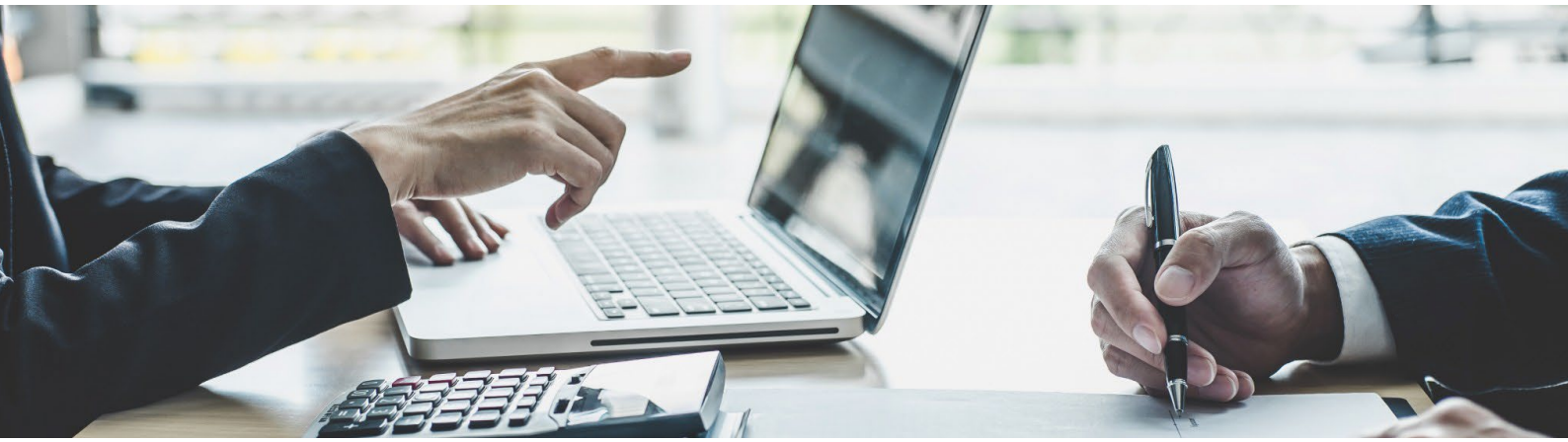
sectona

Case study

Boutique Financial Services Firm in KSA chooses Sectona PAM to Strengthen SAMA Compliance

PAM suite from Sectona helps Morabaha Marina Financing Company with simplified and secured critical privileged access to their IT infrastructure



Need

Morabaha was proactively looking to strengthen their cyber security framework – securing and monitoring the user access to core infrastructure with a PAM solution. Key use cases include:

- Manage and control the third-party contractor access to critical infrastructure resources based on need-to-have, need-to-know access requirement
- Monitor and log third party vendor and internal staff access to critical servers including RDP for accountability tracking
- Enable multi-factor authentication for all privileged and remote user access
- Strengthen compliance & achieve higher maturity of cybersecurity controls in adherence with cyber-security guidelines set by SAMA (Saudi Arabia Monetary Authority)

Industry
Financial Services

Solution

Sectona has provided an automated and integrated Privileged & Remote Access Management suite for securing user access to critical IT assets for better governance, control and visibility

Benefit

With Sectona, Morabaha Marina Finance confidently achieves compliance to SAMA guidelines by adhering to specific policies around need-based access, automated password vaulting and confidentiality, monitoring with review and multi-factor authentication for internal and contractor users alike.

Background

Morabaha Marina Financing Company (MMFC) is a 2012 established financial institution headquartered in Riyadh, Saudi Arabia. It aims to provide financial services to individuals and SME based entities on Islamic Shari'ah principles. They provide various financial products to individuals and corporates clients across major cities in the Kingdom.

Considering the nature of their business, the IT Security team of MMFC was exploring a solution that will help them manage and monitor all the users taking privileged and remote access into their network and provide transparent need-based access of critical systems to all the users.

Allocating Controlled Privileged and Remote Access to Internal Staff and Third-Party Contractors

Access to critical server resources of MMFC is allowed not just for internal IT team and staff but also for third-party contractors. Access to high privilege accounts across such systems involved sharing of passwords among multiple users. Furthermore, it was important to enforce a second level of authentication for such third-party user access for better accountability and enhanced security.

"Avoiding password sharing and creating accountability while segregating or allocating user access based on access needs is a key objective for us", as per the, IT Security Lead.

Moreover, for such third party vendor access, several firewall configurations, port enablement and manual processes for authentication had to be implemented to ensure better security.

With Sectona's modular built Privileged Access Management suite, MMFC IT & security team is now able to leverage its built-in hybrid session management, multi-factor authentication and monitoring capabilities to ensure higher control over all user access to critical systems while associating credibility and accountability to such access.

Hybrid Session Management, MFA and Enhanced Visibility over all User Access with Sectona PAM

"We felt Sectona PAM solution is an integrated solution fulfilling our requirements of easy user access mechanism capable of providing secure user access to all with the right monitoring and governance frameworks built-in", said the security team.

With Sectona PAM installed, all user access to target systems is routed via the Sectona PAM gateway – a secure, encrypted and tunneled channel. Enabling a single port communication from user's machine to the PAM server, all access traffic is now securely routed through Sectona PAM after ensuring appropriate user authentication and access control check. For third-party contractor access, specifically, an offline OTP based MFA is enforced for an additional layer of security through Sectona's built-in MFA mechanism. Moreover, all user activities are monitored with Sectona's built-in session recording capabilities ensuring higher visibility and accountability.

With strong integrations built to protect access to a range of systems including Windows & Unix, Sectona PAM has ensured significant benefits in IT operations.

Automated Management of Internal and External User Access

Sectona provides an automated and attribute-based access provisioning and access definition framework allowing security team to define each user's access to target IT systems based on user's roles, responsibilities and need for access. Each user is provided transparent access to target systems without needing to know or enter privileged account credentials. These critical credentials are encrypted and stored in Sectona's hardened and secure password vault. It thereby enhances security and increases productivity by eliminating manual password management and password sharing.

Better Visibility and Governance

Sectona PAM provides comprehensive session monitoring capabilities including real-time monitoring and risk-based session review for improved gevernance and visibility

Strengthened Compliance with SAMA Information Security Guidelines

MMFC being a financial institution, is required follow compliance mandates in terms of privileged access security set by SAMA's Cybersecurity Frameworks. Sectona's Privileged Access Management Solution helped MMFC achieve this compliance by adhering to policies around need-based access, automated password vaulting and confidentiality, monitoring with review and multi-factor authentication for all users – internal IT staff and third-party contractors.

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