



Privileged Access Management (PAM)

Vos préoccupations sont les nôtres

En tant que **RSSI** vous devez **gérer votre risque cyber** en évaluant, en protégeant et en contrôlant vos comptes à privilèges et vos ressources administrées. Vous devez répondre à des obligations de **conformité réglementaire** de plus en plus nombreuses (NIS, LPM, ISO 27001, etc.), ainsi que des **certifications** de plus en plus contraignantes (HDS, ANSSI, etc.). Cela s'accompagne régulièrement d'**audits** longs et coûteux.

Votre système d'information **s'étouffe quotidiennement** avec de nouvelles ressources à administrer éparpillées entre **vos datacenters et les différentes infrastructures cloud** que vous exploitez.

Vous devez aussi assurer un **contrôle des accès** des utilisateurs à pouvoir en identifier « qui s'est connecté à quoi pour faire quoi » en **enregistrant** au format vidéo et en **analysant** en temps réel et a posteriori toutes les actions d'administration.

En tant que **DSI** vous devez gérer la **rotation du personnel** et assurer une gestion « juste à temps » de l'attribution et du retrait des habilitations des administrateurs. Vous devez aussi **éviter de communiquer les comptes d'administration** aux administrateurs, infogérants et prestataires afin de limiter les risques de divulgation de mots de passe.

Enfin vous devez sécuriser **l'accès des prestataires** depuis l'extérieur à votre système d'information en restreignant au plus juste les accès et les droits attribués (politique de « **Zero Trust** ») et en sécurisant les flux de communication.

Systancia Cleanroom : La solution de PAM qui adapte le niveau de contrôle au contexte des interventions.

Systancia Cleanroom est un produit de « Privileged Access Management » (PAM). Il permet de définir des accès d'administration à des ressources en contrôlant les comptes utilisés pour l'authentification sur la ressource et en traçant finement toutes les actions réalisées. Le niveau de contrôle et de traçabilité peut s'adapter à la criticité du contexte d'intervention.

L'administration d'une ressource consiste en un accès présentant un risque pour le fonctionnement de votre organisation. Cet accès procède par un accès protocolaire sur un serveur (RDP, SSH, Web, ...) ou par l'utilisation d'une application d'administration.

Niveau Standard :

Pour les administrateurs internes et les tâches usuelles

Systancia Cleanroom permet de **découvrir et détecter** les comptes utilisés pour administrer les ressources et ainsi de **surveiller, enregistrer et auditer** l'ensemble des accès à celles-ci. Il est ainsi possible de faire des **recherches précises** sur l'ensemble des sessions enregistrées pour retrouver l'origine et le contexte d'une modification. L'accès aux ressources est protégé par un **renforcement de l'authentification** en amont de la connexion, et par **l'injection des comptes à privilèges** utilisés sur les ressources administrées.

Niveau Avancé :

Pour les administrateurs en mobilité et les tâches sensibles

Pour les contextes d'interventions plus sensibles, Systancia Cleanroom permet de **bloquer en temps réel** les actions des administrateurs ainsi que d'opérer des **rotations automatiques** des mots de passe des comptes à privilèges utilisés. Systancia Cleanroom apporte aussi un **chiffrement systématique des flux de connexion**. La fonctionnalité Systancia Cleanroom Authograph d'**authentification continue** assure l'identité en permanence de l'administrateur connecté. Systancia Cleanroom Application Credential Manager permet l'injection de secret d'authentification dans une **interaction de programme à programme** (AAPM : Application-to-application Password Manager). Enfin Systancia Cleanroom Desk permet la prise en charge immédiate et sans développement de **tout type d'applications d'administration**.

Niveau Complet :

Pour les prestataires et les contextes hautement réglementés

Enfin pour les contextes d'intervention les plus à risques, Systancia Cleanroom apporte un niveau de sécurité optimal, en fournissant aux administrateurs un **poste virtuel d'administration stérile et jetable**. Ce poste virtuel peut être **standardisé par profil d'administrateur**. Systancia Cleanroom Terminal sécurise l'accès aux bureaux virtuels avec un **terminal d'accès inviolable** (sans OS). Enfin le **transfert de fichier ultra-sécurisé** depuis et vers les réseaux d'administration est possible avec Systancia Cleanroom Hawkeye.

Pourquoi Systancia Cleanroom

- › Assurer la **conformité réglementaire** en garantissant l'intégrité du poste d'administration.
- › L'intégration native des accès externes sécurisés pour **limiter les coûts de déploiement** et assurer une ergonomie d'accès transparente pour l'ensemble des administrateurs en mobilité et prestataires.
- › Réduction des **délais de remise en service** en réagissant immédiatement en cas d'action malveillante et en retrouvant l'origine des modifications.
- › Assurer l'identité de l'utilisateur pour réduire les risques d'usurpation d'identité **et les risques de fuites de données**.
- › Empêcher les fuites de mot de passe pour réduire les risques de **connexions non identifiées**.
- › Protection contre les **risques d'infection** en réduisant la surface d'attaque, en empêchant l'utilisation d'outils non validés et en contrôlant les droits et l'intégrité des transferts de fichier.
- › Assurer l'intégrité du terminal d'accès pour réduire les risques **d'infection par le terminal**.

Une offre de déploiement adaptée à vos besoins

Systancia Cleanroom propose plusieurs options de déploiement :

Systancia Cleanroom

Produit logiciel, où les serveurs Systancia Cleanroom sont déployés dans vos datacenters



Mode de déploiement adaptable

Offre proposée sous format de produit logiciel ou d'appliance pour s'adapter à votre besoin



Adaptable économiquement

Licence au nombre d'utilisateurs simultanés proposée en acquisition ou en souscription

Systancia Cleanroom session



Systancia Cleanroom desk



Service Cloud hybride, où les serveurs Systancia Cleanroom sont managés par Systancia et les Cleanroom Gateway sont déployés dans vos datacenters



Rapidement déployable

Ouvrez vos premiers accès en quelques heures sans avoir besoin de modifier votre architecture réseau



Flexible économiquement

Votre contrat de souscription vous prépare à toute éventualité, et vous ne payez que ce que vous consommez

« La solution de Systancia propose toutes les fonctions classiques des bastions qui sont globalement toujours plus ou moins les mêmes. Mais la différence réside précisément dans son côté Cleanroom. C'est la seule solution qui règle le problème d'usurpation des droits administrateurs. »

Yann Renaud

Responsable Pôle Projets Transverses, Architecture et Sécurité Informatique - Klesia

« Au-delà d'être un élément clé dans notre processus d'obtention des certifications ISO 27001 et HDS, Systancia Cleanroom nous permet de monitorer l'ensemble des actions d'administration et ainsi de nous assurer qu'il n'y ait pas de fuites de données, qui peuvent être extrêmement préjudiciables dans le domaine de la santé où les données sont sensibles par essence. »

Christophe Le Lostec

DSI - A2COM

KLÉSIA
PROTECTION ET INNOVATION SOCIALES

A2COM
RESADIA



Systancia Cleanroom s'appuie sur la base technologique de Systancia Gate ayant reçu la certification CSPN (Certification de Sécurité de Premier Niveau) délivrée par l'ANSSI pour l'identification, l'authentification et le contrôle des accès au SI. Cette certification est une garantie de fiabilité, de robustesse et d'imperméabilité aux regards externes pour assurer la sécurité des accès externes au SI des administrations, des OIV (Opérateurs d'Importance Vitale), OSE (Opérateurs de Services Essentiels) et plus largement des entreprises.



Systancia s'attache à proposer les produits les plus innovants du marché. Cette philosophie a été reconnue par Kuppingercole qui classe Systancia Cleanroom comme Innovation Leader dans le Leadership Compass for PAM publié en Mai 2020.