Cyolo

The ‘Last Mile’ of Application Security: Extending Your Privileged Access Management (PAM)

Underpinning every single organization is some sort of digital identity management solution. Whether it is accomplished with an on-premises Active Directory, Software-as-a-Service (SaaS), or a homegrown solution, managing the digital identity of users is crucial to maintaining an efficient and profitable business. These identity systems enable users to access the assets they need to perform their jobs.

Privileged Access Management (PAM) tools were designed to secure, monitor, and control the level of privilege each user receives. PAM secures how privileged users access highly secure, regulated, and mission-critical assets. A privileged user is someone who has access to very sensitive assets, such as HR staff who edit payroll information, or an Industrial Control Systems (ICS) operator who accesses Programmable Logic Controllers (PLCs) in a certain plant. Whenever access is given to a system that is deemed mission-critical for the business, a privileged user is created.

Most PAM solutions work by managing the credentials used in these privileged accounts. Users cannot be trusted to secure or even remember their own credentials, and credential compromise serves as a catalyst for many major breaches. **By centralizing and storing privileged account credentials and layering in the capabilities to check-in/out and rotate credentials, PAM solutions reduce the number of users who have access to sensitive systems and then secure those who truly do need such access.**

PAM solutions only cover credential management and do not account for how a user accessed the application.

‘LAST MILE’ APPLICATIONS

- Leave systems unprotected
- Create vulnerability
- Compromise security controls
- Cause security incidents
- Allow for cyberattacks

While there has been a clear market need for this type of solution across multiple verticals and industries, PAM alone cannot protect your entire organization's tech stack. PAM solutions only cover credential management and do not account for how a user accessed the application. If a user can get to the application and present the privileged credentials, they will be granted access. Validating users *before* they present privileged credentials is a gap for many organizations. Additionally, PAM cannot support password management for legacy, thick-client or homegrown applications.

Simply stated, PAM solutions do not secure the 'last mile' of resources that pre-date the development of modern password security. These resources are often critical to the operation of the business, so upgrading them to be compatible with modern security tools, like PAM, is not immediately feasible.

A PAM solution is a necessary part of most organizations' security strategy, but there remains a gap in the 'last mile' of applications and services that are not covered.

Enter the Cyolo zero-trust access solution,

which augments existing PAM deployments by enforcing identity-based access and connectivity for the 'last mile.' Cyolo defines what users can access based on factors like risk, geo-location, time of day, and a long list of additional policy options. Cyolo can also apply controls for file uploads, clipboard access, and file downloads amongst other physical device controls. When paired with an existing PAM solution like Thycotic or CyberArk, Cyolo handles the actual connectivity to PAM-guarded assets with an arms-length interface. An added benefit is gained by securing access to critical applications, especially those that PAM solutions struggle to secure.

AUGMENTS PAM BY ENFORCING IDENTITY-BASED ACCESS AND CONNECTIVITY

APPLIES CONTROLS FOR FILE UPLOADS, DOWNLOADS, AND CLIPBOARD ACCESS

SECURES ACCESS TO KEY APPLICATIONS THAT PAM STRUGGLES TO SECURE