REDUCING RISK: START WITH PRIVILEGED USERS—DEVELOPING YOUR PRIVILEGED ACCESS MANAGEMENT (PAM) PROGRAM AND STRATEGY

Chrysalis Panel Discussion

TECHVISION
CHRYSALIS

Your Presenters

- Jeff Margolies, Chief Strategy Officer, Saviynt
- Doug Simmons, Principal Consulting Analyst, TechVision Research, author of TechVision's series of PAM Reports

What is This Session About?

- Many if not most breaches start with compromised credentials, especially administrative credentials.
- Multi-cloud deployments are expanding the attack surfaces.
- PAM is a specialized category of access management that provides increased protection for administrative accounts that are the most highly coveted by bad actors and can generally do the most damage.
- This session will describe an approach to developing a “least privileged” security model and leveraging increasingly sophisticated PAM products and services.
- We’ll also get insights into the directions and investments being made by key vendors in this space and include guidance for enterprise security leaders.

Thesis

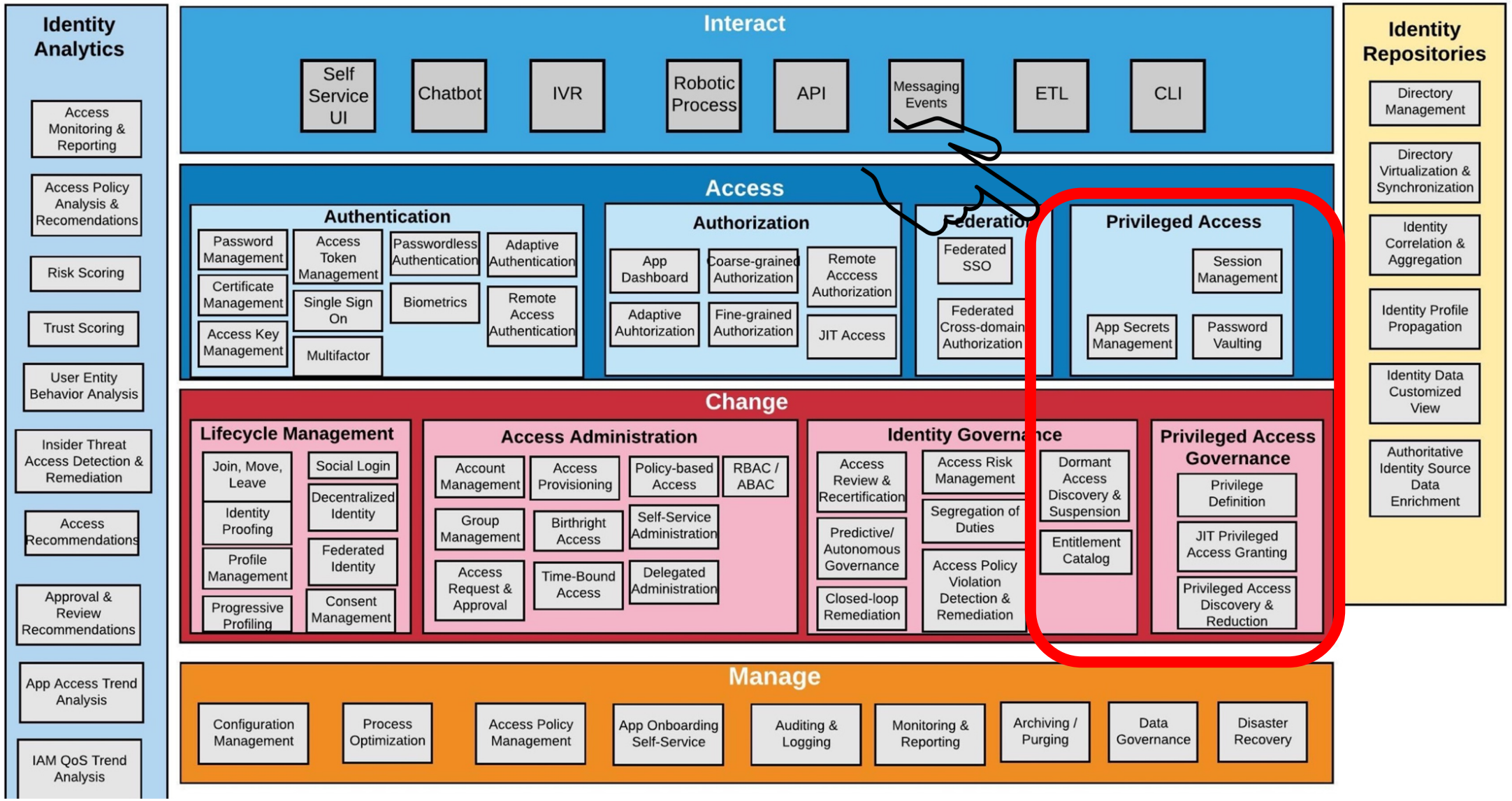
- We continue to get hacked - instead of reaching a place where cyber security can consistently prevent hackers from inserting ransomware, injecting malicious code, stealing sensitive data, etc., we only find ourselves falling further behind.
- With the democratization of traditional IT into an Agile-centric rapid development and deployment model intended to help many businesses stay afloat and meet their customers' ever-increasing demands, the necessary cyber security protections are often ignored or saved for later.
- Why and how do hackers succeed? Broken record: by hijacking privileged access rights in order to drop *their* malicious code in *your* environment.
- To dramatically reduce the attack surface that enables administrative account hijacking, solutions residing under the banner of Privileged Access Management (PAM) have been available for quite a while.

Privileged Access Management Overview

PAM solutions typically address four primary types of privileged access activities:

1. System Administrator Privileged Management (SAPM), which is focused on system administration (SysAdmin), such as Windows Server or Azure Service administration, database administration, etc.
2. Privileged session management (PSM) involves establishing and monitoring sessions to multiple systems. Authenticating users (e.g., using two-factor authentication) and then providing the users access to shared accounts from which all actions will be monitored.
3. Application-to-Application Privileged Management (AAPM) is focused on what are often referred to as ‘service accounts’ associated with application identities and credentials used for system-to-system communications, such as a web application that interacts directly with a backend database.
4. Super User Privileged Management (SUPM) is focused on “root” accounts (e.g., root is the ***superuser*** on Linux systems).

Standard PAM Capabilities



Privileged Access Management Overview

- While PAM and IAM deployments may proceed in parallel, there needs to be an intersection at some point to establish more comprehensive and auditable capabilities reflecting all identities and access rights – whether end users, system or application administrators or application entities.
- The key intersection should occur with Identity Governance and Administration (IGA).
- IGA and PAM are two inter-related technologies because together, they provide one of the most important risk reduction services and enterprise can have.
- This level of management and audit is what IGA enables, in that IGA policies and processes institute a keen level of awareness and monitoring of ‘who has access to what, for what purposes, for how long and under whose authority?’

Privileged Access Management Overview

- Cloud service automation extends application-based PAM functionality across enterprise IaaS infrastructures, which is a major step forward to bringing ‘service account’-type authentication into the highly monitored world of PAM.
- This advancement of special-purpose, cloud-ready vault technology is better suited to enable automation and Agile-method continuous integration/continuous development (CI/CD) use cases while enabling policy to codify, protect, and govern access to secrets.
- The vault can leverage many trusted identity providers, such as cloud IAM platforms, Azure Active Directory, cloud automation platforms such as Kubernetes, and so forth to authenticate into the vault.
- Vaulting allows a service to request secrets for any system through a consistent, audited, and secured workflow.

Privileged Access Management Overview

- Vendors are increasingly describing their offerings in terms of Just in Time (JIT) PAM, which means that system administrators – whether human or application functions, can be assigned privileges in near real time *using their existing, or creating temporary, end-user accounts*.
- JIT PAM limits the duration for which an account possesses elevated privileges and access rights in that the creation and deletion of an appropriate privileged account is assigned only to meet that specific period's mission objectives.
  - The objective is to eliminate the risk surface of having privileged accounts that are "always on".
- In order to make this work, users typically request the access they need via a workflow process – such as ServiceNow or via an existing IAM/IGA workflow process and are quickly granted access or an access privilege level to an application or system.

Panel Discussion

- What are the typical obstacles you may be seeing to successful PAM implementation?
- How do you address the hybrid / multi-cloud infrastructure challenges of privileged account discovery and an increasingly external/extended (B2B) workforce?
- What are one or two of the most significant areas your Product Team is attempting to address, such as JIT PAM?

Questions?

TECHVISION

CHRYSALIS