it safe.

PAM session management in combination with an additional PAM remote access module makes it possible to provide secure remote management access to target systems. Access can then be provided by means of the web browser without requiring the use of VPN or remote desktop solutions. The PAM remote access module is secured and use of multi-factor authentication is mandatory. Based on the assigned authorizations in PAM, only the required privileged accounts are made available. As with the internal use of session management, no passwords of privileged accounts will be shown to users. The use will also be fully recorded in the logging of PAM to ensure traceability.



SITS PAM as a Service (PAMaaS)

While PAM is a very crucial solution to have in place to secure privileged access to critical systems and to adhere to compliancy regulations and laws, the implementation can be considered challenging, especially for small and medium enterprises (SME's). This is due to the fact that a successful implementation requires knowledge, resources and pre-investments, which are difficult to gain. Resulting in pushbacks of PAM implementations with all the potential risks that arise and not adhering to security compliancy.

For all organizations that are in need of a PAM functionality and experiencing challenges, SITS has developed PAM as a Service (PAMaaS). The goal of PAMaaS is that organizations can be unburdened on knowledge and resources for the implementation of the PAM solution but can use a top notch PAM solution. All the knowledge and best-practices that have been developed by SITS over the years have been standardized in design, approach, implementation and management processes and ownerships. Now organizations can protect their most valuable assets with the following advantages;

- Easy acquisition based on "plug & play" PAM solution;
- Get best-in-class PAM features covering all above mentioned PAM use cases including remote 3rd party vendor access and ephemeral access. Based on PAM leading technology from CyberArk, who has been named leader by Gartner, Kuppingercole and Forrester;
- Swift implementation to adhere to compliancy, laws & regulations;
- Unburdened on resource & knowledge challenges within your organization;
- Highly scalable and a ideal fit for small & medium enterprises;
- Transparent pricing and predictable charges.

"We are thrilled that, besides large enterprises, we can provide small and medium-sized enterprises access to CyberArk technology for controlling, monitoring, and securing access to critical systems and sensitive information by privileged users within their organizations. We are proud that we are the first to offer services to SME cloud-based, fully managed, up and running in 6 weeks, at an affordable fixed monthly fee, and without any one-time cost."

Brian de Vries, Teamlead PAMaaS

PAMaaS is fully standardized and managed

With the PAMaaS standardizations developed by SITS, organizations are unburdened on resourcing and knowledge, resulting in minimizing possible delays on the successful onboarding of PAM, while the customer security professionals are able to fulfill their core responsibilities within the organization. The following standardizations are developed;

- **Architecture;** a dedicated cloud-tenant for secure storage of, and access to, privileged credentials, with connectors on customer infrastructure for secure communications and integrations such as target systems, LDAPs and SIEM. The architecture and all pre-requirements are fully documented and available for the customer.
- **Onboarding and configuration; w**hile the onboarding is performed at it most efficient, all related configurations are pre-defined based on the best practices that have been developed over the years. No worries for the customer about logical naming conventions, authorization models and connection components. And all configuration is applied by automation.
- **Documentation;** as part of standardized documentation, the customer receives a pre-requisites list, solution design, Service Level Agreement (SLA), Quick Reference Cards (QRC's) and reports.
- **Processes;** a very important aspect of a successful PAM implementation are the processes around the management and usage of the PAM solution. With our standardized processes, a transparent way of working is created for any on- or offboarding of users/teams, but also for other service requests or incident handling when required. And not to forget, also the Software Life Cycle Management in conducted via a standardized process and fully executed by SITS as part of PAMaaS.

"We are delighted to partner with SITS, a leading player in cybersecurity. The combination of our managed services provider partnership with SITS and their unique PAM as a Service offer marks a significant milestone in our commitment to delivering first-class PAM services to clients of all sizes. With most of breaches involving privileged accounts, this collaboration underscores our dedication to enhancing security measures for reducing the risk of data breaches and ensuring adherence to regulatory standards."

Renske Galema, Area Vice President Northern Europe at CyberArk

CYBERARK®

In summary

Reduce the risk of data breaches and ensure adherence to regulatory standards. PAM as a Service is an unique offering leveraging CyberArk's advanced technologies to deliver PAM as a service that secures, manages, and monitors privileged access in small, medium and large enterprises.

Benefits PAM as a Service:

- Fully managed by SITS (MSP) Cloud Based PAM solution from CyberArk;
- Up and running in 6 weeks;
- No set-up charges, only a fixed monthly fee;
- Standardized processes and fully managed by certified specialists;
- Highly scalable also fit for small and medium-sized enterprises.

Get Started!

Request your Demo or Webinar!

Sign up for a Demo or Webinar now and discover how to enhance your security measures. Reduce the risk of data breaches and ensure adherence to regulatory standards.

Receive your pricing quotation in 48 hours!

- No set-up charges;
- Only a fixed monthly fee;
- Scalable in Users;
- Transparent & predictable.

info.de@sits.com
info.ch@sits.com
info.dk@sits.com
info.nl@sits.com

www.sits.com