Privileged Identity Management in Enterprise IT

ARCON

Privilege Identity Management in Enterprise IT

Privileged User Access

The access to systems, databases, servers and applications through privilege user accounts as well as the password management of these key user accounts is emerging as the most important challenge in today's IT environment, where flexibility in access with quick resolution of issues is of utmost importance to business.

Privilege Access	Market Challenge
Unix/Linux Windows Oracle Sybase My SQL MS SQL AIX AS400 Routers Switches Firewall	Privilege user accounts have complete access to the system thus business data/information can be easily accessed and/or changed if any such account or user password is compromised. Further privileged access is generally not audited as audits on databases and operating systems are cautiously enabled to avoid performance constraints. **Control: None**

Privileged Password Management

Typically, password policies for privileged IDs are very strict. The policies require those passwords to be changed at very short intervals, and sometimes use password strength policies that require people to write down the passwords. Those guidelines can make password management even more costly and risky.

Further the passwords are required to be manually changed on every system and printed on envelopes, with physical register for managing the access to the envelopes and reprints. If this is compared to a scenario where there is more than 2000 database, 2000 operating systems etc. The time and efforts will be significant but would still not ensure secure password management processes.

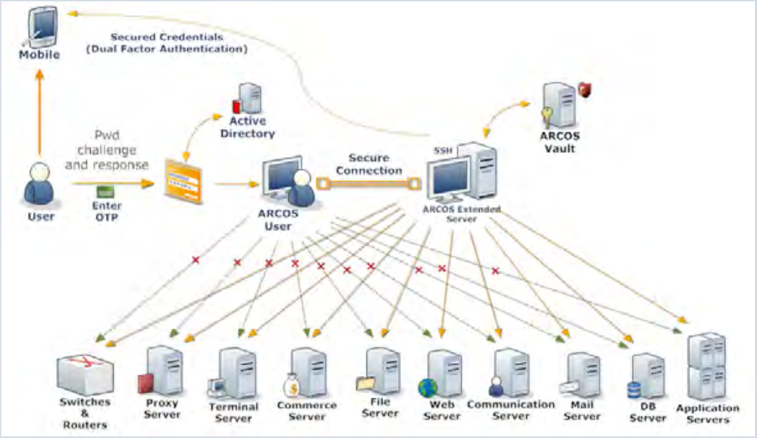
Other organizations recognize this account management overhead and try to avoid it by simply sharing privileged passwords among the teams that require them. This method puts any organization in a very precarious situation, with sensitive credentials being both poorly secured and lacking an ability to trace actions to a single person. Managing privileged passwords are one of the most important challenge in today's shared IT environment.

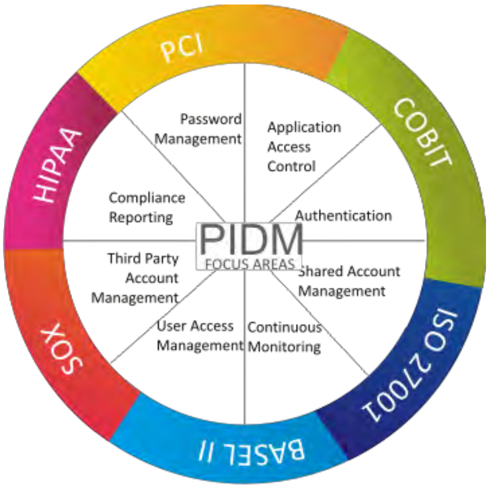
Regulatory Compliances

The increasing focus of regulatory compliances like SOX, PCI, HIPPA, ISO etc has left organizations with no alternative but to implement automated solutions that address these challenges comprehensively.

Our Solution

Our solution provides a security blanket that sits on top of all Operating Systems & Databases. All IT Administrators like Sysadmins, Database Administrators, as well as Application Administrators are allowed to logon to their respective systems only by using a unique user-id & password and OTP (one time password) provided to them. Once logged in, view/modify access is provided on “need to know” and “need to do” basis. Further, activities carried out are recorded and complete audit trails are maintained. The solution provides a secure umbrella around the data stored in various systems. Its key features are listed in
Table 1.





Features

Single Sign On

Privilege user accounts to have restricted access to data.

Complete Audit Trails for all activities performed by privilege users

Automated Password Management

Secure Password Vault for storage of password

Electronic password sharing with workflow

Secured password printing

Remote Vendor Control

Conclusion

Organizations must move from a reactive approach to proactive and cost effective controls. Enterprises must go beyond the minimum requirements of regulatory compliance to internal policy compliance at a higher level of assurance by ensuring compliance to internal polices.

In the current scenario of booming economic growth, large & growing organizations are faced with challenges to information security on account of IT Administrator activities. The solution provides a comprehensive means of tackling such challenges & thereby ensuring adequate controls, regulatory compliance and also reduction in IT spends.