IDENTITY AND ACCESS MANAGEMENT (IAM) SOLUTION

for a Leading Telecommunication Service provider

Service: Security

OVERVIEW

Headquartered in Brussels, Client is a $6billion telecommunication service provider. Client wants to deploy and manage IAM solution for one of their enterprise customers having distributed IT infrastructure across Europe.

The key areas worked upon include:

- CyberArk Privilege Access Management (PAS) solution
- Multi Factor Authentication (MFA)
- Password vault web access management

CHALLENGES

Customer wanted to implement privilege access management solution

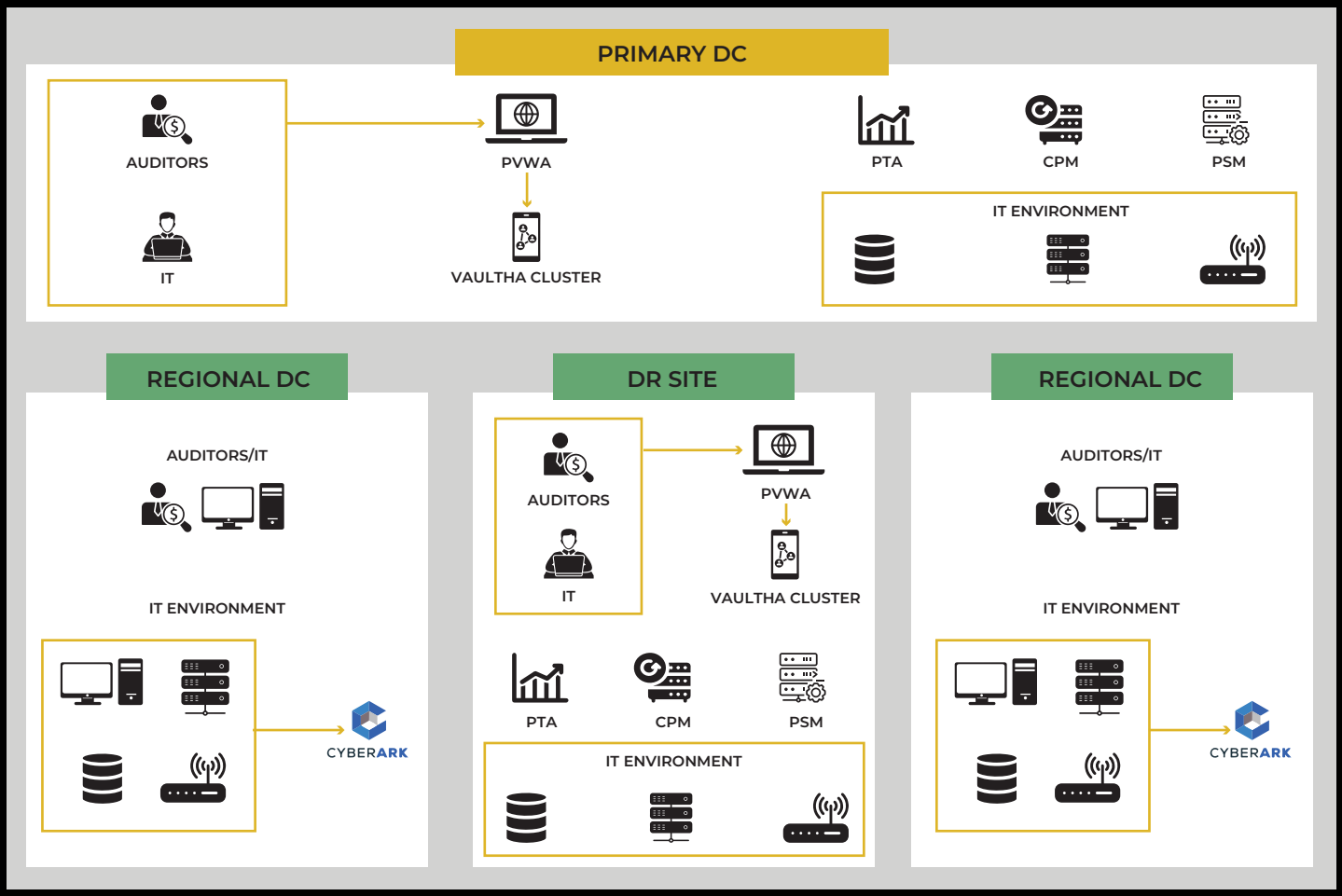
Need for an automated password and privileged session management platform for secure access control to be designed

Build a platform that caters to all types of privileged accounts, ranging from local or domain shared administrator accounts to users personal admin accounts

SOLUTION

1. CyberArk Privileged Account Security (PAS) solution for Privilege account management
2. Build, Design and Implement PAM in DC and DR environment
3. PAM Solution in DC and DR for Password Management, Privileged Access Management
4. Control, Monitor, Manage Privileged user access to critical systems for organization systems
5. Secure storage of administrative and privilege passwords including local admin and domain accounts wherever applicable
6. Centralized access control policy and Privilege User Password Management

Solution Overview



Solution Components

SECURE DIGITAL VAULT	▪ A hardened and secured server used to store privileged account information ▪ Based on a hardened Windows server platform
PASSWORD VAULT WEB ACCESS(PWA)	▪ A web interface for users to gain access to privileged account information ▪ Used by vault administrators to configure policies
CENTRAL POLICY MANAGER (CPM)	▪ Performs password changes on devices ▪ Scans the network for privileged accounts
PRIVILEGED SESSION MANAGER(PSM)	▪ Isolates and monitors privileged account activity ▪ Records privileged account sessions
PRIVIVILAGE THREAT ANALYTICS(PTA)	▪ Monitors and detects malicious privileged account behaviour

OUTCOME

- Users can secure and automate all processes that involve privileged account passwords and SSH keys, such as discovery and management
- Privileged Accounts Discovery and Privileged User Accountability
- Recording and Playback of Privileged User sessions
- Secure way to access applications and systems
- Automatic password management on supported platforms

HIGHLIGHTS

- Active Directory user and Admin account On-Boarding
- Multi Factor authentication (MFA) for users to access critical applications
- Integration of SMTP for E-mail Notifications
  - 15000+ servers for Privilege Account Management
  - 20+ administrative account for privilege access management

To know more about how ACL can partner with you to help create Digital Transformation, connect with: **business@acldigital.com**

www.acldigital.com

USA | UK | France | India