3 LEVELS OF PAM MATURITY

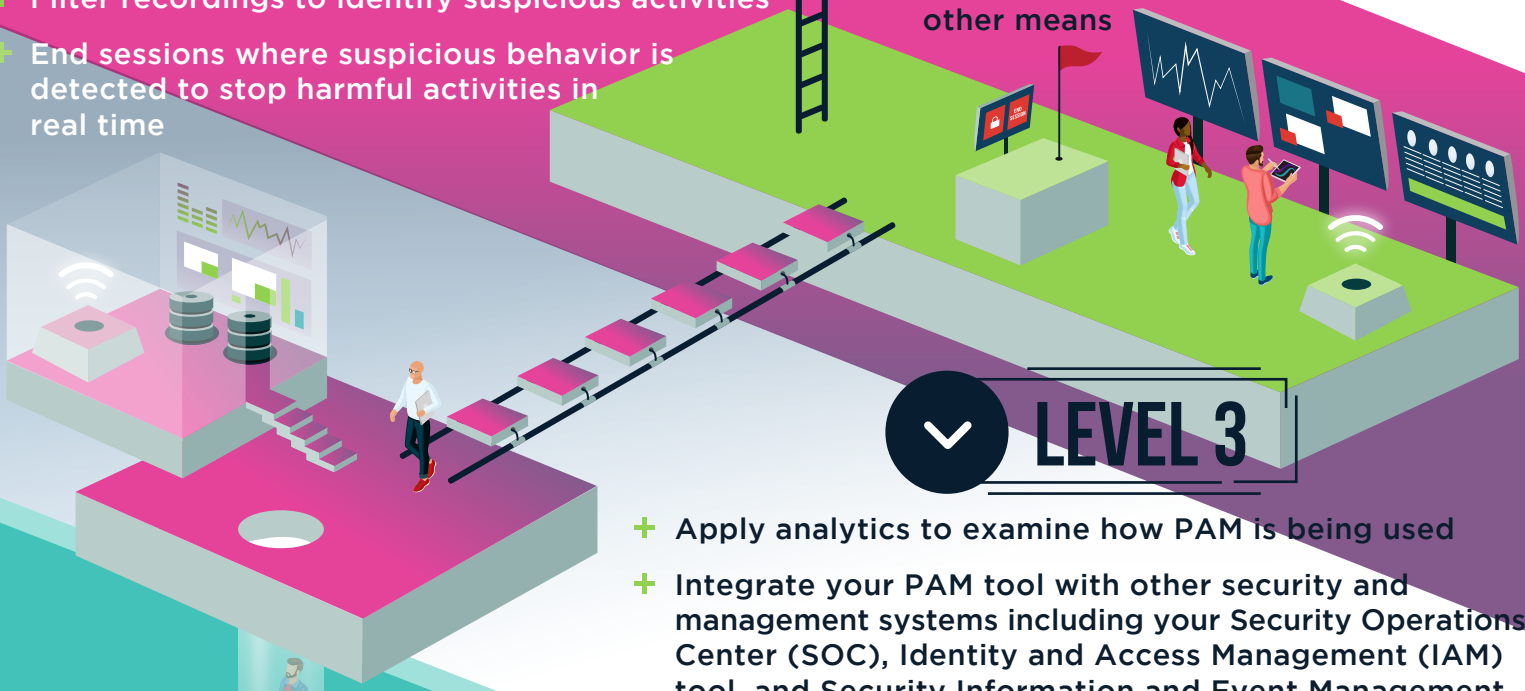
Privileged Access Management (PAM) helps you secure your organization's most powerful access on its most sensitive systems: the privileged administrative accounts that control your critical servers, databases, and networks. A lot goes into building a successful PAM program. Wondering what the journey looks like? Sila has defined 3 levels of PAM maturity to help you chart your course.

LEVEL 1

+ Assess and prepare your organization by defining "privilege" and mapping out PAM-relevant apps, access, and stakeholders
+ Implement manual password check-in/ check-out to prevent unauthorized user access
+ Enable automatic password reset upon check-in to prevent improper password reuse or sharing
+ Harden your vault to ensure users cannot circumvent your PAM system and gain access to critical systems via other means

LEVEL 2

+ Implement full session management to monitor and record user actions
+ Filter recordings to identify suspicious activities
+ End sessions where suspicious behavior is detected to stop harmful activities in real time



LEVEL 3

+ Apply analytics to examine how PAM is being used
+ Integrate your PAM tool with other security and management systems including your Security Operations Center (SOC), Identity and Access Management (IAM) tool, and Security Information and Event Management (SIEM) tool
+ Work closely with all of your security and management systems teams and develop processes to ensure a robust, well-aligned, and scalable security program

For more information about starting your PAM journey, contact Sila at
info@silasg.com | **SilaSG.com**