IDENTITY DAYS
webinars

IdentityDays

Sécurité des identités à l'ère du Cloud et du Zero Trust : Retour d'expérience du groupe Havas

Harouna SOUMARÉ
Solutions Engineer
Harouna.soumare@saviynt.com
+33 6 44 39 20 37

Saviynt

À la tête d'une décennie d'innovation identitaire

2015
INDUSTRY'S 1ST
IGA SaaS Solution

2016
Application Access Governance
1st Identity Security Competency Partner

2018
Cloud Security Analyzer
Gartner IGA MQ Leader

2019
Cloud PAM
1st to achieve FedRAMP authorization

2020
ENTERPRISE IDENTITY CLOUD (EIC)
Multi-tenant platform

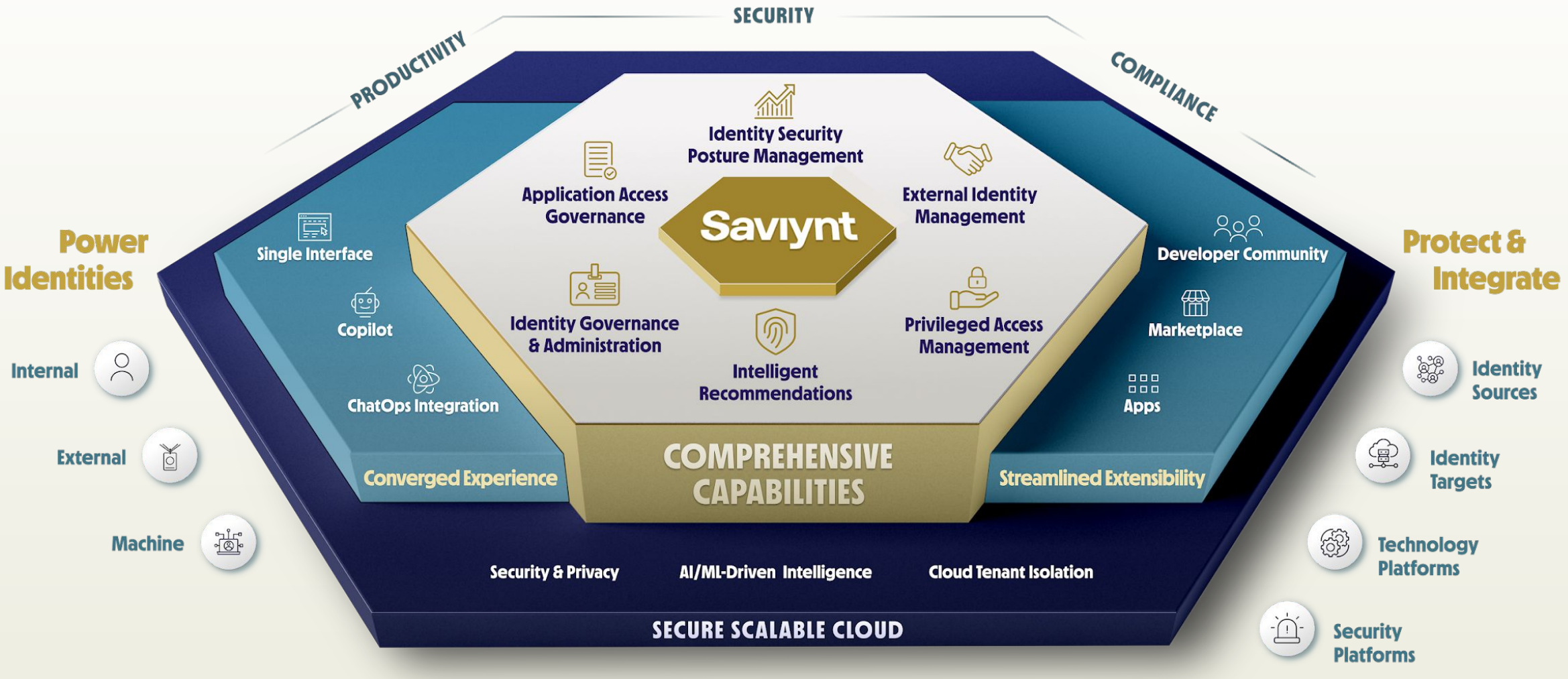
2021
Extended Enterprise Identity Security
Highest Gartner IGA Solution Scorecard Score
KuppingerCole PAM Leadership Compass Leader '21, '22, '23

2022
Advanced Intelligence & Analytics
Only PAM MQ Visionary
IDC Identity Security MarketScape

2023
External Identity Management
Consecutive Customer's Choice Distinction '21, '22 '23

2024
THE IDENTITY CLOUD
Saviynt Intelligence Suite
Machine Identities
Market Guide IGA
Frost & Sullivan FrostRadar™:Leader
KuppingerCole Leadership **Every Category**

THE IDENTITY CLOUD



Intelligence

Saviynt

La vigilance exige une intelligence globale

Prolifération des accès aux identités et accès à risque

L'inefficacité entraîne une augmentation des coûts

L'atténuation des risques relève au mieux de la supposition et reste fortement réactive.

Forte dépendance à l'égard des connaissances techniques pour mettre en œuvre des processus de gouvernance complexes

Les processus de gouvernance ne s'adaptent pas rapidement aux changements organisationnels

Faire les recommandations les plus intelligentes

Prend en compte plus de signaux pour produire les recommandations les plus fiables et les plus précises

Entrées

- **Accès par les pairs**
- **Activité et utilisation**
- **Analyse SoD**
- **14+ signaux de risque internes**
  - Accès hors bande
  - Date de la dernière certification
  - etc...
- **Signaux de risque externe***
  - UEBA
  - Network
  - SIEM
  - etc...

Saviynt

Moteur d'intelligence

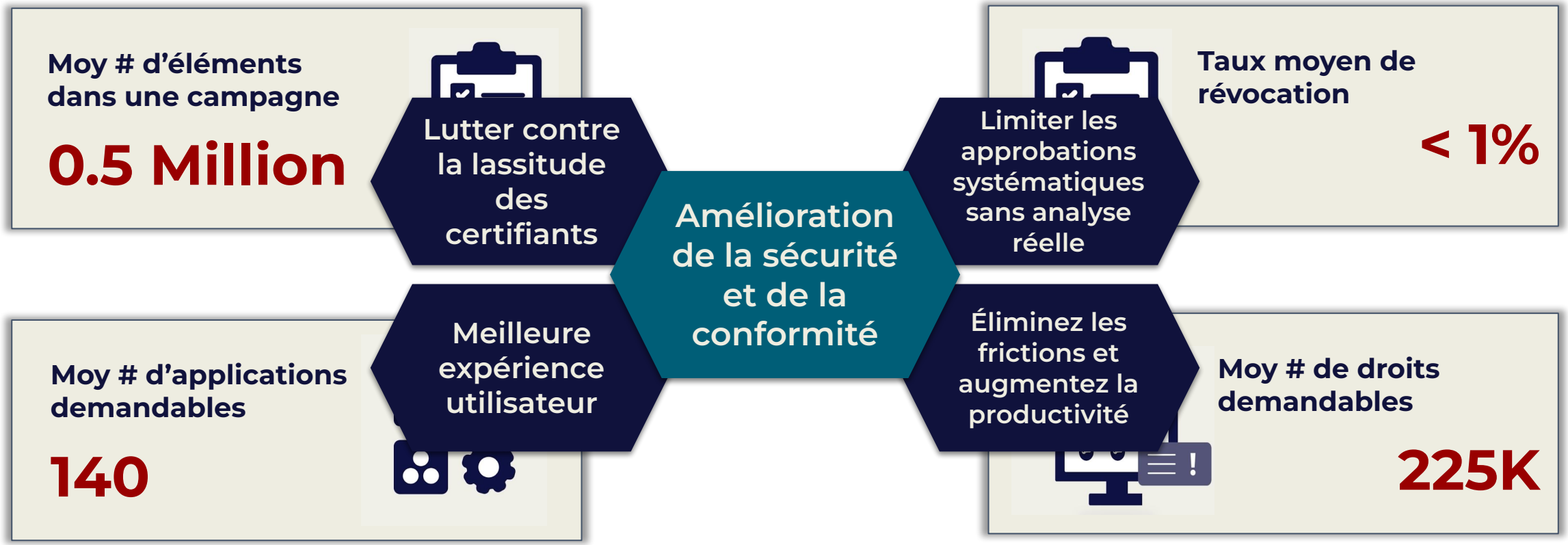
- **Score de confiance**
- **Recommandations d'accès**
- **IA générative**

Sorties

- Requêtes intelligentes
- Certifications intelligentes
- Modélisation d'accès (règles* et rôles)
- Gestion des doublons d'identité

* Roadmap

Augmentation explosive des processus de gouvernance et croissance de l'écosystème applicatif



Exemple d'un client « type » de Saviynt avec + de 20K/20 identités (sur une base annuelle)

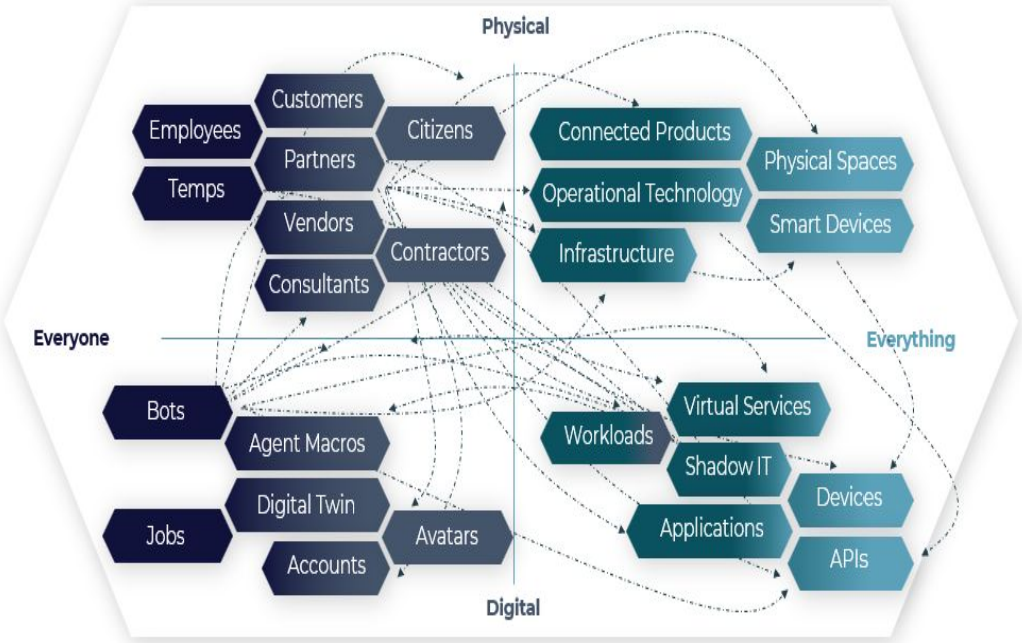
ISPM – Identity Security Posture Management

Saviynt

POURQUOI LES PLATEFORMES D'IDENTITÉ ONT BESOIN DE L'ISPM

Prolifération et accès aux identités

- L'accès surprovisionné augmente le risque pour l'entreprise
  Identités en double



L'inefficacité entraîne une augmentation des coûts

- Missions d'audit coûteuses et chronophages
  Amendes plus élevées en raison de l'échec des audits
  Incapacité à assurer une posture de sécurité correcte

Conjectures et correction réactive de l'exposition à la sécurité

- Valeurs aberrantes manquées avec accès excessif
  Rapports de risque incomplets
  Un travail d'enquête fastidieux et chronophage

Les organisations sont fluides

(Structures organisationnelles et événements J/M/L)

- Accès excessif
  Tâche fastidieuse pour les administrateurs de maintenir des rôles et des politiques précis
  Groupes de pairs obsolètes

L’ISPM

Gain pour pour l'entreprise	**Hygiène des données Observabilité des identités**	**Renforcer la posture de sécurité**	**Accéder à la posture**	**Optimiser les efforts de conformité**	**Préparation à l’audit**
Fonctionnalités Clés	**Tableau de bord ISPM** Classification des identités Source de données Suivre les identités Vues de la chronologie de l’utilisateur Chemin d’accès	**Recommandations** KPI classés en fonction des scores Effectuer des actions basées sur le rapport analytique	**Accéder aux informations** Fournit des informations/mesures de tendance sur les risques de sécurité	**Perspectives sur la gouvernance** Vue détaillée des campagnes Efficacité de la révocation	**Savi AI Copilot** IA conversationnelle conviviale Rapports en libre-service Convertir des rapports en tableaux de bord

JITA – Just In Time Application

Saviynt

Pourquoi pas ma solution actuelle ?

Just-in-Time Access

Avec les Solutions IGA et PAM existantes **Impossible de sécuriser efficacement l'accès aux applications** parce qu'il se situe entre les deux

IGA

Manque de fonctionnalités pour identifier et contrôler efficacement l'accès élevé juste-à-temps des utilisateurs professionnels aux applications

aide les organisations à **combler le fossé** qui existe dans leurs solutions actuelles

PAM

Se concentre principalement sur la sécurisation de l'accès à l'infrastructure ou aux comptes privilégiés, et peut être complexe à mettre en œuvre au niveau de l'application

Saviynt

Présentation de Just-In-Time Access pour les Applications

Visibilité complète

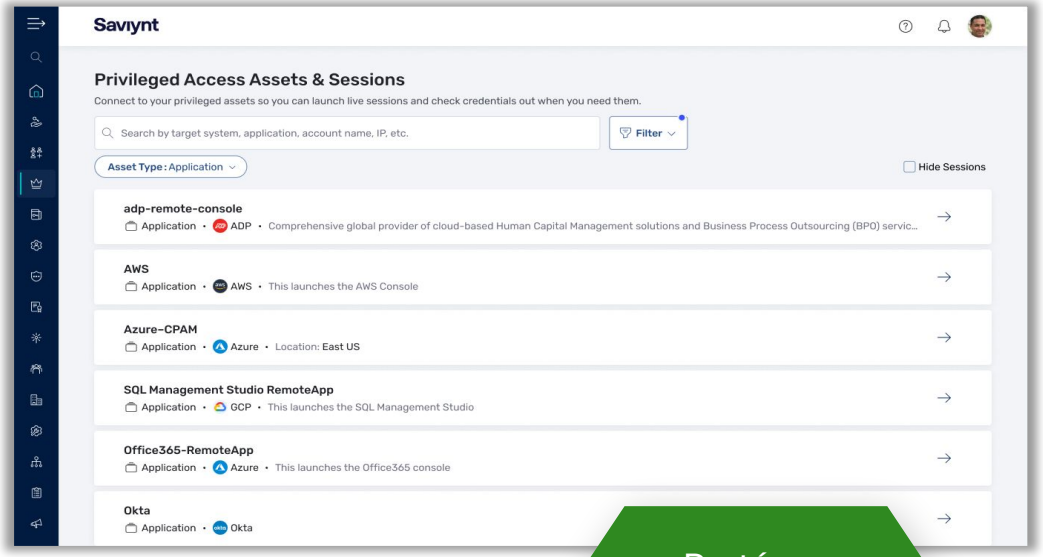
- **Découverte du risque d'accès et du risque de surface d'attaque dans l'ensemble des applications**
  Extraction des informations d'identification d'un compte partagé

Réduire la surface d'attaque

- **Réduire les risques en supprimant les accès permanents et en protégeant les identifiants**

Contrôle transparent de l'application

- **Contrôle d'accès et approbations basés sur des politiques**
  Élévation temporaire des rôles pour les comptes d'utilisateurs individuels



Protégez toutes les applications intégrées

Quelques clics pour activer une fois les applications connectées

Appliquez le Zero Trust et gardez une longueur d'avance sur les menaces

Merci

Harouna SOUMARÉ
Solutions Engineer
Harouna.soumare@saviynt.com
+33 6 44 39 20 37

Saviynt

Identity protects productivity

Identity protects value

Identity Protects growth