Systancia
Workroom
session

ZTNA: Zero Trust Network Access

Your concerns are our concerns

As a **CISO**, you want to reduce **VPN risk** to meet the new needs of mobility and usage in the Cloud, the need for full and granular **traceability** of all external accesses, or the need for **regulatory compliance** to comply with NIS, LPM, ISO regulations, etc.

As a **CIO**, you have **remote access** projects (planned or unplanned) with a variety of use cases, you have **service provider access** that you want to control rigorously, or complex **cloud migration** projects for which the concepts of network access are not appropriate, or **business continuity** issues in exceptional circumstances.

You are in charge of **user** computing and you need a solution that provides the best compromise between **security** and **ergonomics**, a solution that is **easy** to use, while having no impact on user **productivity**.

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

Systancia Workroom Session: Securing remote access for all the users in your ecosystem, in all access contexts, to all your applications, on premise or in the cloud.

Systancia Workroom Session is a "Zero Trust Network Access" (ZTNA) product. It allows to precisely define access to applications (web or client-server) or resources (servers or file shares) according to the user and his connection conditions, and whether they are in one or several datacenters, managed by the company or by a cloud service provider. It allows a wide variety of access scenarios to be taken into account, from controlled workstations, BYOD or third party providers.

Unified resource access portal

Systancia Workroom Session offers an access portal centralizing all the resources and applications provided to the user. The **SSO** (Single Sign-On) mechanisms integrated into the product offer additional comfort to users by increasing their productivity and improve security in case of provider access situations. Resources and applications are accessible via the web portal, **with or without an agent** installed on the workstation to also meet the BYOD or uncontrolled workstations issues.

Architecture focused on the user rather than the network

Systancia Workroom Session's **double-barrier architecture** allows you to provide specific access to applications instead of opening wide access to networks. This approach allows greater precision in terms of access openings and improved information system security. This architecture very easily offers **multi-site** access. It is therefore possible to access from a single portal to applications and resources spread over several datacenters, managed by the company or by a cloud service provider.

Least privilege policy (Zero Trust)

With Systancia Workroom Session, you can define access profiles allowing **rights to be dynamically adapted** according to the trust granted to users. This trust is built on the user's authentication, reinforced by **OTP (One Time Password)** mechanisms and by the user's access conditions, based on the workstation's **compliance check**. It is therefore possible to check the identity and health of the access terminal as well as access criteria such as the place or time of connection.

Full protection

The protocol break provided by Systancia Workroom Session is a shield against the risk of malware, ransomware or other protocol infections. The complete traceability of connections facilitates the forensic analysis, and therefore reduces the time it takes to restore services in the event of an attack.

ZTNA : Zero Trust Network Access

Why you should choose Systancia Workroom?

- A single solution for all remote access use cases allowing to **optimize the investment**
- **Reduced deployment costs** because it does not impact the existing systems and centralizes access to the different data centers
- The CSPN certification from the ANSSI (the French National Cybersecurity Agency) contributes to guarantee the **regulatory compliance**
- Reduction of the **delay to restore services** after an attack by facilitating the forensic analysis
- Strong authentication ensuring user identity to **reduce the risk of data leakage**
- Zero Trust policies improving **information system protection**
- **Protection against malware risks**, ransomware, etc. with protocol break
- Easy and fast access reducing **change management delays**
- **Reduction of the costs of IT equipment** by providing secure access from any device without having to equip all your employees with professional workstations
- **Improved productivity** due to user comfort and Business Continuity facilitated by embedded high availability mechanisms
- A secure assistance mechanism **reducing support costs**

A deployment offer adapted to your needs

Hybrid Cloud service, with the Mediation managed by Systancia
and the Gateways deployed in your datacenters

Rapidly deployable

Open your first remote access in a few hours without needing to modify your network architecture

Economically adaptable

Your subscription contract prepares you for any situation, and you only pay for what you use

"We wanted to be able to manage external access to the information system while avoiding the risks associated with VPN. With this zero-trust solution, we are more confident about the access context, especially for connections from China to our stores : we can check the workstation accessing the information system and have a granularity in access management by deciding to open certain applications to certain people instead of opening the entire network."

Clement Cesneut
Infrastructure & Security Manager - Groupe Beaumanoir

"The solution allowed us to meet our business continuity challenges by deploying teleworking for 92% of our agents within 2 days. They find the same user experience as at their workplace: they access their RDS desktop with all their tools and can therefore carry out all the tasks from their personal workstation, without constraints and in complete security."

Emmanuel Periaux
Information System Manager - OPH Metz Métropole

Systancia Workroom Session is based on the Systancia Gate software product:

The solution received under the name of IPdiva Secure the CSPN certification (First Level Security Certification) issued by the ANSSI in the field of "identification, authentication and access control". This certification guarantees the reliability, robustness and impermeability to external eyes to ensure the security of external access to the IS for administrations, OVIs (Operators of Vital Importance), OES (Operators of Essential Services) and, more generally, companies.

A proven and innovative solution for many years. Systancia is listed among the major publishers of ZTNA solutions in the Market Guide for Zero Trust Network Access, published by Gartner in June 2020, for its Systancia Gate solution.