

CASE STUDY



Company: BRAC Bank Limited, Bangladesh

Bangladesh's BRAC Bank selects CyberArk to defend its assets

Industry: SME, Retail, Corporate and Agent Banking

Employees: Approx. 7,000

CyberArk Products & Services:

- Privileged Access Manager
- Endpoint Privilege Manager
- Secrets Manager
- *NIX Server Protection
- Discovery & Audit (DNA)

BRAC Bank is a private commercial bank in Bangladesh that was founded in 2001 and now employs around 7,000 staff, serving around two million retail, corporate and SME business customers in the country and abroad. Its corporate vision is to “build a just, enlightened, healthy, democratic and poverty-free Bangladesh”. Being one of the largest banks in Bangladesh, BRAC Bank is entrusted with protecting customer and corporate data. It also has multiple digital and transformational initiatives underway.

THE PROBLEM

Despite its success, like all enterprises BRAC Bank Limited (BBL) must face up to the many and varied challenges of security. To do this it has taken bold steps, becoming the first (and so far only) local bank to achieve ISO 27001:2013 certification for security management and BBL was the first Bangladeshi bank to deploy a Security Operations Centre to anticipate and defend against threats. Participating in the highly regulated financial sector, the bank prides itself on being at the forefront of implementing state-of-the-art security controls, policies and procedures across all operations.

However, BRAC Bank must still address the familiar malware, spoofing and other familiar threat vectors. Also, it recognises that the cybersecurity threat landscape continues to change as data governance rules are adapted over time, including the Bangladeshi Guideline on ICT Security for Banks, PCI-DSS and SWIFT, while addressing payment partners' security requirements and other local regulations.

And, again typical, the bank has to fight to justify access to IT security resources and to retain security staff in a world where these skills are highly prized.

THE SOLUTION

BRAC Bank Head of Information Security B M Zahid-ul Haque and his team studied the importance of enhancing policies and practices to protect data held by privileged users as a strategic way to improve security. As they investigated the Privileged Access Management (PAM) sector, members of BRAC Bank's security team were introduced to CyberArk by local systems integrator and consulting firm OneWorld InfoTech.

During its procurement due-diligence process, an evaluation team was formed with a combination of multiple stakeholders that considered RFP responses, feature comparisons, scalability, proof-of-concept findings, financial negotiations, local partnering availability and experience, and support.

BRAC Bank evaluated several firms and products and canvassed internal feedback and expert opinion before settling on the CyberArk solution and OneWorld's assistance in implementation and post-implementation support.

“Finally, due to the track record of continuous innovation and a laser focus on the area, we found that CyberArk set a standard in privileged access management,” said Mr. Zahid-ul Haque. “With the deployment of PAM and CyberArk we are able to address compliance related to privileged access issues while being confident that the market-leading solution in privileged account security is protecting our keys to the IT kingdom.”

“With the deployment of PAM and CyberArk we are able to address compliance related to privileged access issues while being confident that the market-leading solution in privileged account security is protecting our keys to the IT kingdom.”

B M Zahid-ul Haque, Head of Information Security, BRAC Bank Limited

“In short, the big achievement is enhanced monitoring, compliance and security control over privileged access.”

BM Zahid-ul Haque, Head of Information Security, BRAC Bank Limited

Results & Key Benefits

- Stronger defence against internal and external attacks on privileged user accounts without added operational complexity.
- Bolstered compliance with regulatory mandates and local governance frameworks without added complexity.
- Better protection against ransomware.
- Greater ability to manage hard-coded visible passwords in applications.
- Improved analytics and insights into security threats for accelerated incident response.

At a Glance

- BRAC Bank is already an advanced bank with certified ISO 27001:2013 status but like all organisations needs to address security threats relating to privileged access to applications and data.
- BRAC Bank studied the importance of enhancing policies and practices to protect data held by privileged users (Privileged Access Management, or PAM) as a strategic way to improve security.
- Working with CyberArk and local partner OneWorld Infotech the entire PAM phased deployment was completed within six months.
- BRAC Bank is now in a strong position to defend against internal and external attacks on privileged accounts and core assets.
- Compliance has also been strengthened as BRAC Bank can secure more and provision, control and monitor all activities associated with privileged identities used in enterprise systems and applications.

BRAC Bank formed an internal team to work closely with CyberArk, gave team members initial training and decided on a phased approach to deployment. The implementation team rolled out a broad suite of software including solutions for:

- Privileged Access Manager
- Endpoint Privilege Manager
- Secrets Manager
- *NIX Server Protection
- Discovery & Audit (DNA)

THE RESULTS

Despite BRAC Bank’s phased approach, the entire deployment was still completed within six months and it has been a success, thanks to the support of senior management and the strong working relationship between CyberArk, OneWorld and the BRAC Bank internal team.

BRAC Bank is in a better position to defend against internal and external attacks on privileged accounts and its “crown jewels” core assets. Also, compliance has been strengthened as the bank can demonstrate to auditors that appropriate controls are in place and that credentials are being properly managed. “CyberArk has enabled us to secure more, provision, control, and monitor all activities associated with privileged identities used in enterprise system applications,” says Mr. Zahid.

BRAC was the first bank in Bangladesh to have understood the criticality of privilege accounts and as a result is better protected against ransomware, zero-day attacks, high-risk activities and potential vulnerabilities in hardcoded application passwords. It has the ability to detect suspicious activities and to react to incidents quickly, ensuring privileged access management controls are not bypassed by malicious insiders or external attackers.

LOOKING AHEAD

BRAC Bank is actively exploring more use cases for CyberArk in helping to help isolate, monitor and control privileged access activity as well as detect, alert and respond quickly to high-risk activity.

“We are actively exploring new use cases for CyberArk and have already begun initiatives in security operations,” says Mr. Zahid ul-Haque.

“CyberArk stopped password sharing and helped us to achieve regulatory compliance. It has also strengthened the security of legacy systems and removed weaknesses such as hardcoded passwords.”

BM Zahid-ul Haque, Head of Information Security, BRAC Bank Limited