Systancia Cleanroom

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** privileged users **access** by identifying "who logged in to do what" by **recording** in video format and **analyzing** in real time and “a posteriori” all administration actions.

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.

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

Systancia Cleanroom: The PAM solution that adapts the control level to the context of interventions.

Systancia Cleanroom 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 control level and traceability can be adapted to the criticality of the intervention context.

The administration of a resource consists of an access presenting a risk for the operation of your organization. This access is carried out by a protocol access on a server (RDP, SSH, Web, ...) or by using an administration application.

Standard Level:

For internal administrators and usual tasks

Systancia Cleanroom allows to **discover and detect** the accounts used to administer resources and thus **monitor, record and audit** every access to them. It is thus possible to perform **precise searches** on all the recorded sessions to find the origin and context of a specific modification. Access to resources is protected by **strengthening the authentication** before connection, and by **injecting the privileged accounts** used on the administered resources.

Advanced Level:

For mobile administrators and sensitive tasks

For more sensitive intervention contexts, Systancia Cleanroom allows to **block** the actions of administrators **in real time** and **automatically rotate** the passwords of the privileged accounts used. Systancia Cleanroom also provides a **systematic encryption of connection flows**. Cleanroom Authograph, a **continuous authentication** feature, guarantees the identity of the connected administrator at any moment. Cleanroom Application Credential Manager allows the injection of authentication secrecy into a **program-to-program interaction** (AAPM: Application-to-application Password Manager). Finally, Cleanroom Desk provides immediate support for **all types of administration applications** without any further development.

Full Level:

For highly regulated providers and contexts

Finally, for the highest-risk intervention contexts, Systancia Cleanroom provides an optimal level of security, providing administrators with a **sterile and disposable virtual administration workstation**. This virtual workstation can be **standardized by administrator profile**. Systancia Cleanroom Terminal secures access to virtual desktops with a **tamper-proof access terminal** (without OS). Finally, **ultra-secure file transfer** from and to administration networks is possible thanks to Systancia Cleanroom Hawkeye.

Systancia Cleanroom

Privileged Access Management (PAM)

Why you should choose Systancia Cleanroom?

- Ensure **regulatory compliance** by guaranteeing the integrity of the administration workstation.
- Native integration of secure external access to **limit deployment costs** and ensure transparent access ergonomics for all mobile administrators and service providers.
- Reduced **service restoration time** by reacting immediately in case of a malicious action and by tracing the origin of the 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.**
- Protection against **infection risks** by reducing the attack surface, preventing the use of non-validated tools, and controlling file transfer rights and integrity.
- Ensure the integrity of the access terminal to reduce the risk of **terminal contamination.**

A deployment offer adapted to your needs

Several deployment options for Systancia Cleanroom

Systancia Cleanroom

Software product, where Systancia Cleanroom servers are deployed in your datacenters

Adaptable deployment mode

Offer provided as a softwar product or an appliance to adapt to your needs

Economically adaptable

License depending on the number of simultaneous users proposed as an acquisition or subscription

Systancia Cleanroom session / desk

Hybrid Cloud service, where 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’s solution offers all the classic features of bastion hosts, which are always more or less the same. The difference, however, is precisely the Cleanroom element. This is the only solution that solves the usurpation of administration rights issue.”

Yann Renaud
Head of Cross-functional Projects, Architecture and IT Security - Klesia

"Beyond being a key element in our process of obtaining ISO 27001 and HDS certifications, Systancia Cleanroom allows us to monitor all administration actions and thus ensure that there are no data leaks, which can be extremely damaging in the health sector where data is inherently sensitive."

Christophe Le Lostec
DSI - A2COM

ANSSI Certification: Systancia Cleanroom 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.

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