



Guaranty Trust Bank Sets up a Comprehensive Privileged Access Management Framework with Sectona

Background

Guaranty Trust Holding Company Plc (GTCO Plc) is a top African financial services group headquartered in Lagos, Nigeria. Previously Guaranty Trust Bank Plc (GT Bank), it was restructured into a holding company to expand its activities beyond conventional banking.

GTCO Plc's subsidiary, Guaranty Trust Bank Ltd, boasts of a vast network of branches and online platforms in Nigeria, other African countries, and the United Kingdom. Famed for its robust corporate governance and pioneering spirit, GTCO is listed on both the Nigerian Stock Exchange and the London Stock Exchange.

Guaranty Trust Bank: A Global Financial Group

The bank is also prominent in several African nations, such as Côte d'Ivoire, Gambia, Ghana, Kenya, Liberia, Rwanda, Sierra Leone, Tanzania, and Uganda, as well as in the United Kingdom.

For a financial institution like GT Bank, protecting sensitive customer data and managing a wide network comes with serious responsibility. To strengthen IT security, meet regulatory standards, and maintain customer trust, the team put a comprehensive Privileged Access Management (PAM) framework in place.

Securing GT Bank HQ with Sectona PAM

GT Bank began its PAM journey from its headquarters in Nigeria. This first deployment laid the groundwork for a stronger and unified security framework across the entire group.

Before implementing PAM, GT Bank managed vendor accounts and their access privileges in a decentralised and less secure way. With the new system in place, the team brought all vendor access under one roof, gaining full control and



visibility. The shift from vendor-managed access to bank-controlled approach played a key role in reducing third-party risks.

Group Approach and Vision

Successful Pilot

After a successful initial implementation at their HQ, the company expanded its use of PAM.

Swift Global Rollout

After a successful initial implementation at their HQ, the company expanded its use of PAM.

Centralised Control

A key driver for this rollout was centralising core security principles and governance across all entities - a goal they successfully achieved with PAM.

Strengthening Global Operations through PAM

The solution was deployed on an entity-by-entity basis. Each subsidiary received a tailored and segregated PAM configuration to ensure complete adherence to its unique regulatory compliance and business needs.

Given a smooth deployment, Sectona delivered several key outcomes:

Improved Security Posture

Their overall security framework was strengthened immediately.

Efficient Password Management

Beyond standard password management for AD and local accounts, Sectona addressed password sprawl by securing critical application dependencies. This included automating password rotation within application configuration files, Windows Services, and Kubernetes login accounts, ensuring seamless updates across the entire service stack.

Centralised Control

Previously sprawling local accounts, users, and identities were brought under a unified and central management.

Secured Kubernetes Access Control

Sectona streamlined privileged access for the Kubernetes ecosystem by developing a custom plugin for VMware Tanzu. This framework facilitated secure SSO access, complete with session isolation and real-time monitoring. Consequently, GT Bank successfully enforced Segregation of Duties (SoD) and implemented precise Role-Based Access Control (RBAC) across their containerised environments.

Strategic PAM-Driven Security Transformation

GT Bank's adoption and strategic implementation of PAM was pivotal in securing its operations as a global financial entity. Starting with the foundational deployment at its Nigerian headquarters to control vendor access, the bank has expanded its PAM use cases to include the critical function of managing application-based passwords - all underpinned by the core principle of strong encryption.



Sectona with its light, integrated approach provides a single console for securing passwords & secrets in embedded vault, secure access with cross-platform access technology & manage privileges over endpoints. For more information, visit www.sectona.com and follow [@SectonaTech](https://twitter.com/SectonaTech) on X (Twitter) or [@Sectona](https://www.linkedin.com/company/sectona) on linkedin