Banque et Finance

# ACCÈS À DISTANCE PRIVILÉGIÉ

Étude de cas

## À PROPOS DU CLIENT

Le client est une banque régionale de premier plan qui a besoin de gérer et de protéger l'accès à distance à des systèmes privilégiés pour le travail d'administration.

## OBJECTIFS

Le client recherchait la possibilité de mettre en œuvre des flux de travail basés sur des équipes pour accéder à des ressources et à une technologie privilégiées afin de surveiller en temps réel les sessions privilégiées initiées par les fournisseurs à partir d'appareils non gérés.

Il était destiné à fournir une exposition minimale aux périphériques non fiables sur le réseau avec la possibilité d'identifier ou de bloquer rapidement les commandes ou les exécutables indésirables.

Le client souhaitait avoir la possibilité d'effectuer des analyses médico-légales sur les transcriptions et les enregistrements de session avec un mécanisme permettant d'empêcher le piratage de session à partir d'appareils non gérés.

Il recherchait également un accès limité dans le temps pour les fournisseurs externes, la portabilité des journaux et des enregistrements et une capacité à s'intégrer aux plates-formes SSO basées sur des normes (SAML).

En outre, possibilité d'automatisation avec accès API au nouveau système, contrainte minimale sur les pare-feu de périmètre pour la connectivité entrante et réduction des frais administratifs liés à la gestion de la nouvelle infrastructure.

## VUE D'ENSEMBLE DE LA SOLUTION

Sur la base des objectifs du client, ISSQUARED a choisi la solution avec les caractéristiques suivantes.

- Plateforme basée sur le cloud avec accès via HTTPS.
- Solution conforme FIPS pour stocker en toute sécurité la session et les métadonnées associées.
- Capacité à s'intégrer à la plate-forme SSO existante à l'aide de SAML.
- Contrôle d'accès basé sur les rôles et workflows de demande/approbation.
- Capacités d'observation et de contrôle de session par l'équipe de sécurité informatique.
- Capacité à s'intégrer aux solutions de stockage de mots de passe pour la fonctionnalité d'injection de mots de passe.
- API pour l'automatisation et le portage des journaux d'audit vers des systèmes externes avec des capacités d'audit et d'analyse.

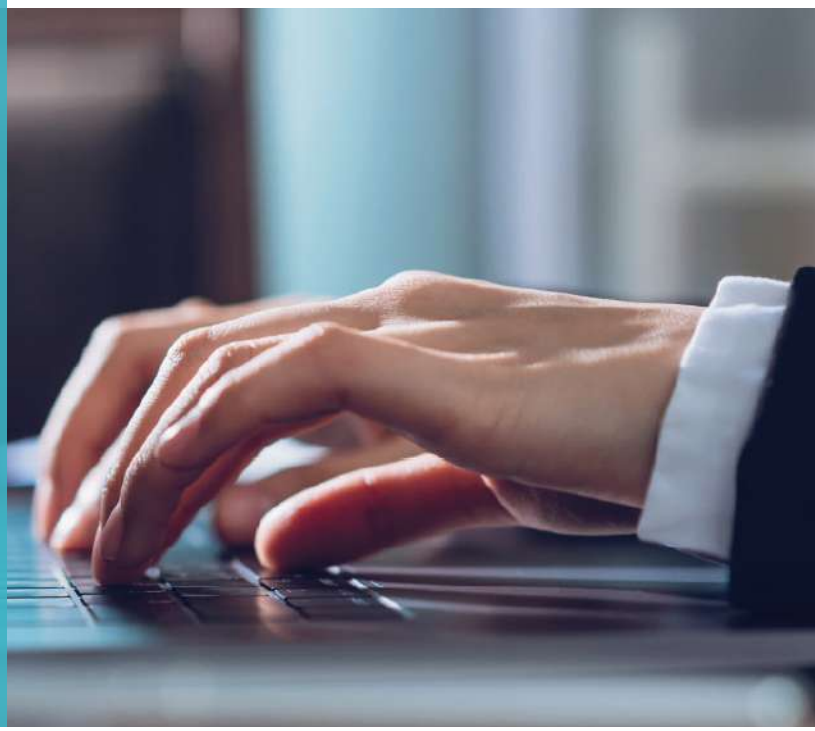
## APPROCHE & TECHNOLOGIE

*Sur la base des directives ci-dessus, l'approche suivante a été adoptée pour les comptes d'utilisateurs privilégiés et réguliers, respectivement.*

- Une solution d'accès à distance Privileged basée sur SaaS a été achetée et déployée.
- L'intégration avec la plate-forme SSO a été effectuée pour fournir un accès basé sur MFA.
- Les équipes IS/IT ont été configurées en fonction des tours de service d'infrastructure.
- Des systèmes ont été configurés pour les équipes afin de s'assurer qu'il n'y avait pas d'accès entre les niveaux/tours.
- Le processus de demande/approbation a été configuré pour l'accès au système.
- Des stratégies d'accès basées sur le temps ont été configurées.
- Les membres de l'équipe de sécurité informatique sont devenus des gardiens capables de surveiller et d'observer toutes les sessions.
- L'intégration avec l'API a été effectuée pour la conservation des journaux et des sessions enregistrées.

## RÉSULTATS

- 0 % d'exposition des informations d'identification privilégiées sur les postes de travail non approuvés.
- Visibilité à 100 % sur l'accès des fournisseurs externes aux systèmes privilégiés.
- 0% de dépendance aux solutions VPN pour un accès privilégié.
- 100% de rétention des journaux de session conformément à la politique de l'entreprise.
- Accès protégé par MFA aux systèmes privilégiés.
- Contrôles dissuasifs et préventifs efficaces sur les sessions privilégiées avec l'observation, l'enregistrement et les transcriptions de session.
- Permet l'identification d'activités malveillantes volontaires/involontaires via une recherche par mot-clé sur les sessions enregistrées.



ISSQUARED

HQ: 2659 Townsgate Rd, Suite 227
Westlake Village CA 91361 USA

+1 805 371 0585
+1 800 779 0587

support@issquaredinc.com
www.issquaredinc.com