

functions of

# PRIVILEGED ACCOUNT MANAGEMENT



## PROTECT FROM INSIDE THREATS

Maintain minimal possible permission level for IT administrators



## SHARE SERVER ACCESS

Let employees and remote partners to access servers easily without disclosing credentials



## DISCOVER AND RESET DEFAULT PASSWORDS

Use strong passwords for local admins and root accounts, IoT and network devices



## ROTATE PRIVILEGED ACCOUNT PASSWORDS

Maintain strong passwords for privileged accounts and minimize number of user who know them



## LIMIT NUMBER OF PRIVILEGED ACCOUNTS

Decrease attack surface by limiting number of accounts with elevated privileges



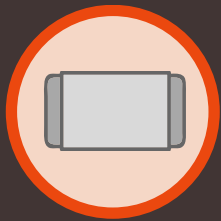
## STORE AND SHARE SECURITY CERTIFICATES

Store and share security keys, code signing, SSL and other certificates in a secure central vault



## DELEGATE EXECUTION OF PRIVILEGED SCRIPTS

Let users to execute limited set of privileged scripts or commands on critical systems



## REMOVE HARD CODED PASSWORDS

Eliminate passwords hard coded in the command line scripts or application configuration



## MONITOR SHARED ACCOUNT ACCESS

Keep audit log of events related to elevated access including recording of remote sessions



## COMPLY WITH INDUSTRY REGULATIONS

Stay on top of security audits and latest trends in Information Security