PRIVILEGED REMOTE ACCESS

Case Study

ABOUT THE CLIENT

The client is a leading regional bank in need of managing and protecting remote access to privileged systems for administration work.

OBJECTIVES

The client sought the ability to implement teams-based workflows for access to privileged resources and technology to monitor privileged sessions initiated by vendors from unmanaged devices in real-time.

It was intended to provide least exposure of untrusted devices on the network with the ability to quickly identify or block any undesired commands or executables.

The client wanted the ability to perform forensics analyses on session transcripts and recordings with a mechanism to prevent session hijacking from unmanaged devices.

It was also looking for time-bound access for external vendors, portability of logs and recordings, and an ability to integrate with standards-based (SAML) SSO platforms.

SOLUTION OVERVIEW

Based on the client's objectives, ISSQUARED decided on the solution with the following features.

a) Cloud-based platform with access over HTTPS.

b) FIPS-compliant solution for securely storing session and related metadata.

c) Ability to integrate with the existing SSO platform using SAML.

d) Role-based access control and request/approval workflows.

e) Session shadowing and control abilities by the IT security team.

f) Ability to integrate with password vaulting solutions for password injection functionality.

g) API for automation and porting audit logs to external systems with auditing and analysis capabilities.

APPROACH & TECHNOLOGY

Based on the above directives, the following approach was taken for privileged and regular user accounts, respectively.

- A SaaS-based Privileged remote access solution was procured and deployed.
- Integration with SSO platform was done to provide MFA-based access.
- IS/IT Teams were configured based on the Infrastructure Service towers.
- Systems were provisioned for teams to ensure there was no cross-tier/tower access.
- The request/approval process was configured for system access.
- Time-based access policies were configured.
- IT security team members were made gatekeepers with the ability to monitor and shadow all sessions.
- Integration with the API was done for log and recorded session retention.

RESULTS

- 0% exposure of privileged credentials on untrusted workstations.
- 100% visibility on external vendor access to privileged systems.
- 0% dependency on VPN solutions for privileged access.
- 100% retention of session logs as per company policy.
- MFA protected access to privileged systems.
- Efficient deterrent and preventive controls over privileged sessions with session shadowing, recording, and transcripts.
- Enables identification of voluntary/involuntary malicious activities through keyword search on recorded sessions.