TECH BRIEF

Privileged Account Management

Software Solution vs Virtual Solution vs Hardened Appliance

Pros & Cons Highlights

Software:

- 👍 Simple to install
- 👎 The host operating system must be maintained and patched

Virtual:

- 👍 Supporting this platform can be simple
- 👎 Additional security is required to secure the virtual appliance

Hardened:

- 👍 Engineered to reduce vulnerabilities and has been hardened by the manufacturer
- 👎 A hardened physical appliance requires power and rack space

There are many vendors providing a wide variety of Privileged Account Management (PAM) solutions that are available in a variety of form factors, the main types being software-based, hardened virtual or hardware appliance. Depending on a number of things – such as industry, employee population, existing systems and business philosophy – enterprises even of similar size and focus can have very different PAM solution needs. This technical brief is designed to outline some key considerations when considering the ideal type of PAM solution for your organization.

Software PAM solution

This is a PAM solution deployed as an application. The organization must supply the platform (hardware and operating system).

Pro:

- Simple to install locally or on a remote data center
- Typically run on a standard Windows platform
- Relatively affordable

Con:

- The organization must supply hardware (physical or virtual) and the host operating system.
- The host platform must be secured by the organization. This includes the physical or virtual host, the operating system and all configurations within the operating system, such as database and firewall.
- The host operating system must be maintained and patched. In most cases, the PAM application runs on a server in the data center, just like any other enterprise application. This server must be maintained with patches, which can introduce vulnerabilities in that the person responsible for maintaining the server will require administrator access to the PAM server and can bypass or disable PAM functionality.
- Breaches of PAM applications can be difficult to detect. Any attempt to breach or copy the application or its database can go undetected as the application may not be aware.
- The PAM solution's scalability is limited by the resources of the host operating system.
- Backup and recovery of the PAM application can be challenging as it should be backed up outside of the normal server backup and recovery plan. And its high-availability requirements need to be considered.

Virtual appliance PAM solution

This is a PAM solution that is deployed as a virtualized appliance. This system can be a physical appliance that has been virtualized – or a PAM application and host OS that has been virtualized.

Pro:

- Most larger organizations have a virtualization infrastructure. For these organizations, a virtualized PAM solution is a good fit.
- If the PAM solution is a truly an appliance that has been virtualized (in that there is no direct access to the host OS), then supporting this platform can be simple.

Con:

- Additional security is required to secure the virtual appliance. The operating system must be protected against all of the standard types of intrusions and must also be protected against cloning or copying. An attacker may attempt to copy or clone the virtual appliance and export it for an offline compromise.
- Vulnerabilities of a virtualized system are similar to the software PAM solution if the solution is simply a virtualized server with a PAM application installed.

Hardened-appliance PAM solution

A hardened-appliance PAM solution is delivered on specific hardware and the operating system is not accessible by users or administrators.

Pro:

- Since all software is preinstalled, deployment can be done very quickly.
- The operating system of the hardened appliance has been engineered to reduce vulnerabilities and has been hardened by the manufacturer. The administrators and users have no access to the host operating system.
- Since the PAM solution is running on a proprietary operating system, regular patching and maintenance of the host OS is not required. If a patch is necessary it is provided by the manufacturer.
- The hardware PAM solution cannot be copied or cloned for an offline attack. For a bad actor to attempt an offline penetration, the appliance would need to be physically removed.
- In a hardware PAM solution, appliances can be easily deployed for high-availability and load balancing.
- Hardware that is purpose-built and dedicated to PAM can easily scale up to meet growing enterprise needs.

Con:

- A hardened physical appliance requires power and rack space.

Hopefully this provides some insight and guidance for your PAM solution decision-making process. One Identity and Quest Software have been a leader in delivering identity and access management (IAM) solutions that easily integrate with your PAM program. Privileged accounts or 'keys to the kingdom' are the most critical accounts in your enterprise. So regardless of the size, focus or the business philosophy of your organization, the One Identity PAM portfolio has solutions to meet your varied needs. We set a strategic goal for our development team to make our PAM solution the most secure and innovative product offering in the market. These decisions have led us to be the lone 'hardware-only' solution in the market, and we believe the security of this solution speaks for itself.

About One Identity

One Identity by Quest, lets organizations implement an identity-centric security strategy, whether on-prem, in the cloud or in a hybrid environment. With our uniquely broad and integrated portfolio of identity management offerings including account management, identity governance and administration and privileged access management, organizations are empowered to reach their full potential where security is achieved by placing identities at the core of the program, enabling proper access across all user types, systems and data.

Learn more at OneIdentity.com

TechBrief-PAM_SoftwareHardwareVirtual-RS-64005