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

Secure all remote accesses regardless of the use case
(teleworkers and service providers)

Challenges:

- Secure remote access to the information system in the context of telework democratization
- Dissociate remote accesses of administrative and nursing staff from remote accesses of IT service providers

Solutions:

- Systancia Workroom Session Service
- Systancia Cleanroom Session Service

Benefits:

- Easy access to the remote desktop thanks to HTML5
- Efficient management of access rights to resources
- Provider interventions recorded and archived
- Cloud simplicity providing speed and flexibility

Challenges

The “Grand Paris Nord-Est” (GPNE) is a French Hospital Group of Aulnay-sous-Bois, Raincy-Montfermeil and Montreuil, born from the modernization law of the health system (January 26, 2016), designed to mutualize the resources of hospitals grouped together within a single Hospital Group.

Within the IT Department, an Information Systems convergence project has been carried out with the aim of ultimately having a common Information System, with a team common to all three hospitals. This new IT Department, composed of 60 people, now manages more than 200 heterogeneous applications used daily by about 7,000 users (between 2,300 and 2,500 per hospital) on heavy and thin clients.

Before the Covid-19 health crisis, some employees were able to access their work environment remotely from controlled workstations via SSL VPN connections. But the health crisis and the resulting democratization of telework led the IT department to look for more secure solutions than SSL VPNs to allow remote access to the work environment from non-controlled workstations. In addition, the IT Department wanted to clearly separate the remote accesses of administrative agents and nursing staff from the remote accesses of IT service providers, requiring some specific functionalities for the traceability of these accesses.

The solution

After a two-month POC phase, the Hospital Group decided to choose Systancia's ZTNA (Zero Trust Network Access) and PAM (Privileged Access Management) cloud services solutions.

Systancia Workroom Session Service (ZTNA) allows to secure the access of teleworking users, in particular by implementing the principle of least privilege, i.e. by allowing access only to those resources to which the user has the right to access.

Systancia Cleanroom Session Service (PAM) allows the Hospital Group's service providers to define administration access to resources by controlling the accounts used for authentication on the resource and by finely tracing all actions carried out.

With up to 200 and 10 simultaneous users respectively on the Systancia Workroom Session Service and Systancia Cleanroom Session Service solutions, the Hospital Group can now secure all remote accesses to the information system, with functions adapted to the heterogeneity of profiles.

> “*Systancia's ZTNA and PAM cloud services solutions allow to meet our two challenges: securing access for teleworkers from their personal workstations by applying the principle of least privilege and monitoring the actions of service providers thanks to the recording and archiving of administration sessions. The simplicity provided by the cloud allowed us to activate these services very quickly and freed us from managing the solutions, since they are managed by Systancia.*”
>
> ***Zehair Benamar***
> *Infrastructure Project Manager*

Easy access to the remote desktop thanks to HTML5

One of the main benefits of Systancia Workroom Session Service is that the teleworking user opens a session directly through a web browser without the IT department having to intervene to install an agent on the user's personal computer, as Zehair Benamar, (Infrastructure Project Manager at GPNE Hospital Group) can attest: *"Users go through the HTML5 RDP, they log in with their login credentials and access their session as if they were at the office."*

Efficient management of access rights to resources

Systancia Workroom Session Service allows to implement the policy of least privilege (Zero Trust) by adapting the rights given to users according to their respective profiles: a doctor and an administrative agent will therefore not have access to the same resources. Each user will only have access to the resources and applications they need to perform their duties.

Moreover, the ZTNA allows to perform a compliance check of the workstation accessing the Hospital Group’s information system by verifying the health of the terminal (presence of an antivirus, latest security updates activated, etc.) or the location or time of connection in order to prohibit or limit access depending on the trust granted to the user or the workstation.

These security features of ZTNA, along with HTML5 access, which does not require the installation of an agent on the workstation, have also allowed remote access to selected information system resources and applications from users' personal computers, without presenting a security risk for the Hospital Group’s information system.

Provider interventions recorded and archived

For Joel Trutaud, System and Network Administrator at GPNE Hospital Group, the recording and archiving of service provider interventions is, along with the password vault, one of the key features of Systancia Cleanroom Session Service. The solution allows to record all the actions carried out by providers, to see them in real time, and to archive them. In this way, if necessary, it will be possible to make precise searches on all the recorded sessions to find the origin and the context of a modification. The password vault avoids the need to give providers the passwords to access the Hospital Group’s servers.

Cloud simplicity provides speed and flexibility

The main reason the Hospital Group chose Systancia's ZTNA and PAM solutions as cloud services rather than on-premise products was the simplicity of the cloud. The IT teams were able to deploy the services very quickly without having to install and manage any additional servers. The Hospital Group has one gateway per site (for each of the three hospitals) to connect to the mediation server managed by Systancia. This allows the IT department to avoid a significant workload in terms of infrastructure management.

About Systancia

At Systancia, we value ingenuity to innovate. We blend application virtualization, cybersecurity and artificial intelligence to create unique, award-winning and certified solutions. Behind every workplace, there is a person who deserves to be empowered and trusted. This is our belief and our goal. This is why hundreds of public and private organizations choose Systancia, to unlock the potential of everyone, in full trust. With all our R&D in France, we sell our application virtualization (VDI), private access (ZTNA), privileged access management (PAM) and identity and access management (IAM) solutions across the globe, with our valued partners.