5 essential elements that YOU SHOULD AVOID WHEN DEPLOYING MODERN PAM

1 Permanent access authorization or credentials

SSH is a very reliable and robust method to secure data-in-transit which is why it is the de-facto access method in Linux-based environments.

However, since SSH keys never expired, you can never be sure if they are shared. You should remove any permanent access in your new environment.

2 Password vaults

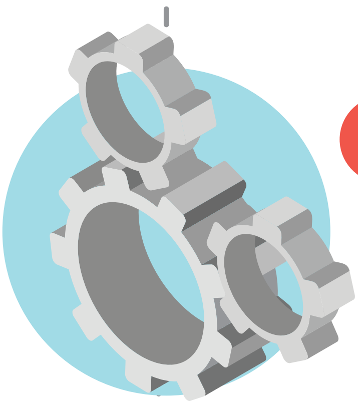
Password vaults are a standard feature of many PAM solutions. On the surface their use might seem to make a lot of sense, but it is actually creating a single point of failure in case of breach or misconfigurations.

It is also trying to solve the problem created by permanent access credentials by still using permanent access credentials.

3 A complex IT project that turns your infra into a monster

It seems many PAM vendors believe that bigger is better. But with bigger you also get complexity and with complexity comes friction & inertia.

Make sure your IT staff does not spend months deploying, installing, configuring, patching up and updating the software instead of using it.



4 Extensive training

The more complicated the solution, the higher risk of misconfigurations due to complexity.

Ensure the solution is lean and easy to use to avoid spending a lot of time and resources on training your staff on-board with the product.

5 Manual, repetitive and time-consuming tasks

A modern PAM with a zero trust approach could keep you away from complicated password policies and procedures for internal staff and external vendors and contractors.

Bad user experience increases the risk of PAM users trying to bypass burdensome controls.

SSH.COM