Systancia Cleanroom session

Privileged Access Management (PAM)

Your concerns are our concerns

As a **CISO**, you must **manage your cyber risk** by assessing, protecting, and controlling your privileged accounts and administered resources. You must meet increasing **regulatory compliance** obligations (NIS, LPM, ISO 27001, etc.), as well as more and more demanding **certifications** (HDS, ANSSI, etc.). Moreover, long and expensive audits are regularly carried out.

Your information system is **growing every day**, with new resources to administer, scattered between your **data centers and the different Cloud infrastructures** you operate.

You also need to **control user access** by identifying "who logged on to what and what did he do?", video **recording** all administrative actions and **analyzing** them in real time and a posteriori.

As a **CIO**, you must manage **staff turnover** and ensure "just-in-time" management of the assignment and withdrawal of administration authorizations. You must also **avoid communicating administration accounts** to administrators, outsourcers, and providers to limit the risk of password disclosure.

Finally, you must secure the **access of service providers** from outside your information system by restricting access and rights to a minimum ("**Zero Trust**" policy) and by securing communication flows.

Phone: +33 (0)**3 89 33 58 20**
www.**systancia**.com

Systancia Cleanroom Session Service: The PAM solution as a Service for all

Systancia Cleanroom Session Service is a "Privileged Access Management" (PAM) product. It allows to define administration accesses to resources by controlling the accounts used to authenticate on the resource and by finely tracing all the actions performed.

The administration of a resource consists of a protocol access on a server (RDP, SSH, Web, ...) that represents a risk to the functioning of your organization.

The approach "As a Service" allows you to drastically increase your security level in a simple and quick way, without investing infrastructure and time, to protect you from cyber attacks (ransomware, crashing, denial of service, data theft, etc.) which are more and more threatening.

These attacks may also have long-term consequences on your company's image deficit or for sanctions imposed by the GDPR in case of serious negligence.

Protect yourself from risky scenarios such as:

Untraceable access to your information system

Your service providers and administrators use generic administration accounts (e.g. root, Administrator), so it is impossible to know who is "behind the keyboard" and to trace who initiated an action.
Systancia Cleanroom Session Service requires each administrator to authenticate themselves individually on the PAM, then automatically injects the real administration accounts into the administered resources.

Malicious former administrators

A former administrator, or service provider who knew your administration accounts, could use it to access your servers to propagate a ransomware or steal your data.
Systancia Cleanroom Session Service applies regular password rotation to ensure that no passwords remain accessible on the loose.

Multiplication of external access to administered resources

Exceptional situations such as epidemics, strikes or harsh weather conditions require increased external access to your servers.
Systancia Cleanroom Session Service is an immediately scalable cloud service, natively supporting external access in complete security without requiring the deployment of an agent on the workstation.

Operational interruption due to an administration action

A malicious or clumsy administrator or provider has disrupted a service that is necessary for the proper functioning of your company.
Systancia Cleanroom Session Service records administration sessions in video format and automatically analyzes their content to quickly find the context and changes made.

Why you should choose Systancia Cleanroom Session Service

› Deployment of a PAM solution **in a few hours** while limiting operating costs.

› Native integration of secure external access to **facilitate the deployment** of the solution.

› Reduce **service restoration time** by immediately reacting in case of a malicious action and by tracing the origin of changes.

› Ensure the identity of the user to reduce the risk of **identity theft** and **data leaks.**

› Prevent password leakage to reduce the risk of **non-identified connections.**

› All recorded traces are stored on your local network for **maximum confidentiality.**

A deployment offer adapted to your needs

Systancia
Cleanroom
session

Hybrid Cloud Service - Systancia Cleanroom servers are managed by Systancia and Cleanroom Gateways are deployed in your datacenters

Rapidly deployable

Open your first accesses in a few hours without needing to modify your network architecture

Economically flexible

Your subscription contract prepares you for any situation, and you only pay for what you use

---

Systancia Cleanroom Session Service is based on Systancia Gate, which has received the CSPN certification (First Level Security Certification) issued by the ANSSI in the field of identification, authentication and IS access control. This certification guarantees the reliability, robustness and impermeability to external eyes to ensure the security of external access to the IS for administrations, OVIs (Operators of Vital Importance), OES (Operators of Essential Services) and, more generally, companies.

Systancia is committed to providing the most innovative products on the market. This philosophy has been recognized by Kuppingercole, which ranks Systancia Cleanroom Session Service as an Innovation Leader in the Leadership Compass for PAM in May 2020.