The National Social Security Fund for Uganda Leverages Sectona to Improve Compliance and Govern Privileged Access

Need

"Over the years, with IT Teams associated with mistrust, Privileged Access Management has come on board to address these issues, as an adversary in the IT security world" remarkably quoted by Simon Kule, Infrastructure Manager at Uganda National Social Security Fund. Privileged Access Management has seen a quick adoption in the East African Region, especially the likes of private sector organizations in Banking and Telecom Industries, prioritizing this to the extent of setting up dedicated office spaces. At the same time, the Government Sector organizations have been embracing Privileged Access Management to ensure adherence to audit requirements and benchmark. Being a quasi-government agency, The Uganda National Social Security Fund had seen a decline in audit ratings due to a lack of control over users' actions in the organization's environment and a dedicated process to manage privilege delegation. Identifying the Gaps, NSSF identified vital objectives they needed Sectona to help them.

- Control and monitor access of privileged users in the organization's environment
- Restrict and Manage delegate privileges throughout their lifecycle with a time-bound factor
- Record and analyze all the sessions for enhanced auditing purposes and enabling granular visibility into the user's actions

Industry

Government

Solution

NSSF was looking to implement a solution that helps them address critical privileged access management issues, which involves going through a rigorous procurement process, as all the arms of the government are watching them. Sectona provides a purpose-built access platform that brings together different elements to secure privileges across the growing attack surfaces in an organization. Sectona Leverages a platform developed from scratch, light build and integrated, focusing on automation, and bringing together diverse teams into a single platform, controlling and governing their access through a centralized console, helping achieve the security objectives with the desired velocity. Simon said that "Sectona has made us mature in terms of security, auditing, and ratings laying the foundation for extended business opportunities."

Benefit

NSSF has successfully implemented Sectona for over two years, granting them control and monitoring capabilities from a centralized console. Simon said that "Sectona is an Easy-to-Use and Affordable Solution with Value for Money. Currently in our third year with Sectona, and all that we have needed have been taken care of." Also pointing out a crucial benefit, Simon mentioned, "Stuck with audit rating issues for few years, Sectona helped us resolve them, and thereby maturing our audit rating."

Background

National Security Fund is a quasi-government agency founded in 1985 to provide social security services to employees in Uganda. NSSF is a provident fund mandated by the government of Uganda for the employers and employees in the private sector not covered under the Government Retirement Scheme. This fund is a contributing scheme responsible for collecting, safekeeping, responsible investment, and distributing retirement funds for private-sector employees. Being the largest pension fund in the East African Region, the Uganda National Social Security Fund manages assets worth over UGX 14 million invested in Fixed Income, Equities and Real Estate Assets.

Delegating Privileges from a Centralized module with a single-click

NSSF as an organization considers Privilege Delegation a challenge, where privileges, once assigned and left unchecked, can be utilized to cause harmful repercussions. Sectona's Account Lifecycle Management Capability accommodates provisioning, disabling and de-provisioning account access from a single console, confining the access credentials only to the authorized user, reducing the risk of unauthorized access and excessive privileges. This capability facilitates provisioning accounts with the least privileges access based on roles to perform a specific task. In addition, Account Lifecycle Management logs comprise all the account details through its journey, from account creation, assigning roles, access rights, assets, grouping to their expiration, facilitating centralized management of privileged account operations, ensuring better accountability.

More robust and Flexible Password Management

Home to contributions of several private employees and employers, NSSF, the largest pension fund, wanted a solution to prevent any unauthorized access into the organization's network and cause any discrepancies. Sectona's Password Management facilitates creating a random and hard to guess password by enforcing rules on the password policy parameters, encrypting these credentials with algorithms AES-256 with FIPS 140-2 support and salting and storing them in the Embedded Password Vault, ensuring robust security. Furthermore, Password Management facilitates a controlled and auditable password checkout for a resource while also providing the option to integrate with more than 150+ out of the box connectors or Ready to use Frameworks to build custom connectors like a Password Change.

Simplified Auditing with Reinforced Monitoring and Intelligent Risk Scoring

ENPI Group is associated with many external applications for ERP Services, Business Intelligence or Active Directory Exchange, leaving the network exposed to external attack vectors at the risk of a compromise, which requires constant monitoring. Sectona Security Platform strengthens the governance with real-time session recording & store the session logs in tamper-proof & encrypted storage for enhanced auditing for all the sessions at different capacities in the form of video & text/command format. "We have complete visibility into the sessions and have been able to identify few mistakes based on the session recordings and have them rectified," remarkably said Mr Simon.
Sectona Security Platform also helps assess all the sessions and profile a threat with intelligent risk scoring based on 30+ varied yet focused parameters associated with common privileged account attacks. Along with this, Sectona provides an in-depth analysis of user behaviour linked to individual session access and notify if any attacks are triggered and offer a centralized view of the logs of operating system activities.

Building a Roadmap for Continued Business Partnership

Successfully Implementing Sectona for two years, Simon said, "Along the way we have realized the need to scale up and have increased the number of user licenses two-fold for administrators and privileged users in our organization, to control and monitor their actions." Speaking about their plans, he said, "We are moving towards Integrating Two-Factor Authentication and along the way hopefully add Single Sign-On, to continue making life easier for the administrators whilst also having control over their actions."

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