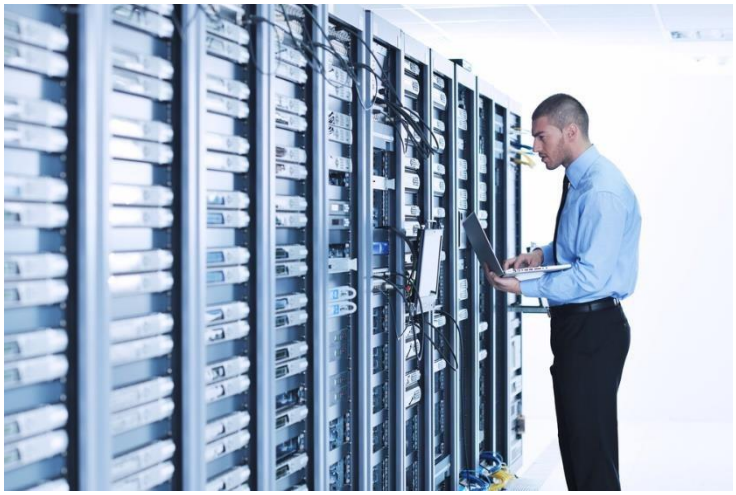
KUMO
The Cloud by arcITek

Systancia

Pourquoi vous faut-il plus qu'un bastion pour sécuriser vos postes de travail administrateurs ?

Bastion & PAM

Le terme « bastion » réfère à un hôte exposé au réseau externe (non réputé de confiance). En règle générale, un bastion informatique vise à protéger un réseau ou une partie d'un réseau de menaces extérieures ; il constitue en conséquence l'élément le plus exposé, celui qui est susceptible de subir un maximum d'attaques de la part d'agents menaçants externes. Si un bastion « tombe » alors c'est toute l'organisation protégée qui sera impactée.



Une solution PAM peut être vue comme un bastion en informatique permettant, notamment de tracer et surveiller des utilisateurs à pouvoirs ainsi qu'éventuellement analyser en temps réel des données et comportements afin de détecter des actes suspicieux ou anormaux.

Le bastion a cependant plusieurs écueils. Celui-ci n'est pas forcément à jour et, pour les administrateurs, il constitue **une contrainte qui est contournée** lorsqu'ils en ont la possibilité. L'analogie militaire peut évoquer une forteresse statique et donc contournable alors qu'une armée moderne se veut composée de petites unités d'interventions agiles, embarquant leurs moyens de défense.

En résumé, une solution PAM est techniquement intéressante pour la gestion ainsi que la surveillance des comptes à privilèges (internes et/ou externes). Mais comme le rappelle l'ANSSI dans ses ***recommandations relatives à l'administration sécurisée des systèmes d'information***, comme tout produit de sécurité, de surcroît disposant d'un nom commercial pouvant procurer un sentiment de sécurité, il est important d'être vigilant sur le choix, le déploiement et l'exploitation d'une telle solution : « Le déploiement d'un bastion pour les actions d'administration ne se substitue évidemment pas […] au cloisonnement du SI d'administration et à la sécurisation du poste d'administration ».

Dans ce contexte, comment traiter le cas d'un **infogéreur** ou d'une **administration à distance** depuis un **poste non maîtrisé** ? En effet, il est illusoire de penser qu'un poste dédié sera utilisé pour chaque réseau administré. La propagation d'un virus entre deux réseaux différents administrés par le même infogéreur devient alors possible.

Recommandations de l'ANSSI relative à l'administration sécurisée des SI (extrait)

- ✓ **R9** : Utiliser un poste d'administration dédié
- ✓ **R9-** : Utiliser un poste d'administration multi- niveaux
- ✓ **R9--** : Utiliser un poste d'administration avec accès distant au SI bureautique
- ✓ **R15** : Connecter les ressources d'administration sur un réseau physique dédié
- ✓ **R15-** : Connecter les ressources d'administrationsur un réseau VPN IPsec dédié
- ✓ **R16** : Appliquer un filtrage interne et périmétrique au SI d'administration
- ✓ **R17** : Appliquer un filtrage local sur les ressources administrées
- ✓ **R18** : Dédier une interface réseau physique d'administration
- ✓ **R18-** : Dédier une interface réseau virtuelle d'administration
- ✓ **R21** : Protéger les flux d'administration transitant sur un réseau tiers
- ✓ **R27** : Utiliser des comptes d'administration dédiés
- ✓ **R29** : Réserver les comptes d'administration aux seules actions d'administration
- ✓ **R30** : Utiliser par défaut des comptes d'administration individuels
- ✓ **R32** : Prévoir un processus de gestion des comptes d'administration
- ✓ **R34** : Modifier les mots de passe par défaut des comptes natifs
- ✓ **R35** : Stocker les mots de passe dans un coffre- fort de mots de passe
- ✓ **R36** : Privilégier une authentification à double facteur pour les actions d'administration
- ✓ **R38** : Privilégier une authentification centralisée

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

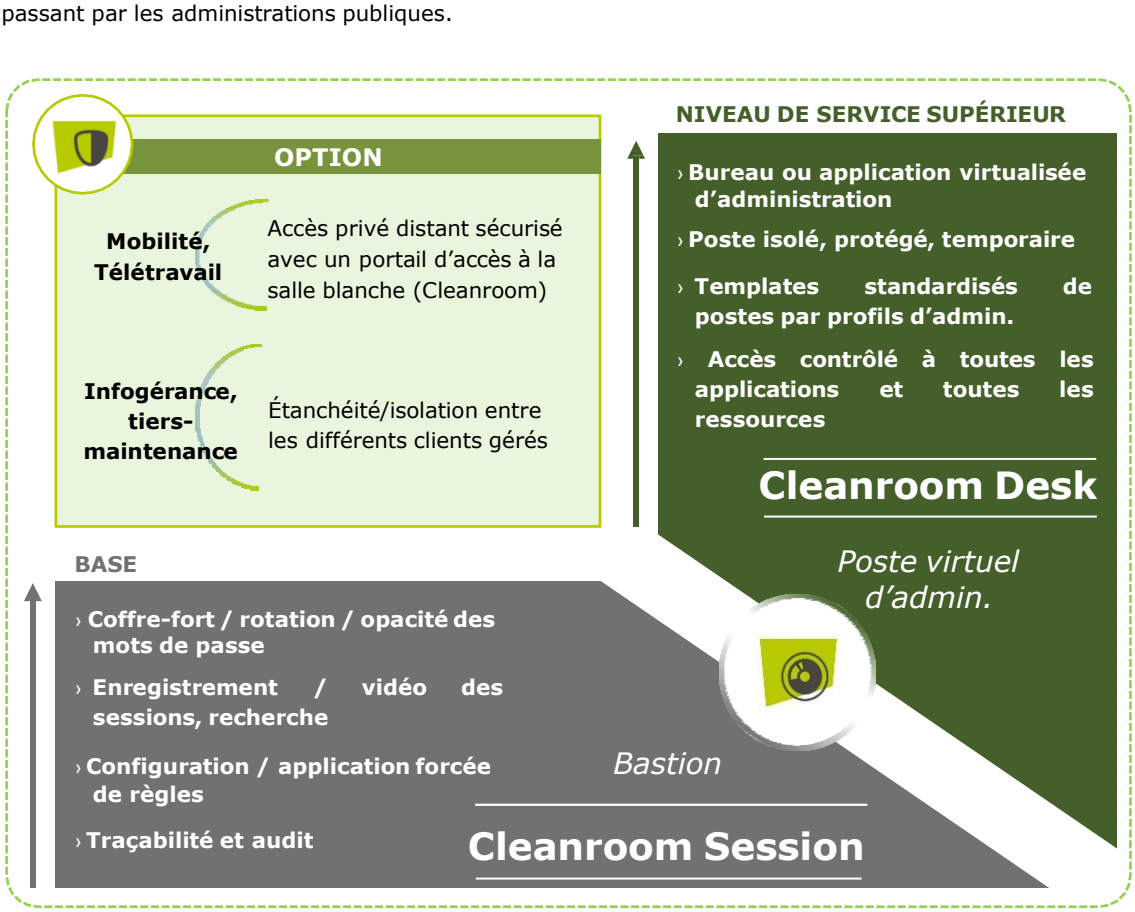
KUMO
The Cloud by arcITek

Systancia

Pourquoi vous faut-il plus qu'un bastion pour sécuriser vos postes de travail administrateurs ?

Bastion vs Cleanroom

Systancia Cleanroom propose une autre approche du PAM, pour un système de défense moderne avec le seul poste d'administration virtuel stérile et jetable qui va bien au-delà du bastion classique. Systancia Cleanroom répond en effet à certaines recommandations et problématiques non adressées par les autres solutions de PAM. Elle se veut modulable et évolutive afin de coller au plus près des attentes de l'entreprise ou de l'organisation cliente et permet ainsi d'adresser tous types de profils, des ETI aux grands comptes, en passant par les administrations publiques.



PRODUIT COMPLÉMENTAIRE

Gestion des identités et des habilitations des utilisateurs à pouvoir et des comptes à privilèges. **Gestion des changements**, de la **rotation** et de la **mutation** du personnel (des utilisateurs et des administrateurs)

Systancia Identity

IAM pour comptes PAM

KLESIA
PROTECTION ET INNOVATION SOCIALES

Retour d'expérience : Klesia a choisi Systancia Cleanroom

« 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

Après une étude du marché des bastions, Klesia, groupe de protection sociale à but non lucratif a lancé un appel d'offre auprès de 7 éditeurs de solutions. Lorsqu'un test d'intrusion sur le LAN a démontré que les comptes d'administrateurs devaient être mieux protégés afin d'éviter l'usurpation de leurs droits, Systancia Cleanroom s'est démarquée des autres acteurs grâce à sa capacité à adresser cette problématique à laquelle les autres solutions ne pouvaient pas répondre. Deuxième élément déterminant, le mode de **licensing à l'utilisateur simultané, ressources illimitées**, s'est révélé être un point majeur dans le processus de choix étant donné que ce mode de licensing est particulièrement adapté lorsque l'entreprise a recours à de l'**infogérance**, ce qui est le cas du groupe Klesia.

KUMO
The Cloud by arcITek

Systancia Cleanroom

Pourquoi vous faut-il plus qu'un bastion pour sécuriser vos postes de travail administrateurs ?

4 différentiateurs clés de Systancia Cleanroom

1

Bastion	Ne permet l'accès qu'aux ressources gérées par le bastion
Cleanroom	Permet nativement l'accès à toutes ressources quelles qu'elles soient

2

Bastion	Accès sécurisé uniquement aux administrateurs présents dans le réseau de l'entreprise
Cleanroom	Accès sécurisé pour tous les administrateurs y compris les administrateurs à distance et les administrateurs nomades

3

Bastion	Poste d'administrateur gardant des traces des actions d'administration précédentes
Cleanroom	Des masters uniques, personnalisés et stériles à chaque session d'un administrateur

4

Bastion	Mode de licensing par ressource ou par utilisateur nommé
Cleanroom	Mode de licensing à l'utilisateur simultané, ressources illimitées

KUMO
The Cloud by arcITek

Systancia Cleanroom

Pourquoi vous faut-il plus qu'un bastion pour sécuriser vos postes de travail administrateurs ?

Les technologies au service de la Cleanroom

L'association de différents types de solutions permet de répondre de manière exhaustive aux recommandations de l'ANSSI relatives à l'administration sécurisée des SI. Cependant, l'intégration et la coordination de ces solutions hétéroclites au sein du SI d'un client peut s'avérer fastidieuse et être source de dysfonctionnements. Une solution unifiée telle que Systancia Cleanroom permet de faciliter la protection du SI en se substituant à des solutions multiples répondant indépendamment à certaines des recommandations de l'ANSSI.

FONCTIONNALITÉS	Bastion	Cleanroom
Solution de PAM qui prend en compte la problématique "poste d'administration" et qui permet la séparation du poste d'admin du poste bureautique (R9)	-	++
Aider à la mise en œuvre d'un poste d'administration multi-niveaux (plusieurs environnements sur le même poste) (R9-)	-	++
Mettre à disposition un poste virtuel bureautique à partir d'un poste d'administration (R9--)	-	++
S'insérer facilement dans une architecture avec un réseau dédié, physique ou virtuel (R15, R15-), et une interface réseau dédiée, physique ou virtuelle (R18, R18-)	+	++
Accès aux ressources administrées depuis le réseau d'administration : filtrage réseau entre les outils d'administration et les ressources administrées (pare-feu applicatif, R16, R17)	++	++
Sécuriser nativement le passage du flux d'administration par un réseau tiers (R21) - Administration à distance (infogérance, tierce-maintenance) - Nomadisme (télétravail, mobilité)	+	++

L'intégralité des recommandations de l'ANSSI relatives à l'administration sécurisée des systèmes d'information sont accessibles sur https://www.ssi.gouv.fr/entreprise/guide/securiser-ladministration-des-systemes-dinformation/

« Bastion » et « poste d'administration »

- Le « bastion » ne suffit donc pas : il est également nécessaire de sécuriser le poste d'administration.
- De la même manière que l'ANSSI recommande de ne pas accéder à un poste d'administration depuis un poste bureautique, elle recommande de ne pas accéder à un « bastion » depuis un poste bureautique.
- Il convient donc de sécuriser le poste d'administration indépendamment de toute solution de « PAM » retenue.
- Systancia Cleanroom apporte des nouvelles approches de sécurisation du poste d'administration dans les environnements réels et souvent virtualisés des organisations actuelles.

Systancia