cloudbridge
uc_clearly;

Achieving Zero Trust with PAM?

WHAT IS PAM?

Privileged Access Management (PAM) refers to security processes and technologies to control elevated ("privileged") access (i.e. Administrator accounts). This is usually accomplished by putting the privileged credentials inside a secure repository (a vault). This has the effect of isolating the use of privileged accounts to reduce the risk of those credentials being stolen or used incorrectly.

WHY PAM?

Privileged credentials are the "keys to the kingdom"; they provide access to all systems and all data. Should these credentials become compromised, a significant security breach would likely occur.

Each system, application and device typically has at least one privileged credential, in some cases multiple. When looking at an organization as a whole, there are often hundreds if not thousands of these credentials.

Since system administration is typically performed using these credentials, the industry has sought to move these credentials to a PAM system. The PAM system then dispenses temporary credentials or directly brokers access to a system via industry standard access methods such as SSH and RDP.

The organization is not just concerned with the credentials but also with how they are used. As such, most PAM systems provide some form of auditing, often in the form of session recording. Of course, this only works for brokered sessions.

The many systems, credentials and accesses make PAM a very significant investment for an organization. Many orgs report huge costs and implementation times of over one year.

THINGS TO KNOW BEFORE IMPLEMENTING PAM

The acronym means "privileged access management". It's thus easy to believe that PAM is the answer to managing privileged access but there are some very serious issues that an organization should consider when planning for their access management.

1. **PAM does not fulfill the goal of Zero Trust.** PAM is a password and session management technology, but organizations must still place trust in their administrators to do the right things.

2. **PAM doesn't control privileged access.** PAM controls access to credentials, not systems and data. Once credentials are retrieved from the PAM system, the user has uncontrolled native access to the systems and data. Even if the PAM system brokers the connection via RDP, it does not control what the user does. Once connected to the resource, the user can perform any action that the credentials allow.
3. **PAM adds significant overhead** – It can take many organizations up to a year to deploy and become operational with PAM. Once credentials are moved into the PAM system, staff become 100% dependent on the PAM system to perform administration. When an administrative operation requires access to many systems, the admin must make multiple credential requests to PAM. This adds layers of complexity, burden and dependence. This requires a significant cultural commitment and is one of the leading reasons PAM deployments fail.
4. **PAM is a password manager.** Often, for many organizations, PAM becomes little more than a complex password manager. PAM grants temporary access to credentials and the connection to the system is completely uncontrolled.
5. **PAM does not solve the problem of human error.** When an admin deletes the wrong resource, or misconfigures a policy, PAM does nothing to prevent it; the damage is done and at best, PAM has recorded it.
6. **PAM is forensic, not preventative.** When PAM brokers a connection to the remote host, it typically audits the session. In most organizations, these recordings are not reviewed. At best, when they are reviewed, they provide forensic data for understanding what happened subsequent to a serious breach. PAM is not preventative.
7. **PAM is hard to remove.** Once an organization's credentials are migrated to the PAM system, it can be incredibly painful to roll back to pre-PAM operations.

SHOULD YOU DEPLOY PAM?

PAM systems are becoming a mainstay of modern computing. Understanding the issues noted above can help an organization plan for success. While most organizations consider PAM as necessary, it's important to understand that it is only one step in managing access and it's an expensive step that will take significant organizational resources to fulfill.

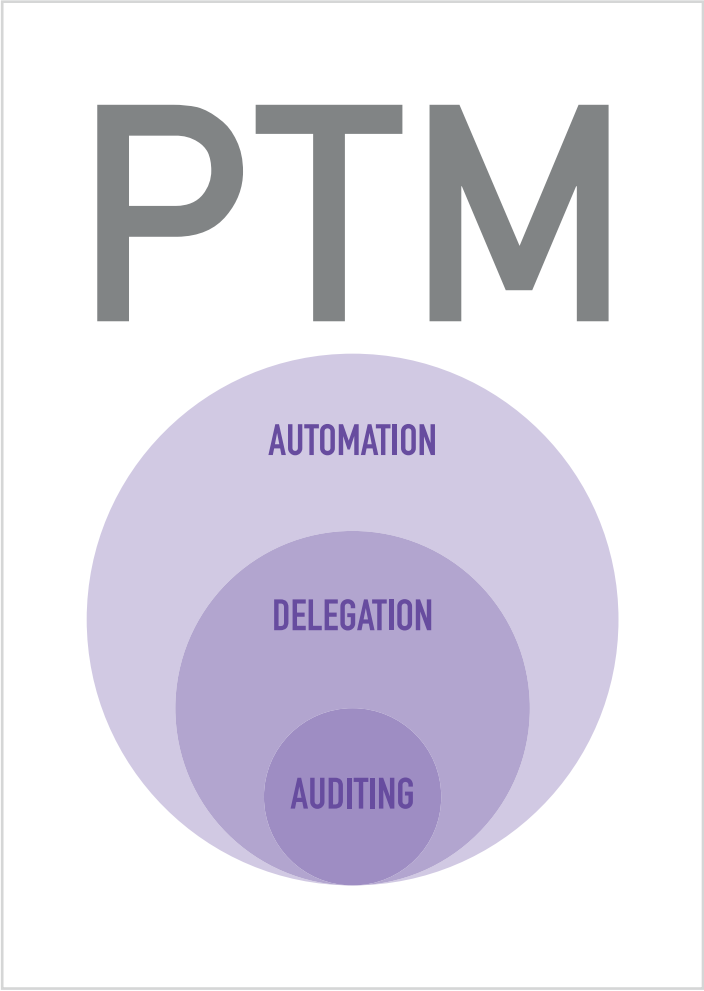
ACHIEVING ZERO TRUST?

To achieve zero trust, the organization must remove privileged access. To date, this is not possible with PAM. Organizations with a PAM investment can achieve zero trust with the addition of PTM. PTM directly integrates with an organizations PAM system.

WHAT IS PTM?

PTM is the intersection of three disciplines: Automation, Delegation and Auditing. PTM is a business-centric approach to systems management that was created to solve the problem of zero trust and data privacy.

PTM removes all native access to systems and data. Instead, users perform operations via automated Tasks. These Tasks are then delegated to the people that need to perform the Task. Tasks are programmed, repeatable, controlled; no trust is required. A user can perform only the operation allowed within the task. Tasks are delegated to roles or individuals within the organizations, whether that is an admin, helpdesk or business user. Tasks provide the benefit of a secure framework for operations but also provide optimal efficiency through automation. When a Task is executed, an audit record is captured that properly tells the story of the business task being performed; the who, what, where, and when of the operation.



A BUSINESS-CENTRIC APPROACH TO SECURITY

Every method of security to date has required trust. We have historically seen our IT systems from a systems-centric view; a bottom up perspective. A sea of atomic systems that need to be managed with ever-increasing complexity. PTM changes this to a top down, business-centric approach where the operational tasks are modeled and delegated to the people that need those tasks. PTM provides significant business benefits:

- Zero Trust is achieved
- Unwanted access to systems and data is eliminated and can be demonstrated for GDPR, CCPA and other privacy regulations
- Builds on an existing PAM investment
- Adds value on day one and continues to grow in value each day
- Removes barriers rather than adding them
- Removes IT as a bottleneck, makes systems accessible to the business
- Allows IT staff to focus on creating Tasks rather than doing them
- Reduces helpdesk costs
- Integrates operations across multiple systems
- Allows an organization to grow faster than their IT departments can grow

TASKS, THE HEART OF PTM

At the heart of PTM is a modeled Task. PTM makes it simple for an organization to model complex tasks. In just a few hours, an organizations first Tasks become operational with the following benefits:

- Tasks are modeled once and used repeatedly
- Tasks encompass business process knowledge
- Tasks remove dependence on people
- Human error is eliminated
- Task audit records tell the true story of who, what, where and when
- Eliminate complex log assembly and diagnosis for operational awareness
- Capable of complex, multi-system operations and incorporating approvals
- Reduce organizational burden

CLOUDBRIDGE PTM

Cloudbridge is the undisputed leader in the PTM space. Cloudbridge makes it simple to realize PTM. Cloudbridge includes hundreds of already-modeled Tasks for managing users, groups, mailboxes, mailflow, and more. Cloudbridge makes it extremely simple to model Tasks using familiar PowerShell and then provides instant Web Portals where Tasks are delegated to roles or individuals in the organization. In under 30 minutes, typical organizations are getting PTM value. Advance 24 hours and several tasks are modeled that will never again need privileged access. With each additional day, the labor of doing tasks is exchanged for modeling tasks and a snowball effect is created. In months, an organization has achieved zero trust across many disciplines and the business becomes increasingly secure, and increasingly empowered with automation.

CLOUDBRIDGE PTM FEATURE LIST

REQUIREMENTS	SUPPORTED
BUSINESS	
Enables true Zero Trust operations	**YES**
Eliminates privileged access	**YES**
Satisfies burden of proof (who, what where, when why)	**YES**
Automates complex multi-system Tasks	**YES**
Alerts staff to unexpected environmental changes	**YES**
Reduces technical staff workload	**YES**
Reduces technical issue escalations	**YES**
Reduces impact of staff turnover	**YES**
Enables Task delegation direct to business users	**YES**
Automates Help desk operations	**YES**
Multi-tenant and hybrid support	**YES**
Supports separation of duties	**YES**
Consistent UX for business user tasks	**YES**
Retain data over time for compliance	**YES**
INTEGRATIONS	
Service Now integration	**YES**
Other ITSM integration	**YES**
Integration with 3rd party PAM	**YES**
Integration with IAM systems	**YES**
HRMS integration	**YES**
Active Directory integration	**YES**
Azure AD integration	**YES**
Third party LDAP directory integration	**YES**
Multi-database integration	**YES**
Bi-directional REST integration	**YES**
PowerBI integration	**YES**

REQUIREMENTS	SUPPORTED
IDENTITY SUPPORT	
Supports SSO	**YES**
Supports linked identities (IAM, Directory)	**YES**
Role based access	**YES**
Self-service, business facing portals	**YES**
IAM integration	**YES**
Multi-tenant support	**YES**
SECURITY	
Integrated credentials vault	**YES**
Data at rest encryption	**YES**
Data in motion encryption	**YES**
Data in motion encryption	**YES**
Integrated security alerting	**YES**
Dual layer 256 bit encryption	**YES**
Supports end-user MFA	**YES**
End user supplied certificates for code signing	**YES**

REQUIREMENTS	SUPPORTED
DEPLOYMENT / ONBOARDING	
SaaS based, zero deployment*	**YES**
Scales to enterprise	**YES**
Supports multiple on-prem locations	**YES**
Supports mulitple cloud tenants	**YES**
Predefined Tasks for immediate value	**YES**
Value on day one	**YES**
TASK CREATION AND MANAGEMENT	
Task based auditing	**YES**
Scripted Task creation	**YES**
Delegate individual Tasks	**YES**
Supports complex workflow	**YES**
Supports open-source community driven content	**YES**
Leverages existing PowerShell script investments	**YES**
Task tamper protection	**YES**
Integrated, multi-cert code signing	**YES**
Automatic script versioning	**YES**
Empower external entities with privileged Tasks	**YES**

ABOUT CLOUDBRIDGE

Cloudbridge's solutions re-imagine IT management. By enabling true automation, we empower organizations to reduce their security exposure, reduce their operational costs and embrace new technologies in ways that empower their business.

FOR MORE INFORMATION AND A FREE TRIAL, VISIT :

http://www.cloudbridgeplatform.com

cloudbridge
uc_clearly;

555 Legget Drive
Suite 304, Kanata, ON
K2K 2X3

info@ucclearly.com
+1 (613) 867 7177
www.cloudbridgeplatform.com