sectona

Case study

Nation’s best broker secures platform that facilitate over 800,000 trades per day with Sectona

Kotak Securities leverages Sectona’s light weight privileged access management solution for securing access to over 300 users to their sensitive hybrid IT environment

Challenge:

Kotak Securities manages high volume trades and caters to customers across 390+ cities in India. With a strong focus on technology, they always believe in providing the best services to their customers without interruption. To ensure this, securing its IT backbone that supports the fast-paced nature of business is priority. Summarizing the need:

- Securing and monitoring the access of internal users and third-party vendors to IT
- Managing access to cloud (AWS and Azure) workloads
- Automating password management and user lifecycle management across multiple sites
- Ensuring business continuity and redundancy with minimal room for downtime

Industry
Financial Services

Solution:

Sectona with its modern architectural approach (Active-Active) provides Kotak Securities with the much-needed security framework and availability capable of securing high user access traffic to critical hybrid IT systems. The pre-packaged built-in vault of Sectona ensures that system is highly available and the redundancy switch during failover is simpler and faster, helping achieve business continuity at minimal MTTR. Sectona also helps monitor user activities including that of third-party vendor access and enforce restrictions for users to access or execute specific applications and commands while working on target systems.

Background

Kotak Securities is one of the oldest and largest equity broking institutions in India. As a subsidiary of Kotak Mahindra Bank, it was founded in 1994 with its headquarters in Mumbai. The company has a customer base of approximately 17 Lakh customers with over 8 Lakh trades per day catering to 393 cities in India. Kotak Securities is a corporate member of the Bombay Stock Exchange (BSE) and National Stock Exchange (NSE). With a national footprint of 1539 branches, franchisees and satellite offices, Kotak Securities has been adjudged the best broker by FinanceAsia Country Awards, 2019.

Kotak Securities being a firm believer of Digital First, is constantly working on innovating their technology platforms. To keep up with its fast-paced nature of business and service customers, securing their IT backbone is a priority. That is the reason they were looking for a solution that could solve its problem of managing diverse user access while optimizing resources and maintaining business continuity. To summarize, Kotak Securities was looking for a comprehensive privileged access solution that could take care of their critical infrastructure access situated across multiple locations while achieving high availability.

Managing access to a diverse user base

Being an equity broking institution, Kotak Securities infrastructure is quite heavy in terms of user access. On average, there are approximately 200 to 300 sessions taken by IT users every day. Concurrencies, at any given time, graces a modest 70+ sessions. With these numbers only expected to increase, it is imperative for the Kotak infra team to moderate and secure critical user access. With a segregated user set that witnesses an even split between internal IT users and third-party vendor users, Kotak team can streamline such user access with Sectona's advanced session management techniques.

Internal IT Users

Internal IT users connecting to RDP, SSH or client-based sessions (e.g. MS SQL), secure access is delivered from Sectona via its native launcher utility invoking sessions on the user machine.

Third-Party Vendor Users

Granting third-party vendors who access via VPN, RDP or SSH sessions over browser (a unique technique that delivers sessions without the need for native utility or client on end user machine). This technique isolates the user machine's session and ensures sensitive passwords are not cached or exposed within the end user machine. There is flexibility to allow the browser-based access without routing access through VPN.

For client or application access, eg. MS SQL, such sessions are delivered via an in-house jump server. This again ensures native clients or utilities are not needed on the end user's machines truly isolating critical session access for third-party vendor users.

Cloud Users

Kotak Securities has a hybrid infrastructure with resources spread across cloud platforms as well, primarily AWS. Leveraging Sectona's deep integration with cloud platforms, Kotak achieves easy login and management of internal and cloud partner users alike for access to AWS admin console. Achieving this integration without requiring additional resources or a dedicated setup of PAM on cloud.

Adding an extra layer of security here, Kotak Securities also maximizes Sectona's built-in MFA mechanism. With an offline OTP based MFA app, users connecting to the system are mandatorily required to enter the second factor OTP for added authentication.

Ensuring business continuity with minimal downtime

Kotak Securities has its infrastructure spread across two locations. With a high level of user traffic at both locations, ensuring the PAM system is available at any time has high impact on their daily volume of business.

To address this, Sectona uniquely proposed an Active-Active architecture with independent yet centrally connected PAM instances at both locations. With a singular PAM-PAM communication between both locations, local users at both locations, can take access to respective location's IT systems through the locally available PAM instance via location based proxy servers. While access gets granted locally, logs are pushed to central instance in real time. Furthermore, with Sectona's built-in vault and application load balancing capabilities, high concurrencies can be managed without relying on external clustering or load balancing techniques. It safeguards critical sessions and ensures system is highly available with minimal downtime. This approach also ensures limited external exposure between communication of both locations minimizing the need for increased ports and firewall rules.

Automated password and user lifecycle management

Kotak Securities have their infrastructure spread across two locations. Manually managing the passwords of all the accounts in both the locations for 1000+ privileged accounts was a daunting task. Furthermore, with a Microsoft heavy environment, IT users were segregated methodically at the Active Directory level. For an increasing base of such users, manually provisioning and onboarding users onto PAM would grossly impact employee productivity.

For this, Sectona adopted a two-prong approach.

Unique architecture

Sectona extended the above proposed Single Master-Multiple Service Nodes architecture wherein the password changes are automated and managed centrally at the single master node and is replicated across service nodes in real-time.

Continuous discovery

Sectona PAM provides built-in asset and account discovery that ensures continuous discovery and onboarding of newly added IT assets and privileged accounts into the infrastructure. This capability, coupled with attribute-based grouping ensures users added onto the Active Directory are defined access to target systems via PAM based on attributes.

With a dedicated approach to keeping maturing their privileged management program, Kotak Securities is closely working with Sectona.

As part of this alignment, Anil Nair, the Head of IT Infrastructure & Security, comments "Deployment of the product is very fast, 2FA is inbuilt in the system, and the best part of the solution is you can take the remote of the server via a browser which helps you to avoid password-stealing due to limitation with RDP protocol. Keep innovating".

Sectona is a Privileged Access Management company that helps enterprises mitigate risk of targeted attacks to privileged accounts spread across data centers and cloud. Sectona delivers integrated privilege management components for securing dynamic remote workforce access across on-premises or cloud workloads, endpoints and machine to machine communication.

For more information, visit www.sectona.com and follow @sectona1 on Twitter or @Sectona on linkedin