Enhancing cybersecurity through *privileged access management*

A European telecom leader strengthens identity security with cloud-based PAM, automation, and disaster recovery readiness.

As part of its general effort to strengthen cybersecurity, a multinational telecommunications company engaged Capgemini to implement a new cloud-based Privileged Access Management (PAM) solution. The CyberArk PAM system delivered granular access control and introduced automation that simultaneously improved the organization's efficiency.

A global telecom leader sought to bolster its security posture through a series of transformative projects. More specifically, the company wanted to improve its ability to manage privileged accounts on a global scale. To do so, the organization needed a robust solution to deploy and migrate its PAM system, onboard various applications, and establish a reliable disaster recovery plan.

The existing system lacked governance and monitoring for database access, and the company possessed limited documentation related to its database architecture and processes. Additionally, the sale of public IPs at its data center posed a risk to PAM servers, necessitating a swift and effective disaster recovery solution.

Client: European multinational telecommunications company

Region: Europe

Industry: Telecoms

Client challenge: The organization wanted to more effectively manage global privileged accounts, introduce onboarding applications, and establish a reliable disaster recovery plan, with limited governance and documentation for database access and architecture.

Solution: Capgemini implemented a cloud-based PAM solution, performed detailed database assessments, and deployed disaster recovery components.

Benefits:

- 25 databases onboarded
- Expanded security and access controls
- Streamlined account management

The Cybersecurity Identity and Access Management (IAM) team at Capgemini stepped in to deliver three key initiatives using CyberArk's PAM solution. These projects included a Greenfield implementation, migration of entitlements from the incumbent system to Capgemini's Identity as a Service (IDaaS) platform, and comprehensive application onboarding.

Strategic privilege management for enhanced security and efficiency

Following a methodical and strategic approach, Capgemini conducted a six-week fast-track assessment to evaluate the existing system and identify areas for improvement. Based on the results of this review, the project team transitioned the company to a cloud architecture hosted within Capgemini's Cloud. This move ensured that the service remained up-to-date and efficient.

In the application onboarding phase, Capgemini performed detailed assessments on 25 databases of various types, including Oracle, DB2, and MS SQL. Custom plugins were developed for session management in the QA environment, and additional databases such as Azure MSSQL, SAP S/4HANA, and Oracle were onboarded. The team also automated the onboarding of SOX servers to the PAM solution, providing clear visibility and a comprehensive solution blueprint.

The disaster recovery project was critical due to the company's mandate to complete the DR change before September 2024. Capgemini deployed CyberArk DR components, including the Central Password Manager and Session Manager for both Windows and Unix, each of which were installed and configured in the new Azure Data Center. This ensured seamless integration with all target applications and enabled smooth, uninterrupted updates to partner connectivity systems. Finally, the project concluded with a thorough clean-up of regional license records.

Achieving robust cybersecurity and operational excellence

The telecom leader now enjoys granular privileged access controls, preventing unauthorized access to account credentials while ensuring authorized users have the necessary access for legitimate business purposes.

Centralized secure storage protected privileged account credentials across on-premises, hybrid, and cloud environments, as well as throughout the DevOps pipeline. In addition, detailed audit reporting provided security and audit teams with clear visibility into who accessed which accounts, as well as when and why. Automatic credential rotation ensured that privileged account passwords and SSH keys were regularly updated and synchronized. End-to-end automation simplified privileged account management tasks by implementing REST APIs, streamlining workflows, onboarding new rules, and clarifying permission granting.

The successful implementation of CyberArk's PAM solution represented a significant step forward for the company's cybersecurity posture. By enhancing security, providing granular access control, and achieving end-to-end automation, Capgemini helped the organization demonstrate a strong commitment to security and resilience. This partnership propelled the company to develop a more secure and efficient operational environment, solidifying its position as a global leader in cybersecurity.

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Make it real | **www.capgemini.com**

For more details contact:

cybersecurity.in@capgemini.com