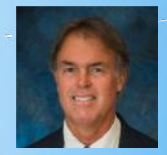
PAY PARTICULAR ATTENTION TO PRIVILEGED USERS—DEVELOPING YOUR PRIVILEGED ACCESS MANAGEMENT (PAM) PROGRAM AND STRATEGY

CHRYSALIS PANEL DISCUSSION

TECHVISION
CHRYSALIS

Featured Speakers



Doug Simmons, TechVision Managing Director, Principal Consulting Analyst. Doug is a pioneer in the IAM space. Led consulting at Burton
for 10 years and security & identity consulting at Gartner for 5 years. Has worked with hundreds of large enterprises. Doug helps companies get IT security, risk management, and IAM right in an accelerating and ever-changing digital landscape.

Andy Smith, Centrify Vice President of Marketing responsible for Centrify's demand generation, brand and go to market strategy. Andy is a veteran of 30 years in the high tech industry and of several security startups. A frequent speaker on technology and security at industry events around the globe.

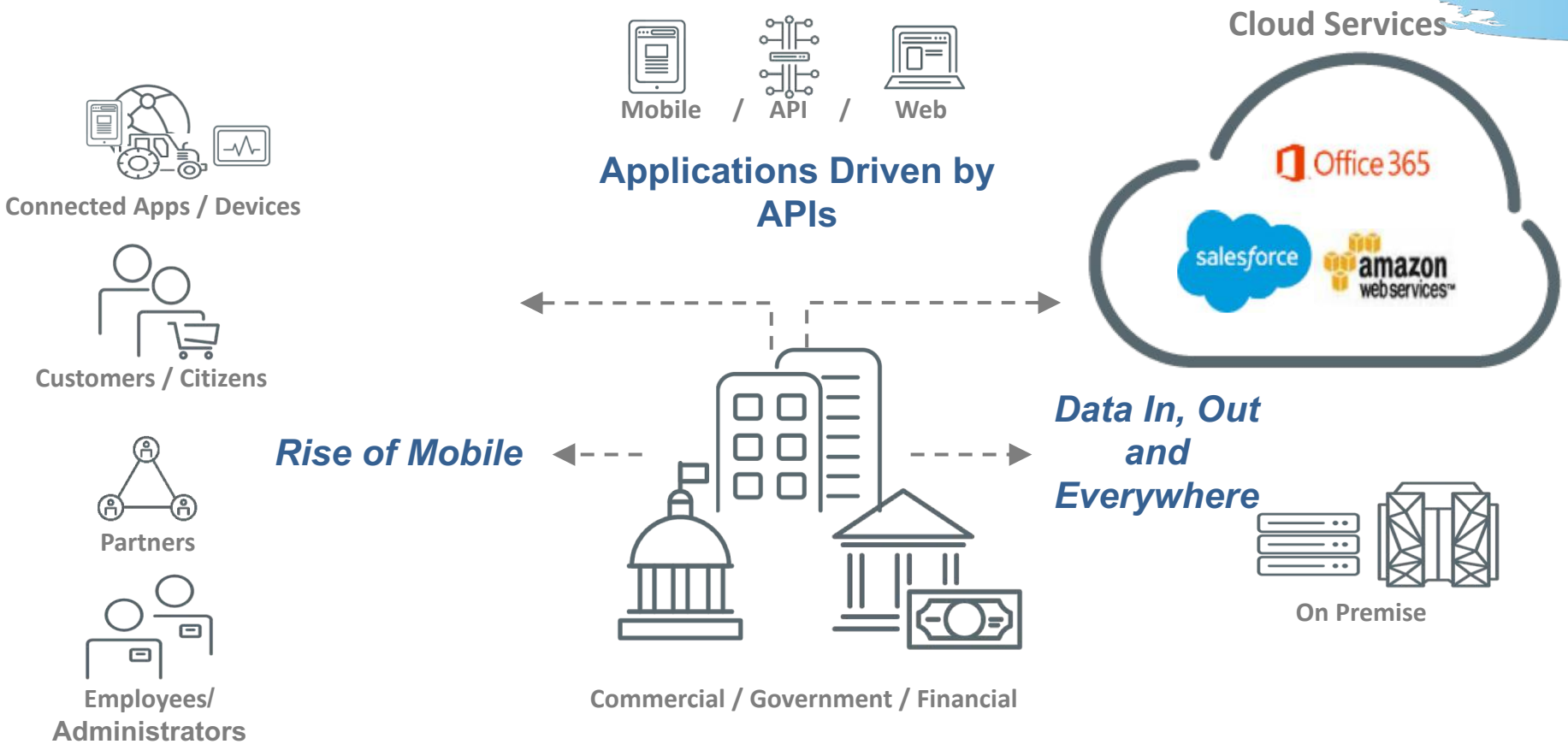
Vibhuti Ranjan Sinha, Saviynt Chief Cloud Officer is the owner of Saviynt's cloud platform and products. Responsible for the strategy and innovation of products to secure various cloud providers, cloud applications and platforms. 16+ years of experience in defining security vision and roadmap, building security solutions, defining IAM strategy and implementing large scale security platforms for Fortune 500.

Christopher Hills, BeyondTrust Deputy Chief Technology Officer and Senior Solutions Architect focused on PAM implementations. With more than 15 yrs. experience as a Sr. Security and Architecture Engineer operating in highly sensitive environments. Prior to joining BeyondTrust he led the Privileged Access Management (PAM) team as Technical Director for a Fortune 500 organization.

Art Poghosyan, Britive Inc. Founder & CEO. Art has spent nearly two decades of his professional career in Information Security. Art co-founded Advancive, a market leading brand for Identity & Access Management (IAM) consulting and solutions implementation
acquired by Optiv. Built Optiv's first managed IAM service offering on PAM. Industry contributor and speaker.

TECHVISION
CHRYSALIS

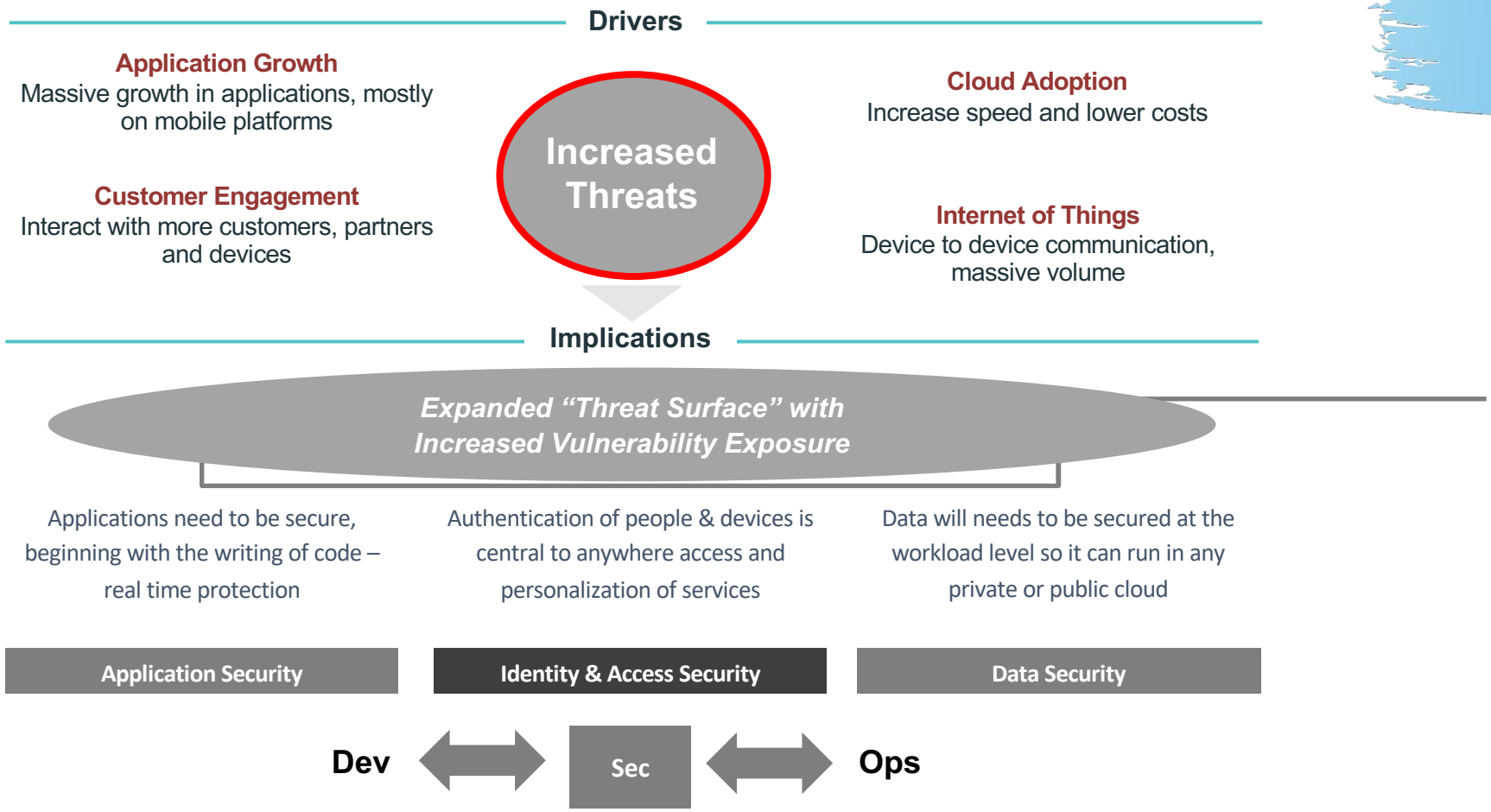
Cloud and Mobility Have Opened Up New Opportunities



…and created a larger threat surface

TECHVISION CHRYSALIS®

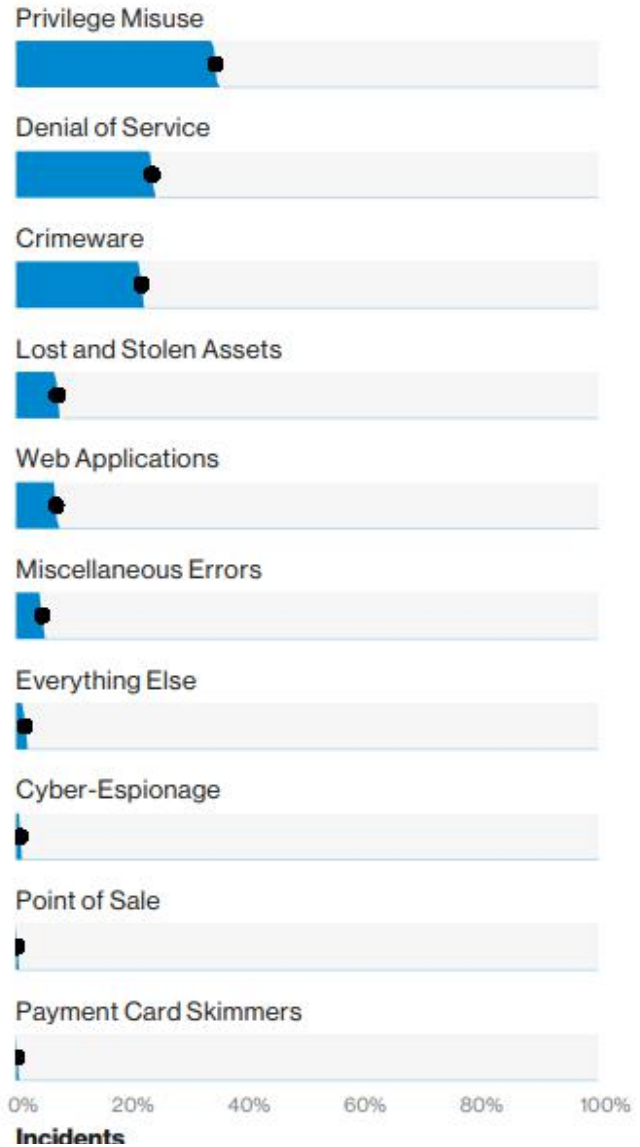
Putting Cybersecurity in Context



DevSecOps: Enable and Secure while not slowing down the development process

TECHVISION
CHRYSALIS®

Trends of Threat Actions



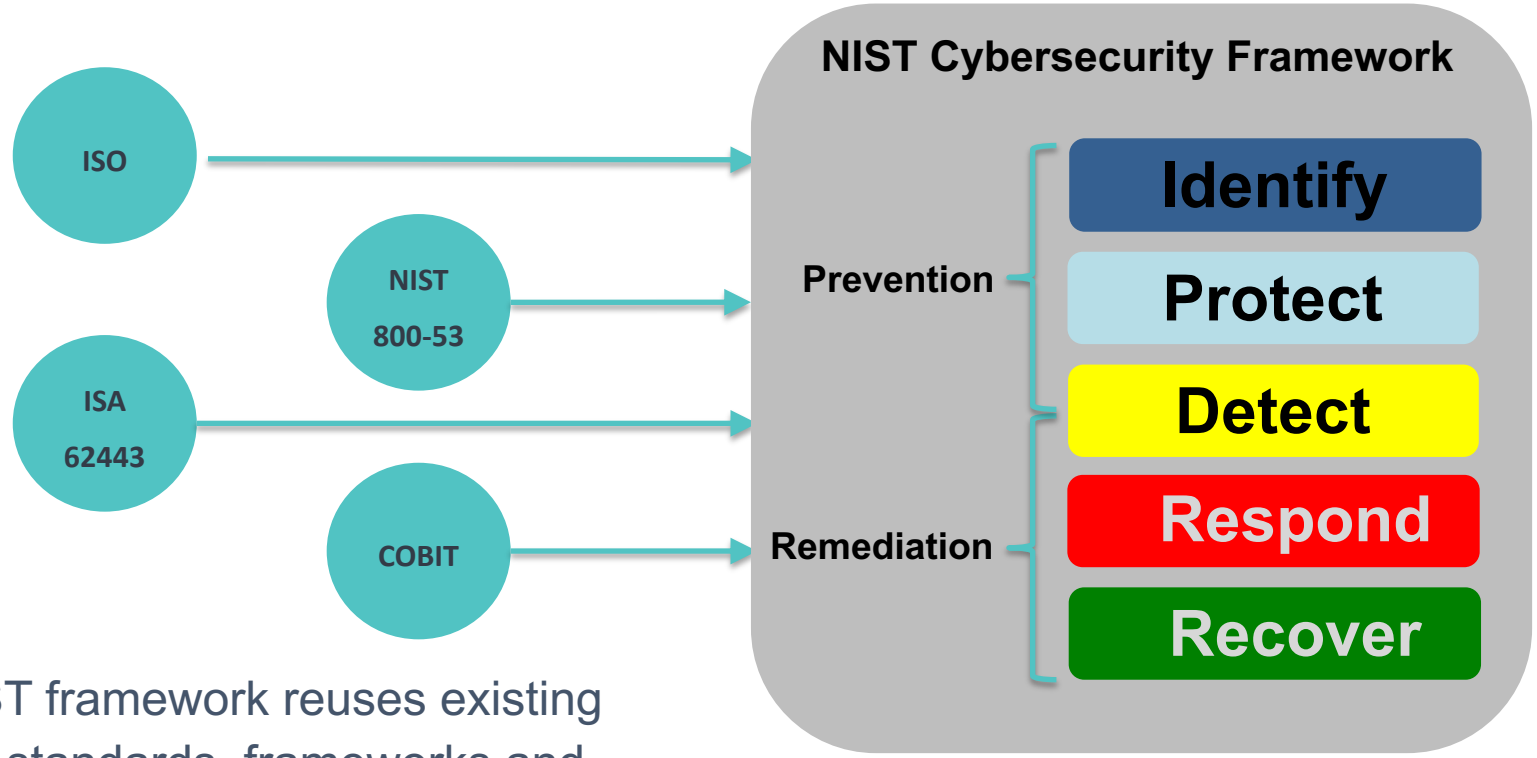
Compromised credentials are still the largest portion of threat actions taken

From Verizon 2019 Data Breach Report

TECHVISION
CHRYSALIS®

How Can We Protect Ourselves?

- An ounce of prevention is worth a pound of cure

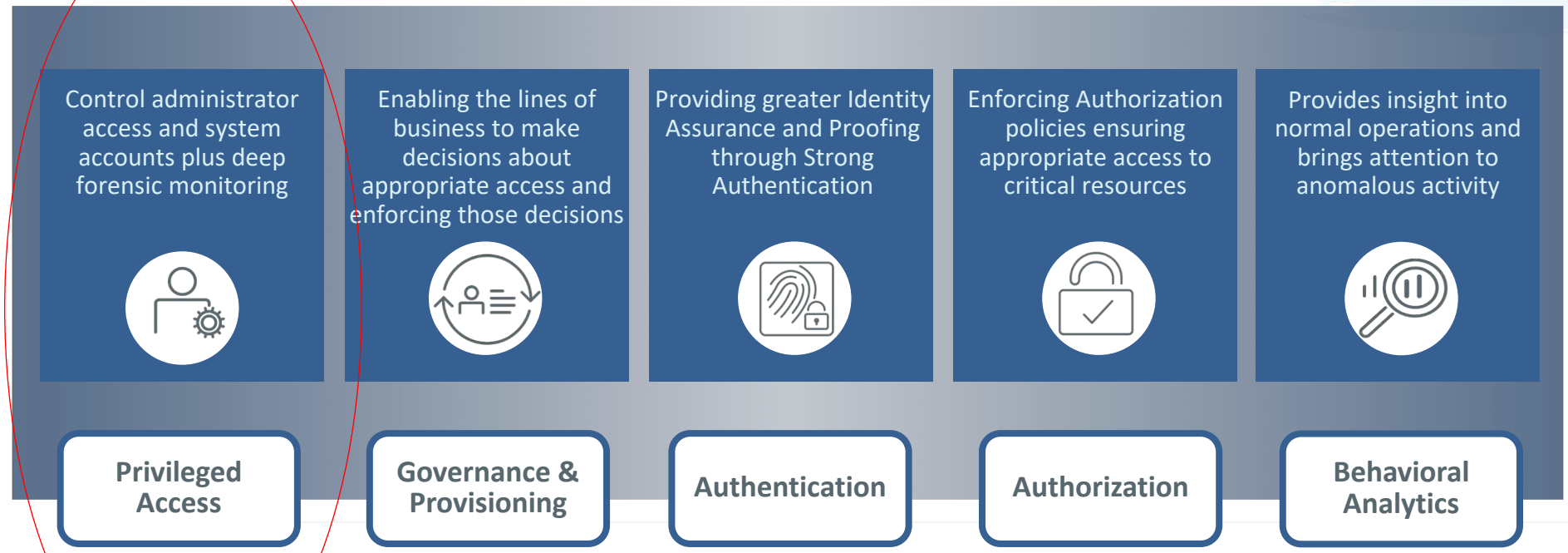


The NIST framework reuses existing security standards, frameworks and guidelines

TECHVISION
CHRYSALIS®

Identity-based Cybersecurity Controls

Facilitating understanding of the relationships and determining the appropriateness of the activities



TECHVISION
CHRYSALIS®

PAM: Required Features

- A secured, hardened and highly available vault for storing credentials and secrets.
- Tools to discover, map and visualize privileged accounts in multiple systems, applications and devices.
- Tools to automatically randomize, rotate and manage credentials for system, administrative, service, database, device and application accounts.
- Tools to manage the end-to-end process of requesting access through UIs by privileged users with approval workflows.
- UIs to check out privileged credentials.
- Supports command filtering to restrict super user capabilities to specific functions.

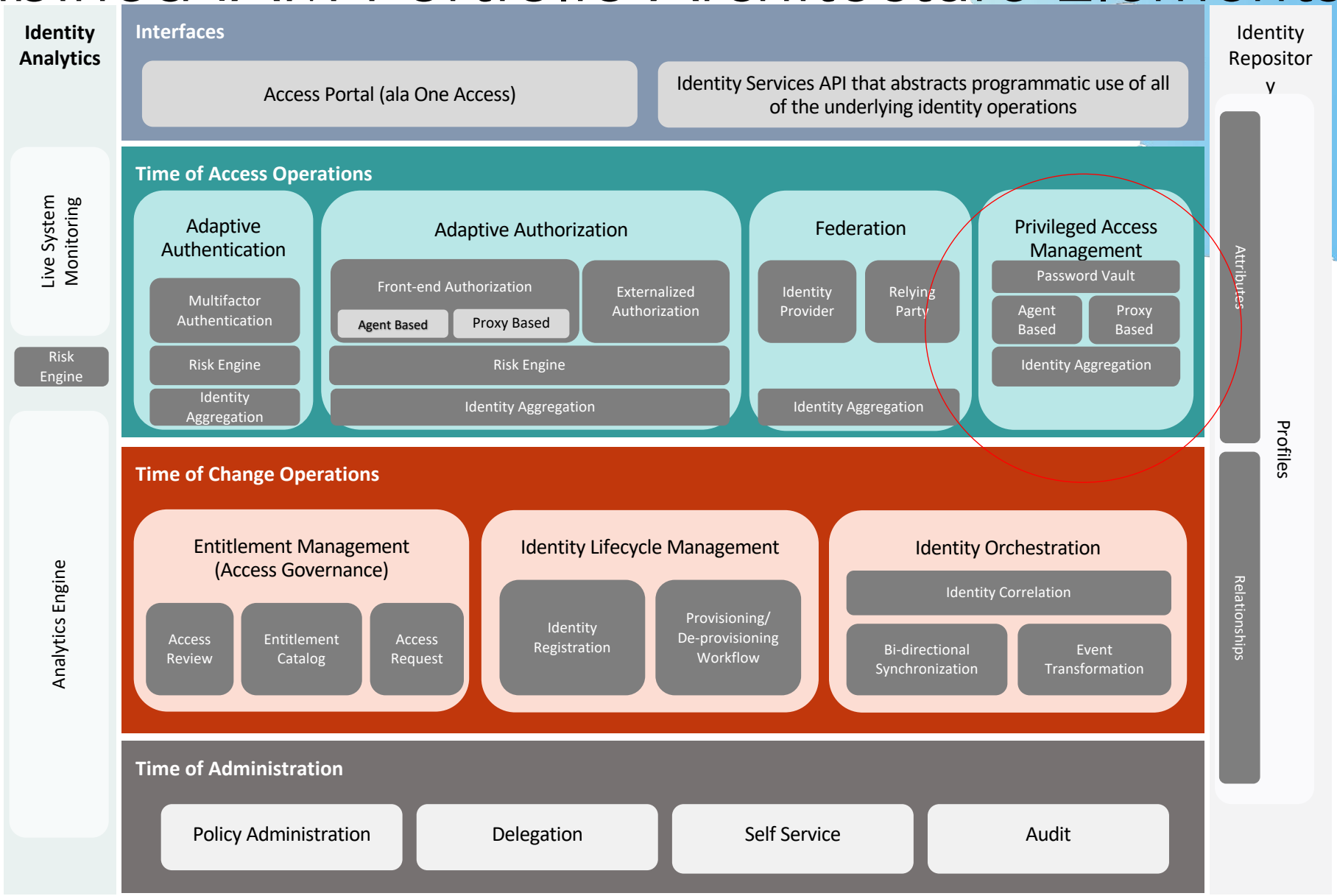
PAM: Required Features

- Tools to allow a privileged session to be automatically established using a protocol such as SSH, RDP or HTTPS without revealing credentials to the user. Features must exist to fully record and review sessions, as well as manage live sessions by allowing them to be accompanied or terminated.
- Tools that broker credentials to applications, thereby allowing the elimination of clear-text credentials in configuration files or scripts.
- Support for role-based administration, including centralized policy management for controlling access to credentials and privileged actions.
- Analytics and reporting on privileged accounts and their use.
- Session recording and audit report services.

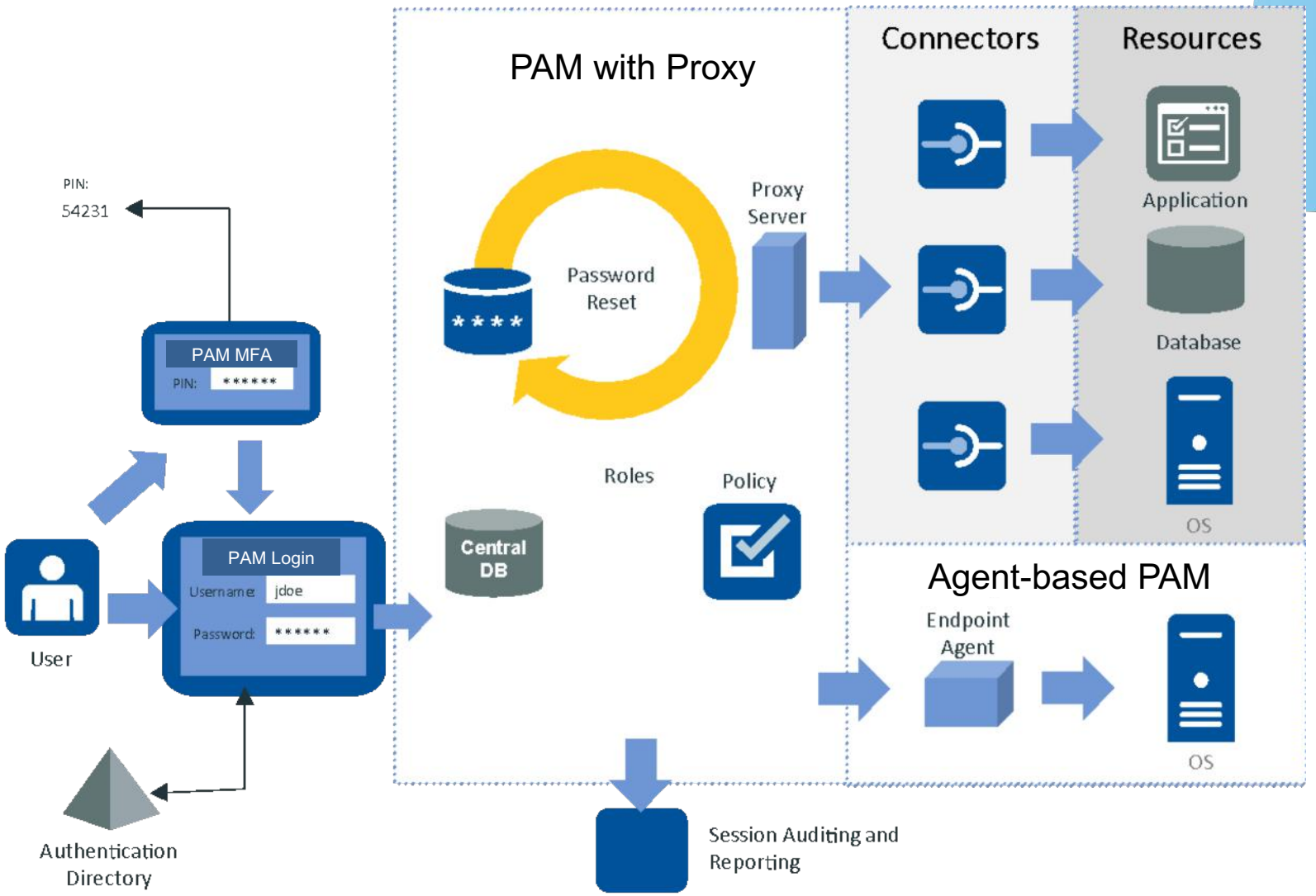
PAM: Required Features

- Cloud integration and support:
  - Autodiscovery of new hosts, VMs and apps
  - Management of administration accounts on:
    - Hypervisor/cloud management platform (CMP)/IaaS
    - Guest OSs
    - Applications
  - Restricting access to the hypervisor/CMP/IaaS management console
  - Multifactor authentication
  - Restrict operations that allow the instantiation, deletion, starting, stopping and copying of VM images and other cloud-delivered services.

Combined IAM Portfolio Architecture Elements

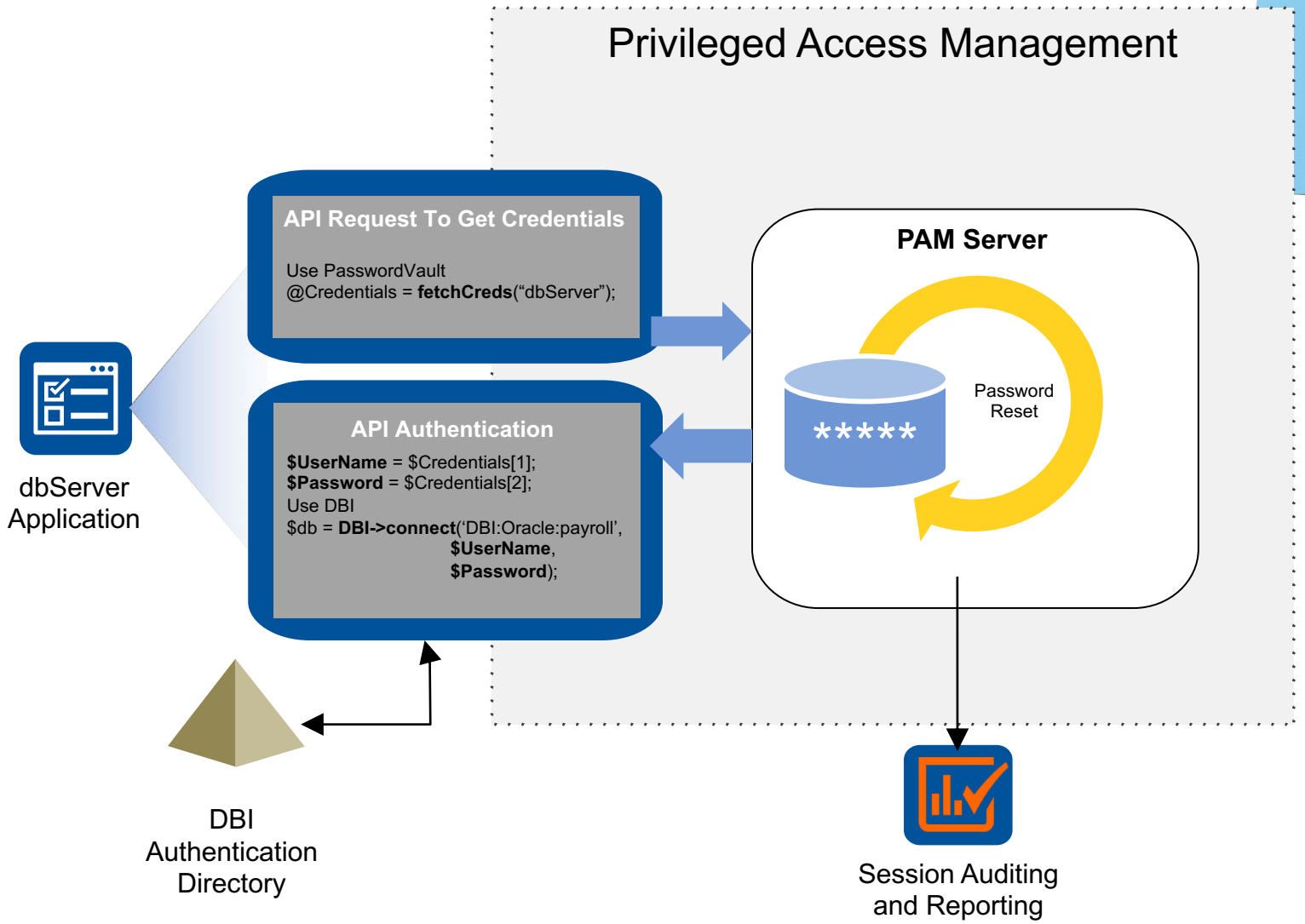


Privileged Access Management



TECHVISION CHRYSALIS®

Programmatic PAM



TECHVISION
CHRYSALIS®

Access Governance

Time of Change Operations

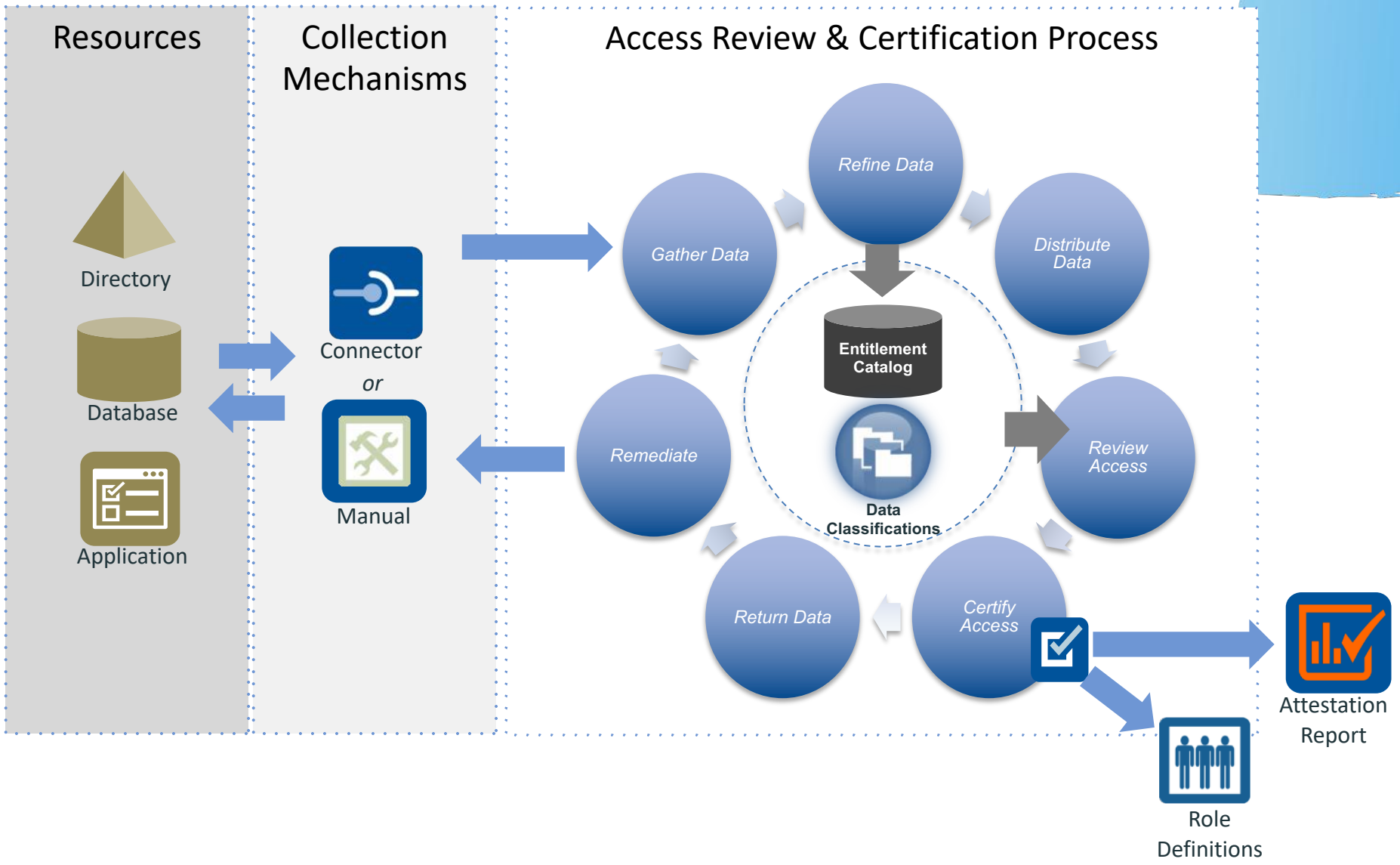
Govern

What does appropriate access look like?

- Provides a mechanism for collecting current entitlement state
- Provides an entitlement catalog for organizing and entitlement definitions and mappings
  - Listing what is assignable
  - Describing what these entitlements actually do
- Facilitates entitlement ownership and accountability
- Provides process for reviewing and certifying entitlement entries
- Provides a self service mechanism for requesting access

TECHVISION
CHRYSALIS®

Access Governance



TECHVISION CHRYSALIS®

Identity / Access Analytics

Inspect

Monitor and analyze,
What can we learn from this?

- Live System Monitoring
  - Collects real time data on user activities and behaviors
- Risk
  - Assesses risk based on collected context and analysis
- Analytics
  - Correlates historical and real time events

TECHVISION CHRYSALIS®

The Future: Just in Time?

- JIT PAM 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 goal is to eliminate the risk surface of having privileged accounts that are "always on".

TECHVISION
CHRYSALIS®

Panel Questions

- Where is the evolution of PAM headed?
  - Do you see critical inhibitors to wider adoption?
  - Are more standards in order to facilitate multi-cloud environments?
  - Do you see PAM and IGA as becoming more inextricably linked?
- Is JIT PAM the wave of the future or can it create administrative issues?

TECHVISION

CHRYSALIS