Case Study

NANJGEL SOLUTIONS

Leader in global development support and aid empowers its workforce with on-demand, secure access to critical business applications

10+ hours
saved per week
through remote access

45% increase
in productivity

Thousands saved
within 1st year of deployment

Industry: Banking & Finance

Environment: 1200 end users with more than 2000 devices connecting simultaneously

Challenges

- Remote & Secured access
- Clientless
- Multi factor authentication
- Virtualization of critical business applications
- Platform independent

Security Solution
Accops Hyworks,
Accops HySecure with HyID

Use Cases

- Sandboxed access
- Secure access gateway
- Multi-factor authentication
- Device entry control
- Persona-based context control
- Time based access restrictions
- Clipboard restrictions.

Overview

Being the development arm of the UAE government and the leader in global development support and aid the company aims to help developing countries to achieve sustainable socio-economic growth; through financial assistance in the forms of concessionary loans, managing government grants and equities. They also peruse investments in order to encourage the private sector in the recipient countries to play an essential part in accelerating the economic development process, and at the same time playing a pivotal role in strengthening and diversifying the future resources of the Fund.

The Fund's strategy focuses on continuing its active role in stimulating economic growth in developing countries, the geographical expansion of its development funding operations, as well as in supporting the national economy.

To meet this strategic goal, the organization had the need to provide access to their business applications to its user from anywhere, while not compromising on the security and confidentiality of the data that is present within these applications and accessible by these remote users.

Business Challenges

- Secure and seamless access to business applications from any device and from any location
- Mitigating data security concerns associated with the open internet utilization
- Reduced maintenance costs
- Improving visibility on user activities and control over endpoints

NANJGEL SOLUTIONS

Why Nanjgel Solutions

Nanjgel Solutions has years 12+ experience and capabilities to understand the requirements of the organization and provide the right solution(s) that will benefit the organization at an affordable cost. We also have a dedicated team of certified experts that can assist with the design, architecting, deploying and supporting the provided solutions.

Nanjgel Solutions was able to understand the customers key requirements in depth and also understood their current infrastructure and mode of operation. Nanjgel proposed to deploy the Accops Digital Workspace solution which consists of Secure Remote Access, Desktop and Application virtualization along with Multi-Factor Authentication.

The solution was quickly acquired and deployed in their infrastructure within a short duration of 10 Man Days. The solution was not only used for their Secure Remote Access requirements but was also deployed to virtualize many in-house developed and legacy applications which weren't supported by any other solution in the market.

Use Cases

Complete Digital Workspace Solution (Sandboxed access to applications)
Using the Accops solution we were able to achieve a complete sandboxed access to the business applications. The users were able to access the application directly through the browser or using the client application without getting direct access to the network. The IP addresses were also obfuscated during the access to ensure additional security.

Secure application access gateway
Users were able to access the applications through the sandboxed gateway while working remotely or from within the organization seamlessly and in a secured manner using our Zero Trust Access model.

Multi-factor authentication
Users were able to connect to the applications and environment with their AD username and password and additionally were asked to provide a second factor of authentication using Email/Mobile tokens, Push notification or biometrics.

Device entry control and persona-based context control
Device restrictions and profile-based control were applied based on the type of user and the type of access. These restrictions include but are not limited to mapping set of devices to users and restricting any other device connection, providing access to applications based on location and device posture, etc.

Time based access restrictions
Restrictions were applied for application access based on day and time of the week. All users were provided either restricted access or no access after office hours based on their role.

Clipboard restrictions such copy/paste, snipping tool, etc.
While accessing critical business applications through our solution, copy/paste, printing, download of files and snipping tools were blocked for users based on their profiles.

Key Benefits

- Users were able to remotely access authorized applications without being given access into the network.
- Custom and legacy applications were accessible from anywhere
- Strong User & device visibility & control
- Secure Access from Anywhere
- Better monitoring and enhanced risk profiling
- Secure enterprise mobility
- Improved user experience
- Reduced IT operations costs