Business challenge

Lacking an automated way to track privileged user access to sensitive IT systems, The Bank of Punjab (BOP) manually viewed and maintained data and asset records, increasing its exposure to risk and insider threats.

Transformation

To enhance security and eliminate the need to manually review privileged user activities on IT systems, BOP engaged IBM Gold Business Partner Trillium Information Security Systems (TISS) to implement IBM® Security Privileged Identity Manager technology. The solution centrally manages and audits privileged identities, reducing the bank's risk to internal threats.

Ali Manzar
Head of Information Security
The Bank of Punjab

Results

Helps minimize insider threats and improve security
by managing privileged identities across systems companywide

Reduces total number of privileged identities
by centralizing and streamlining identity management

Helps address compliance regulations
through automated password management, single sign-on (SSO) capabilities and auditing tools

The Bank of Punjab

Reducing risk and enhancing security with privileged management technology

Founded in 1989 and based in Lahore, Pakistan, BOP is a commercial bank with more than 450 branches throughout the country. It offers an array of retail and corporate banking products and services, including savings and term deposit accounts, personal and mortgage loans, credit cards, wealth management, insurance, and investment banking. In 2017, the bank employed over 6,500 people and reported total assets of PKR 649.5 billion.

"We chose IBM Security Privileged Identity Manager because it's a reliable security solution that met all the requirements of our customer."

—Waleed Rafique, Team Lead, Security Operations Center, IBM Business Partner Trillium Information Security Systems

trillium Information Security Systems
INSTITUTUM DE EXCELLENTIA

Share this

Manually auditing privileged user access

According to the 2017 IBM X-Force® Threat Intelligence Index, the financial services industry experienced the highest number of security attacks in 2016. The majority of those attacks—58 percent—came from inside organizational walls; of those, 53 percent were inadvertent and 5 percent were malicious. Whether originating from human error or intentional sabotage, a security breach can result in data loss, regulatory fines, erosion of consumer trust and other consequences that can devastate a bank. The risks make controlling and managing shared privileged IDs a corporate imperative.

At BOP, a group of privileged users, including IT administrators and systems managers, had elevated access to sensitive IT resources across systems, applications and databases. As the number of superusers increased, so did the bank's risk. Any accidental or intentional misuse of these privileged permissions could not only compromise customer data but also cause serious accountability and compliance issues for the bank and catastrophically damage its reputation.

Waleed Rafique, Team Lead of the Security Operations Center at IBM Business Partner TISS, elaborates on his client's security landscape: "In the past, if BOP wanted information regarding a privileged user, it had to access this information manually by viewing the logs on the endpoint device. Because it lacked a centralized solution for log management, it also had to maintain data and asset records manually."

Recognizing its vulnerability to insider threats, BOP sought a solution that would enable it to centrally manage and audit the use of privileged access credentials across its critical enterprise systems and applications. Rafique continues: "BOP's executives needed more visibility into privileged activity to improve security and demonstrate compliance. They wanted strong password management policies and the ability to track and provision privileged user accounts. Ultimately, they wanted to reduce the total number of privileged IDs. So they turned to us."

Centrally managing privileged user identities

To fully understand the bank's requirements, TISS performed a detailed analysis and produced a comprehensive statement of work (SOW) and project plan. Working closely with BOP, it then finalized a deployment plan to install and configure an IBM Security Privileged Identity Manager virtual appliance along with a directory server on the client's Microsoft Windows Server 2012 R2 operating system.

"IBM is a big name when it comes to security," says Rafique. "We chose IBM Security Privileged Identity Manager because it's a reliable security solution that met all the requirements of our customer. We were sure that this solution, coupled with our deployment and support, would be the best fit for BOP."

TISS began the engagement by preparing the bank's virtual machines. Next, based on solution configuration recommendations from IBM, it installed the security software and directory services to support virtual machines provisioning. Thereafter, it integrated the solution with the client's infrastructure.

To help BOP manage access to resources and automate administrative tasks, TISS also installed and configured the software's Active Directory Adapter agent on both the Microsoft Active Directory and SSO agents within the administrator's endpoints. Ultimately, based on its customer's requirements, TISS implemented the following use cases:

- Password randomization after initial input
- Manual check-in and check-out
- Automatic check-in and check-out using the SSO agent
- Workflow approval from resource owners in case of manual check-in and check-out
- SSO on the Active Directory through a remote desktop protocol
- SSO through VMware vSphere Hypervisor (ESXi) servers
- SSO through a secure shell (SSH) client
- SSO on Microsoft SQL Server databases using the Microsoft SQL Management Studio application

At the close of the project, TISS held a comprehensive knowledge-sharing session to ensure the bank's IT department could optimally use and troubleshoot the solution.

Improving security and reducing risk

Today, with centralized privileged identity management technology, BOP can manage and monitor privileged IDs easier and more effectively. In addition to improving security, it also reduced the total number of privileged IDs, with one superuser managing all privileged users through a centralized dashboard. As a result, it minimized instances of human error and, in turn, risks and insider threats.

"BOP significantly reduced the requirement of privileged IDs," adds Rafique. "Plus, managing the administrators is very easy and hassle-free."

With automated password management and SSO capabilities, Security Privileged Identity Manager technology helps BOP protect access to its resources. These capabilities, combined with auditing features, enable the bank to better address compliance, regulatory and privacy requirements.

Ali Manzar, Head of Information Security at BOP, is pleased with the solution and with the service TISS provided. "Trillium Information Security Systems has a very proficient technical team," says Manzar. "They resourcefully resolved all the problems at our end. They were very accessible and answered all our queries efficiently. We definitely recommend them."

About Trillium Information Security Systems

Founded in 2005 with a head office in Rawalpindi, Pakistan and local offices in Karachi and Lahore, IBM Gold Business Partner TISS is the country's leading cybersecurity company and Pakistan's first organization focused on information assurance. Named one of the top 25 IBM Solution Providers in 2017 by APAC CIOoutlook Magazine, the company provides services, solutions, training and distribution represented by four dedicated brands, respectively: TRIAM, TriSol, TRISECT and TISP. TISS employs roughly 100 people and has a dedicated in-house R&D department that developed Pakistan's first and only threat intelligence platform, "T-Eye", which has received multiple local and international awards and recognition.

Solution components

- IBM® Security Privileged Identity Manager
- Trillium Information Security Systems

Take the next step

To learn more about the IBM solutions featured in this story, please contact your IBM representative or IBM Business Partner.

Please Recycle

07018607USEN-02