

THE PANDEMIC BOOSTS SINGLE CONNECT

CUSTOMER OVERVIEW

A commercial bank, 100% owned by a big national bank. The bank specializes in consumer credit and credit cards and has a decade of history in providing consumer credit and retail financing.



CHALLENGE

The bank engaged Single Connect before the pandemic expressing a willingness to pilot and buy a small piece of the Single Connect product to be able to control remote system administrators. In 2020, a considerable part of the bank employees transitioned to a work-from-home model.

After a successful experience with Single Connect, the bank's IT department decided to expand the deployment within the organization by connecting more users through Single Connect, thus providing safe connections for the bank's remote employees.

SOLUTION

The Single Connect platform the customer had deployed in their test environment went into production when the pandemic happened.

Single Connect was intended to provide remote access for external users, such as IT equipment vendor's support engineers. The customer required control of this external access with a range of policies – mandatory session recordings (RDP as the main protocol), non-disclosure of internal accounts' passwords, and limitation of infrastructure visibility.

Single Connect offered the customer a renewal license with a competitive and discounted price to reduce costs during the pandemic and satisfy the customer's service requirements as quickly as possible.

With the Privileged Session Manager (PSM) as part of the Single Connect solution, the requirements were quickly addressed using Single Connect's reliable solution architecture. The PSM functionality fully allows the customer to provide secure points of access to their infrastructure, with a wide definition of policies, and continuous session recordings with OCR (optical character recognition engine), providing the IT security team with the ideal tool to manage privileged and remote user access in real time.



With recording storage needs continuing to grow since deployment, Single Connect provides fast and scalable database storage, with last-generation tools to investigate all past activity within the infrastructure and user sessions.

Single Connect is based on a virtual infrastructure, which is easy to manage by the customer's IT support team, and easy to backup and restore (if needed).

The solution is widely used by the customer's IT and security departments to organize not only remote access, as intended at the beginning of the project, but also internal access, thanks to the solution's adaptability and compatibility with both types of access.

By the end of 2020, with the remarkable success of the solution, the customer decided to extend the deployment and upgrade to a permanent license.

Single Connect features an active-active cluster architecture for resilience and stability as the standard deployment. The customer configured two virtual server instances for Single Connect, to minimize the risk of infrastructure failure and to provide constant, uninterrupted access to the infrastructure.

RESULT

By SLA requirements, Single Connect's seamless implementation, steadfast support, and problem-solving capabilities of the Single Connect Support Team ensured customer satisfaction.

The solution has two active-active server instances working 24/7 and provides remote and internal access control to the customer's infrastructure, for both external users and employees. Single Connect has been recording many thousands of sessions since its deployment, fulfilling audit and compliance requirements.

Single Connect made remote access secure and allowed the customer's business-critical bank systems to remain online, secure, and uninterrupted.

KEY BENEFITS

- Zero trust privileged management
- Unified and centralized privileged access management
- Additional security layer with built-in multi-factor authentication, providing secure remote access
- Advanced password vault features for secure storing and sharing of sensitive information
- Application-to-application password management for safe application access to sensitive data

