Groupement Hospitalier de Territoire
Grand Paris Nord-Est
Aulnay-sous-Bois - Le Raincy-Montfermeil - Montreuil

Sécuriser tous les accès distants quel que soit le cas d'usage
(télétravailleurs et prestataires)

Enjeux :
> Sécuriser les accès distants au système d'information dans le cadre de la démocratisation du télétravail
> Dissocier les accès distants émanant des agents administratifs et du personnel soignant des accès distants des prestataires informatiques

Solutions :
> Systancia Workroom Session Service
> Systancia Cleanroom Session Service

Bénéfices :
> Une simplicité d'accès au bureau à distance grâce au HTML5
> Une gestion des droits d'accès aux ressources efficace
> Des interventions de prestataires enregistrées et archivées
> Une simplicité du cloud qui apporte rapidité et flexibilité

Les solutions de ZTNA et de PAM en services cloud de Systancia nous permettent de répondre à nos deux enjeux : sécuriser l'accès des télétravailleurs à partir de leurs postes personnels en appliquant le principe de moindre privilège et surveiller les actions des prestataires grâce à l'enregistrement et l'archivage des sessions d'administration. La simplicité apportée par le cloud nous a permis d'activer très rapidement ces services et nous libère par ailleurs d'une charge de travail en matière de gestion des solutions puisqu'elles sont managées par Systancia.

Zehair Benamar
Chef de projet infrastructures

Les enjeux

Le GHT Grand Paris Nord-Est (GPNE) est un groupement des hôpitaux d'Aulnay-sous-Bois, du Raincy-Montfermeil et de Montreuil, né de la loi de modernisation du système de santé du 26 janvier 2016, visant notamment à une mutualisation des ressources des hôpitaux regroupés au sein d'un même GHT (Groupement Hospitalier de Territoire).

Au sein de la DSI, un projet de convergence des systèmes d'information a été mené avec pour objectif d'avoir, in fine, un système d'information commun, avec une équipe commune aux 3 hôpitaux. Cette nouvelle DSI, composée de 60 personnes, gère aujourd'hui plus de 200 applications hétérogènes utilisées quotidiennement par environ 7 000 utilisateurs (entre 2 300 et 2 500 par hôpital) sur des clients lourds et clients légers.

Avant la crise sanitaire liée au Covid-19, certains collaborateurs avaient la possibilité d'accéder à distance à leur environnement de travail depuis des postes maîtrisés via des connexions VPN SSL. Mais la crise sanitaire et la démocratisation du télétravail qui en a découlé a amené la DSI à chercher des solutions plus sécurisées que les VPN SSL pour permettre ces accès distants à l'environnement de travail depuis des postes non maîtrisés. Par ailleurs, la DSI souhaitait dissocier clairement les accès distants des agents administratifs et du personnel soignant des accès distants émanant des prestataires informatiques, nécessitant certaines fonctionnalités spécifiques pour la traçabilité de ces accès.

La solution

Après une phase de POC de deux mois, les solutions de ZTNA (Zero Trust Network Access) et de PAM (Privileged Access Management) en services cloud de Systancia ont été retenues.

Systancia Workroom Session Service (ZTNA) permet de sécuriser les accès des utilisateurs en situation de télétravail, notamment en mettant en œuvre le principe de moindre privilège, c'est-à-dire en ne permettant l'accès qu'aux seules ressources auxquelles l'utilisateur a le droit d'accéder.

Systancia Cleanroom Session Service (PAM) permet de définir pour les prestataires du GHT 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.

Avec respectivement jusqu'à 200 et 10 utilisateurs simultanés sur les solutions Systancia Workroom Session Service et Systancia Cleanroom Session Service, le GHT peut désormais sécuriser l'ensemble des accès distants au système d'information, avec des fonctionnalités adaptées à l'hétérogénéité des profils.

Une simplicité d'accès au bureau à distance grâce au HTML5

L'un des principaux bénéfices de la solution Systancia Workroom Session Service est que l'utilisateur en télétravail ouvre une session directement à travers un navigateur web sans que le service informatique doive intervenir pour installer un agent sur le poste personnel de l'utilisateur, tel qu'en atteste Zehair Benamar, Chef de projet infrastructures au sein du GHT GPNE : *« Les utilisateurs passent par le RDP HTML5, il se loguent avec leur login et mot de passe et accèdent à leur session comme si ils étaient au bureau. »*

Une gestion des droits d'accès aux ressources efficace

Systancia Workroom Session Service permet de mettre en œuvre la politique de moindre privilège (Zero Trust) en adaptant les droits donnés aux utilisateurs en fonction de leurs profils respectifs : un médecin et un agent administratif n'auront ainsi pas accès aux mêmes ressources. Chacun accèdera uniquement aux ressources et applications qui leur sont nécessaires dans le cadre de leurs missions.

Par ailleurs, le ZTNA permet aussi un contrôle de conformité du poste accédant au système d'information du GHT en vérifiant notamment la santé du terminal (présence d'un antivirus, dernières mises à jour de sécurité activées, etc.) ou encore le lieu ou l'heure de connexion pour interdire ou limiter l'accès en fonction de la confiance donnée à l'utilisateur ou au poste de travail.

Ces apports du ZTNA en termes de sécurité, de même que l'accès HTML5 qui permet de ne pas installer d'agent sur le poste de travail a aussi rendu possible des accès distants aux ressources et applications choisies du système d'information par des postes de travail personnels des utilisateurs, sans pour autant faire peser de risque sur la sécurité du système d'information du GHT.

Des interventions de prestataires enregistrées et archivées

Pour Joel Trutaud, Administrateur des systèmes et réseaux au sein du GHT GPNE, l'enregistrement et l'archivage des interventions des prestataires est, avec le coffre-fort de mots de passe, l'une des fonctionnalités clés de Systancia Cleanroom Session Service. La solution permet en effet d'enregistrer l'ensemble des actions des prestataires, de les voir en temps réel, et de les archiver pour ensuite, en cas de besoin, faire des recherches précises sur l'ensemble des sessions enregistrées pour retrouver l'origine et le contexte d'une modification. Le coffre-fort de mot de passe évite quant à lui de donner aux prestataires les mots de passe pour accéder aux serveurs du GHT.

Une simplicité du cloud qui apporte rapidité et flexibilité

Si le GHT a choisi les solutions de ZTNA et de PAM de Systancia en services cloud plutôt qu'en produits on-premise, c'est avant tout pour la simplicité qu'apporte le cloud. Les équipes de la DSI ont pu déployer les services très rapidement sans avoir de serveur supplémentaire à installer et à gérer. Le GHT a une Gateway par site (pour chacun des 3 hôpitaux) pour se connecter sur le serveur de médiation managé par Systancia. Cela permet à la DSI d'éviter une charge substantielle de travail en termes de gestion de l'infrastructure.

À propos de Systancia

Chez Systancia, nous valorisons l'ingéniosité pour innover. Nous associons virtualisation d'applications, cybersécurité et intelligence artificielle pour créer des solutions uniques, reconnues et certifiées. Dans tout environnement de travail, il y a une personne qui mérite d'être en pleine maîtrise et en pleine confiance. C'est notre conviction et notre but. C'est pourquoi des centaines d'organisations publiques et privées choisissent Systancia, pour libérer le potentiel de chacun, en toute confiance. Avec toute notre R&D en France, nous commercialisons nos solutions de virtualisation d'applications (VDI), d'accès réseau privé (ZTNA), de contrôle des utilisateurs à pouvoir (PAM) et de gestion des identités et des accès (IAM) dans le monde entier, avec notre réseau de partenaires.