Systancia Workroom session

ZTNA : Zero Trust Network Access

Vos préoccupations sont les nôtres

En tant que **RSSI**, vous voulez réduire le **risque VPN** pour vous adapter aux nouveaux besoins de mobilité et d'usage dans le cloud, ou vous avez des besoins de **traçabilité** complète et granulaire de tous les accès externes, ou encore une obligation de **conformité réglementaire** pour répondre aux réglementations NIS, LPM, ISO, etc.

En tant que **DSI**, vous avez des projets de **télétravail** organisé ou massif avec des cas d'usages variés, vous avez des **accès prestataires** que vous souhaitez contrôler rigoureusement, ou des projets de **migration cloud** complexes où les notions d'accès réseau ne conviennent pas, ou enfin des enjeux de **continuité d'activité** en cas de circonstances exceptionnelles.

Vous êtes Responsable de l'informatique **Utilisateur** et vous avez besoin d'une solution apportant le meilleur compromis entre **sécurité et ergonomie**, une solution **simple** à utiliser, tout en n'ayant aucun impact sur la **productivité** des utilisateurs.

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

Systancia Workroom Session : La sécurisation de tous les accès distants de tous les acteurs de votre écosystème, dans tous les contextes d'accès, à toutes vos applications, on premise ou en service cloud.

Systancia Workroom Session est un produit de « Zero Trust Network Access » (ZTNA). Il permet de définir des accès à des applications (web ou client-serveur) ou des ressources (serveurs ou partages de fichier) finement en fonction de l'utilisateur et de ses conditions de connexion, et qu'elles soient dans un ou plusieurs datacenters, gérées par l'entreprise ou par un prestataire de services cloud. Il permet de prendre en compte une grande variété de scénarios d'accès, depuis des postes maitrisés, du BYOD ou des prestataires tiers.

Portail d'accès unifié aux ressources

Systancia Workroom Session propose un portail d'accès centralisant toutes les ressources et applications mises à disposition de l'utilisateur. Les mécanismes de **SSO (Single Sign-On)** intégrés dans le produit offrent un confort supplémentaire aux utilisateurs en augmentant leur productivité et augmentent la sécurité dans les cas d'usages d'accès prestataires. Les ressources et applications sont accessibles à travers le portail web **avec ou sans agent** sur le poste pour répondre également aux enjeux de BYOD ou de postes non maîtrisés.

Architecture centrée utilisateur et non plus centrée réseau

L'architecture à double barrières de Systancia Workroom Session permet d'offrir des accès spécifiques sur des applications au lieu d'ouvrir des accès larges à des réseaux. Cette approche permet une plus grande précision sur les ouvertures d'accès et une plus grande sécurité du système d'information. Cette architecture offre très facilement des accès **multisites**, permettant d'accéder depuis un portail unique à des applications et des ressources réparties sur plusieurs datacenters, gérées par l'entreprise ou par un prestataire de services cloud.

Politique du moindre privilège (« Zero Trust »)

Avec Systancia Workroom Session, vous pouvez définir des profils d'accès permettant d'**adapter dynamiquement les droits** en fonction de la confiance donnée à l'utilisateur. Cette confiance se construit sur son authentification, renforcée par des mécanismes d'**OTP (One Time Password)** et par les conditions d'accès de l'utilisateur, basées sur du **contrôle de conformité** du poste pouvant vérifier l'identité et la santé du terminal d'accès ainsi que des critères d'accès comme le lieu ou l'heure de connexion.

Une protection complète

La **rupture protocolaire** disponible dans Systancia Workroom Session est un bouclier contre le risque malware, ransomware ou d'autres infections par le protocole. La **traçabilité** complète des connections facilite l'analyse forensic, et réduit donc les délais de remise en service en cas d'attaque.

Systancia Workroom session

ZTNA : Zero Trust Network Access

Pourquoi Systancia Workroom Session

- Une solution unique pour tous les cas d'usages d'accès distants permettant d'**optimiser l'investissement**
- Un **coût de déploiement réduit** car ne remettant pas en cause l'existant et centralisant les accès aux différents datacenters
- La certification ANSSI contribuant à l'assurance de la **conformité réglementaire**
- Réduction des **délais de remise en service** après une attaque en facilitant l'analyse forensic
- Authentification forte assurant l'identité de l'utilisateur pour **réduire les risques de fuites de données**
- Des politiques de Zero Trust améliorant la **protection du système d'information**
- **Une protection contre les risques malware**, ransomware, etc. avec de la rupture protocolaire
- Simplicité et rapidité d'accès réduisant les **délais de conduite du changement**
- **Réduction des coûts du parc informatique** en permettant l'accès sécurisé depuis n'importe quel terminal sans avoir à équiper tous vos collaborateurs de postes informatiques
- **Une productivité améliorée** par un confort d'utilisation et un MCO facilité par les mécanismes de hautes disponibilités intégrés
- Un mécanisme d'assistance sécurisée **réduisant les coûts de support**

Une offre de déploiement adaptée à vos besoins

Systancia Workroom session

Service Cloud hybride, où Gate Mediation est managé par Systancia et les Gate Gateway sont déployées 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

« Nous souhaitions pouvoir gérer les accès externes au système d'information en évitant les risques liés au VPN. Avec cette solution zero-trust, nous sommes plus sûrs du contexte d'accès, notamment pour les connexions de nos magasins depuis la Chine : nous pouvons vérifier le poste de travail qui accède au système d'information et avoir une granularité dans la gestion des accès en décidant d'ouvrir certaines applications à certaines personnes au lieu d'ouvrir tout le réseau. »

Clément Cesneut
Infrastructure & Security Manager - Groupe Beaumanoir

GROUPE BEAUMANOIR

« La solution nous a permis de répondre à nos enjeux en matière de continuité d'activité en déployant en 2 jours le télétravail pour 92% de nos agents. Ils retrouvent exactement la même expérience utilisateur que sur leur lieu de travail : ils accèdent à leur bureau RDS avec tous leurs outils et donc peuvent réaliser l'ensemble de leurs tâches, depuis leur poste personnel, sans contrainte, et en toute sécurité. »

Emmanuel Periaux
Responsable Système d'Information - OPH Metz Métropole

OFFICE PUBLIC DE L'HABITAT METZ MÉTROPOLE

Systancia Workroom Session s'appuie sur le produit logiciel Systancia Gate :

Ayant reçu sous le nom IPdiva Secure la certification CSPN (**Certification de Sécurité de Premier Niveau**) délivrée par l'ANSSI dans le domaine « identification, authentification et contrôle d'accès ». 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.

Gartner

Une solution éprouvée et innovante depuis de nombreuses années. Systancia est ainsi cité parmi les éditeurs majeurs de solutions ZTNA dans le **Market Guide for Zero Trust Network Access**, publié par le Gartner en juin 2020, pour sa solution Systancia Gate.