sectona

Case study

Cloud-born insurance company secures and monitors critical user access to SAP on AWS with Sectona PAM

Sectona PAM helps EGI secure access and monitoring of internal and external/third-party user access over cloud and SAP.

Need

Edelweiss General Insurance Company Limited (EGI) was proactively in search of a solution that could:

- Allow secure access to users with built-in dual-factor authentication enabled for an additional layer of security
- Monitor internal users and third-party vendor access to critical AWS resources
- Enable secure remote access to critical business applications from outside the office network

Industry
Insurance

Solution

Sectona PAM is an AWS compatible solution, with capabilities to be hosted over cloud. Since EGI's complete infrastructure is hosted on AWS, it was easy to deploy Sectona. EGI leveraged Sectona PAM solution's capabilities to address its requirements including:

- In-built MFA along with a secure and isolated browser-based access of business applications for business users
- Comprehensive monitoring and access policy management to control and manage user access to critical AWS resources
- Cross-platform capabilities to enable access to users from any platform for taking access to critical systems anytime from anywhere

Benefit

With Sectona PAM, EGI is in better control of user access to its critical resources and further is able to accomplish the below:

- With Sectona's unexposed embedded database, EGI achieves higher security along with built-in replication mechanism for HA and failover scenarios
- Better visibility with advanced risk scoring capabilities and higher monitoring of users' accesses regardless of location or time
- Agentless platform independent access to users without impacting productivity and security

Background

Edelweiss General Insurance is one of India's first cloud born insurance companies. Established as a subsidiary of the Edelweiss group, a large investment and financial company based out of Mumbai. The group has been in existance for over 2 decades now and caters to a client base of over 1.2 million. The general insurance arm was founded in 2017. Considering the nature of its business, Ninad Chavan, the Chief Information Security Officer was proactively planning to implement a centralized solution that could:

- Monitor all the remote users (including business users) taking access to the target servers on AWS from external network
- Enable a second-factor authentication for users accessing business applications like SAP
- Allow secured and seamless file transfer from development to production environments

Enabling Better Control of User Access to Target Systems on AWS

EGI business users are required to take access of critical business applications remotely, essentially connecting from outside the perimeter of the secure office network. Moreover, authorized third-party users access EGI's cloud workloads for routine business activities including file transfers between development and production environments. It was vital for Ninad to have complete monitoring of all user access to critical resources on cloud – both remote business user access and third-party user access. Additionally, he had to ensure file transfers could be secured and monitored to mitigate any data loss. Ninad realized this could be possible by enforcing a centralized monitoring and access control solution.

Monitoring and Securing All User (Internal and External) Access with Sectona PAM

Sectona PAM with its AWS platform compatibility and deep integrations can seamlessly integrate with EGI's applications hosted on AWS environment. The access policy definition for users accessing critical resources, including SAP client, is now aligned and configured to be connected through Sectona PAM. This definition enables users to securely access its business applications from the internet-facing Sectona PAM portal. "Sectona is a robust access control solution that easily adapts with my AWS environment. It provides the capability to define access rights on a need-to-know basis for all my users and helps me monitor their activities", says Ninad. By enabling Sectona's built-in MFA, there is an additional layer of security, verification and accountability created. All the user sessions initiated through Sectona PAM are monitored with comprehensive logs capturing relevant user access details for audit and governance purposes.

Unhindered Cross-Platform Access to Target Systems Anytime from Anywhere

Often, business users must take access, even on public holidays, to serve their customers. In such scenarios, they may not be at the liberty of accessing from their designated laptops and may be forced to rely on any available laptop or desktop or device.

"Sectona PAM's cross-platform capabilities that allow access to users from any device over the internet and still, be able to monitor those sessions is a stand-out for us, especially in such scenarios ", observes Ninad.

Securely Transfer Files between Environments Mitigating Risk of Data Theft

EGI has the need to allow third-party vendors to be given access to target business applications and servers for support or maintenance activities. Earlier, this access was provisioned via VPN to control the access, however, it also left room for users to copy data outside of EGI network. With Sectona PAM in place, access can now be provided to third-party vendors through its browser-based access mechanism, allowing such users to connect to target servers and applications while restricting any file copying or file transfers. The browser-based access mechanism in Sectona essentially isolates the target server session and in its default nature, disallows file copy and file transfers. Such a control framework protects the business-critical data from getting out of the corporate network by any means.