Saviynt

IDENTITY DAYS

7ème édition

@IdentityDays
#identitydays2025

21 octobre 2025 - PARIS

IDENTITY DAYS

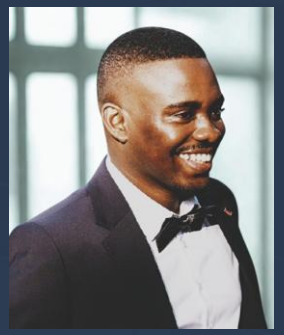
21 octobre 2025 - PARIS

Saviynt

Au-delà de l'IAM : Évaluation continue des risques liés aux identités avec l'ISPM

Harouna SOUMARÉ – Sylvain THOMAS

Sylvain THOMAS
Responsable avant-vente



Harouna SOUMARÉ
Avant-vente technique

AGENDA DE LA CONFÉRENCE

- Introduction
- Les Limites du Modèle IAM/IGA Traditionnel
- Introduction à l'ISPM
- 3 Personas, 3 Défis
  - Le RSSI - De la réactivité à la proactivité
  - L'Admin IT/Sécurité - De l'incident à la maîtrise
  - L'Auditeur - De la frustration à la preuve
- La Plateforme Convergée Saviynt
- Conclusion et Q/R

Introduction

Les attaques évoluent

Comment adapter les protections ?

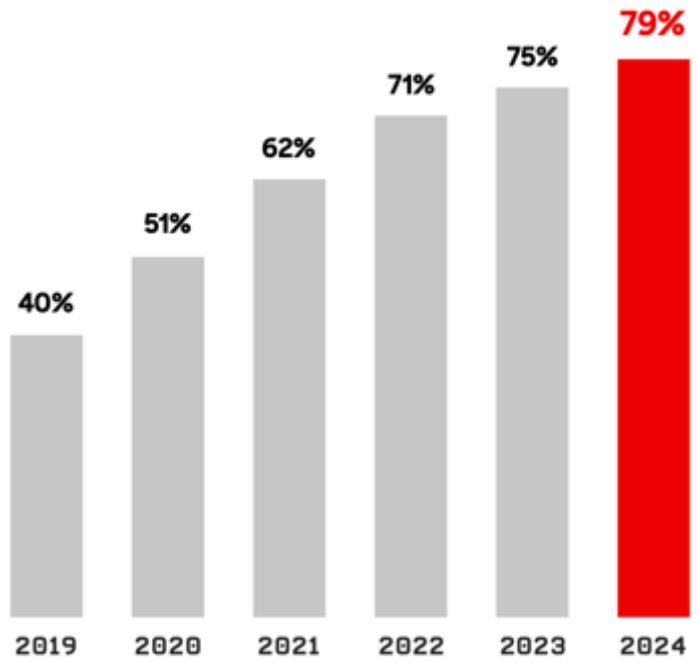
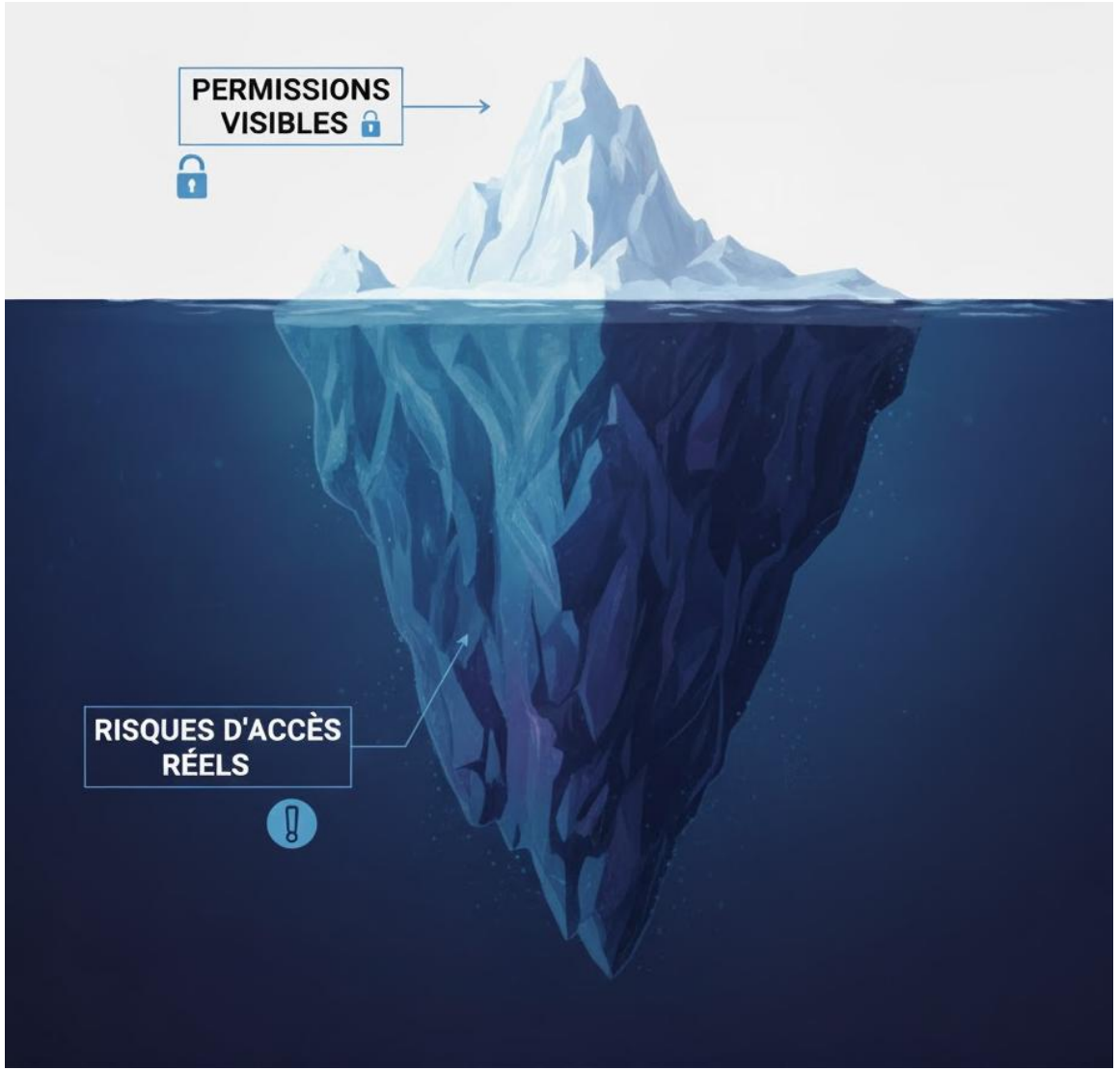


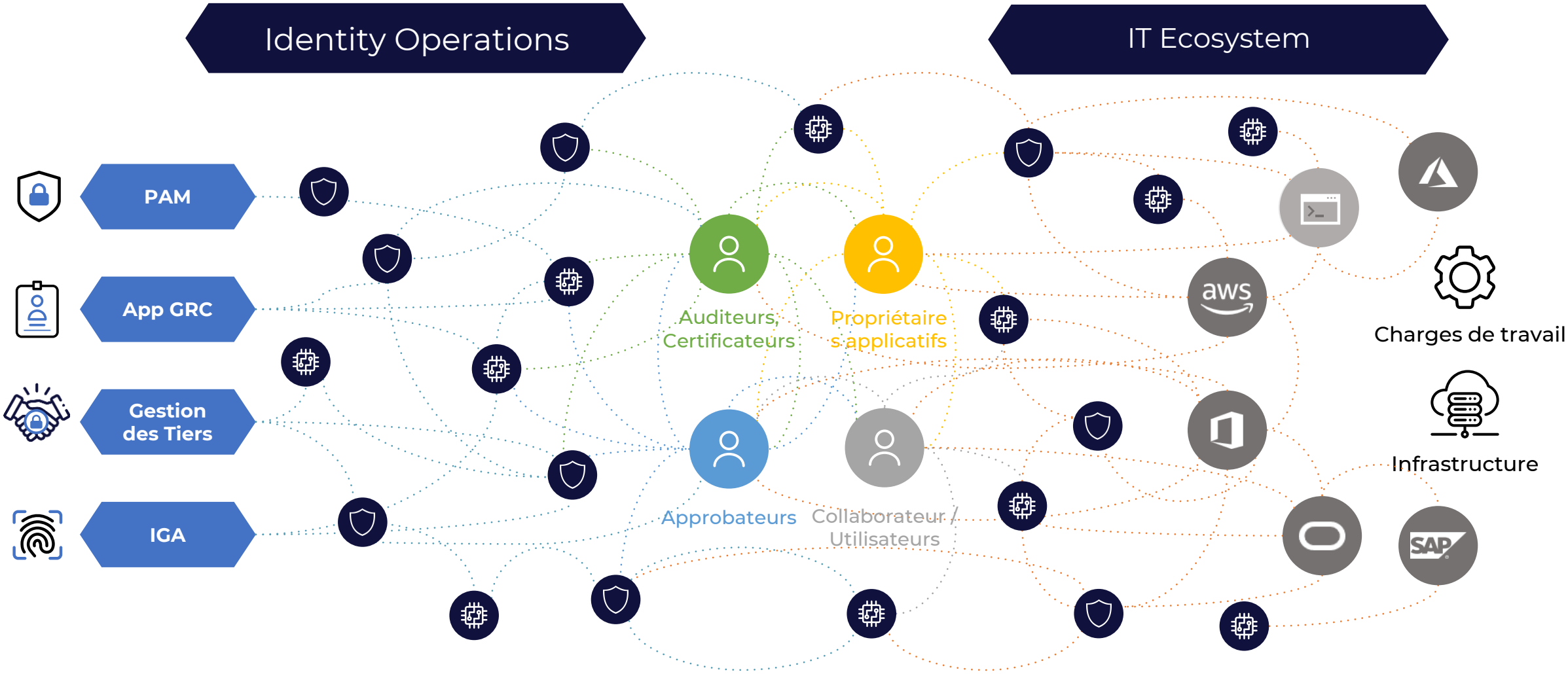
Figure 4. Percentage of detections that were malware-free, 2019-2024

Source: Crowdstrike, Global Threat Report 2025

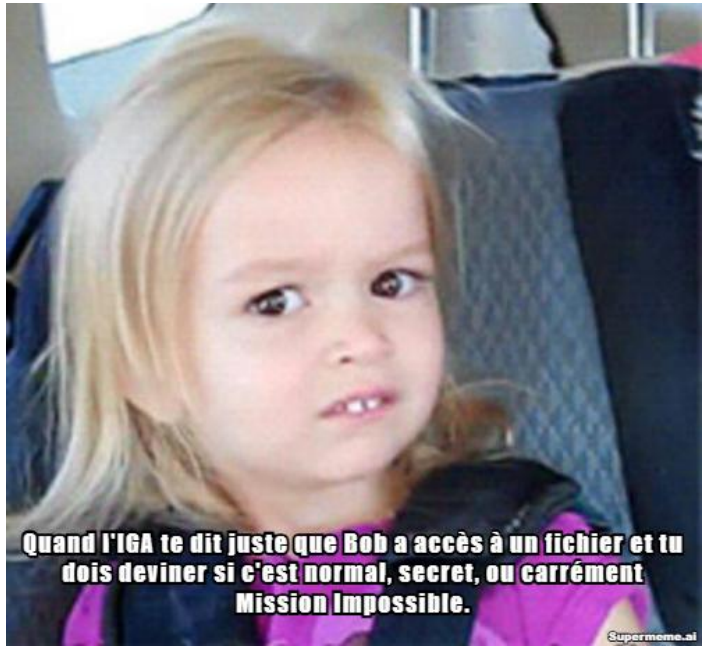


Les Limites du Modèle IAM/IGA Traditionnel

Le monde de l'IAM



Les "angles morts" de l'IGA



Les "angles morts" de l'IGA

Visibilité limitée de la posture de sécurité sur les données, les accès et la gouvernance

Dépendance aux ressources techniques

Des processus en réaction plutôt qu'en anticipation

Mauvaise qualité des données d'identité

Difficulté à mesurer le succès/le retour sur investissement

Introduction à l'ISPM

Les missions de l'ISPM

Identity Security Posture Management

Zéro Trust appliqué aux identités : de la surveillance à l'observabilité

- Découvrir les identités et les accès en temps réel
- Corréler, consolider et analyser
- Prioriser et remédier

3 Personas, 3 Défis

Mise en situation pour 3 personas

RSSI

Vision stratégique
Gestion des risques
Conformité règlementaire

Admin Système

Opérations quotidiennes
Maintenance
Cybersécurité opérationnelle

Auditeur IT

Evaluation indépendante
Contrôle interne
Conformité des processus

Le RSSI – De la réactivité à la proactivité

Les défis du RSSI

De la donnée au risque maitrisé

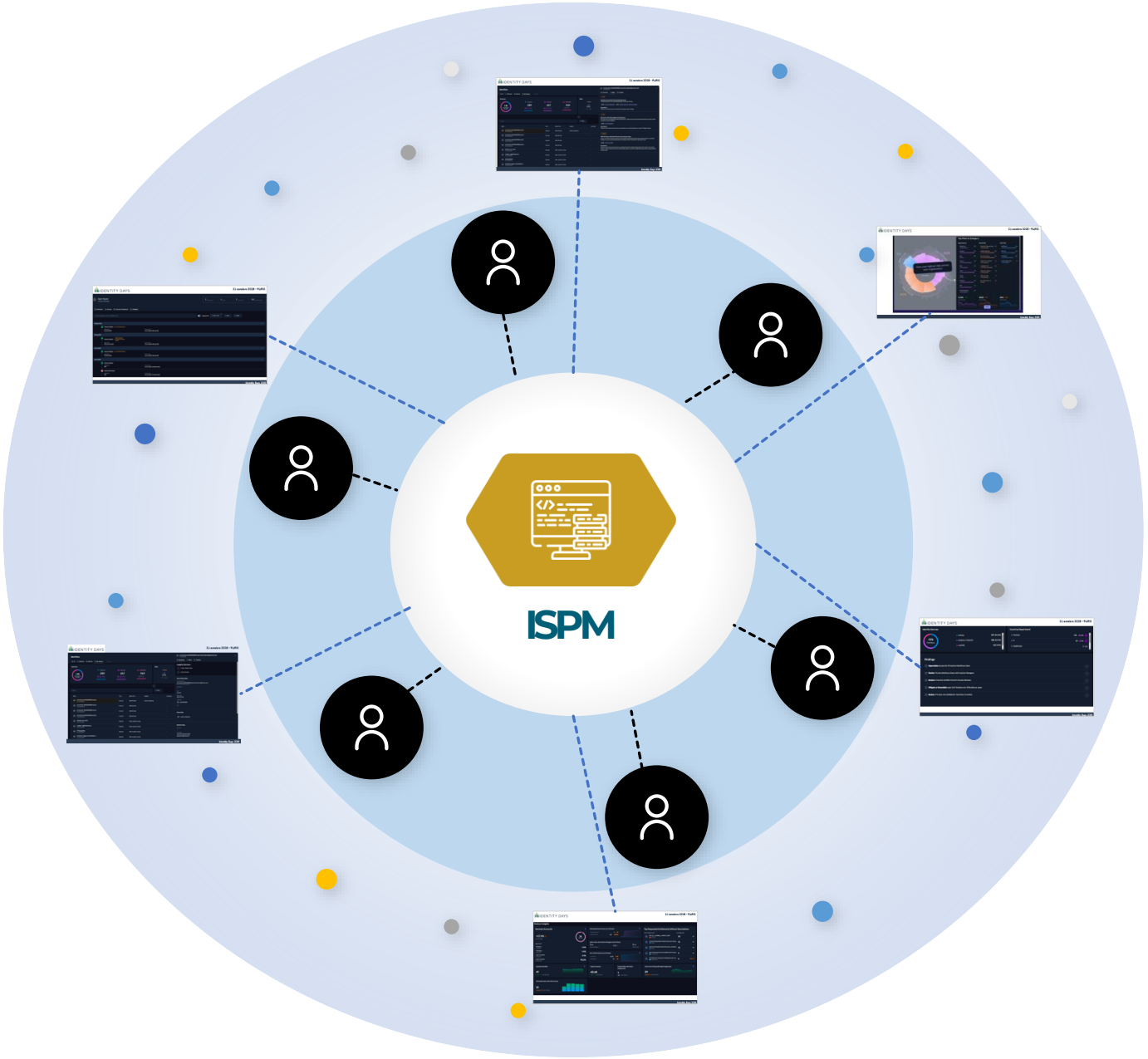
Claire : Ses cauchemars ?
Les signaux faibles :

- un accès anodin,
- un droit oublié,
- un cumul non détecté.

Son quotidien :
Des tableaux de bord d'alertes et des listes d'exceptions interminables.

Son objectif :
Passer de *"j'espère que nous sommes protégés"* à *"je sais où sont mes risques et je les maîtrise."*

Le RSSI – De la réactivité à la proactivité



Identity Sources

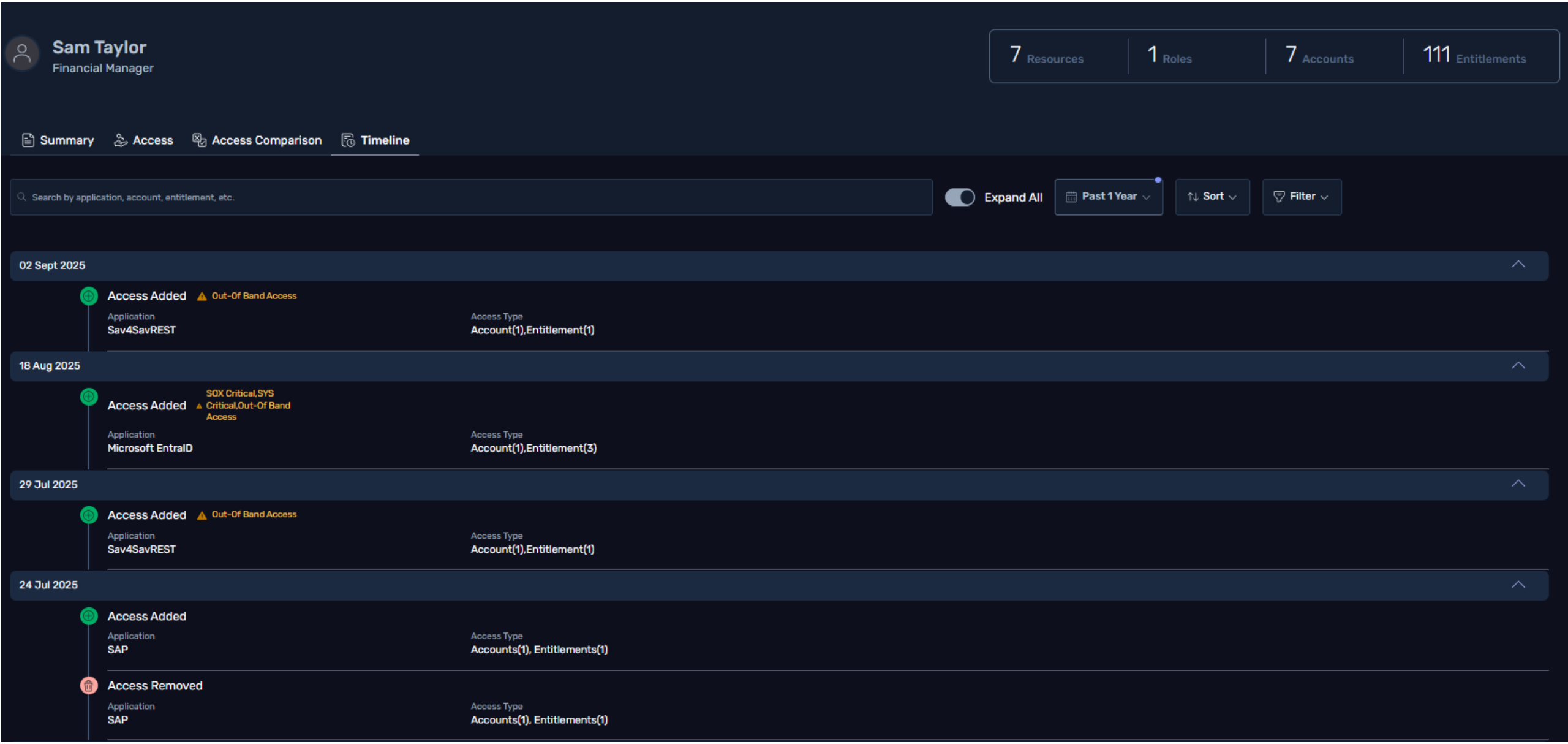
Workday	347 (44.8%)
MANUALLY CREATED	255 (32.9%)
IceHRMS	163 (21%)

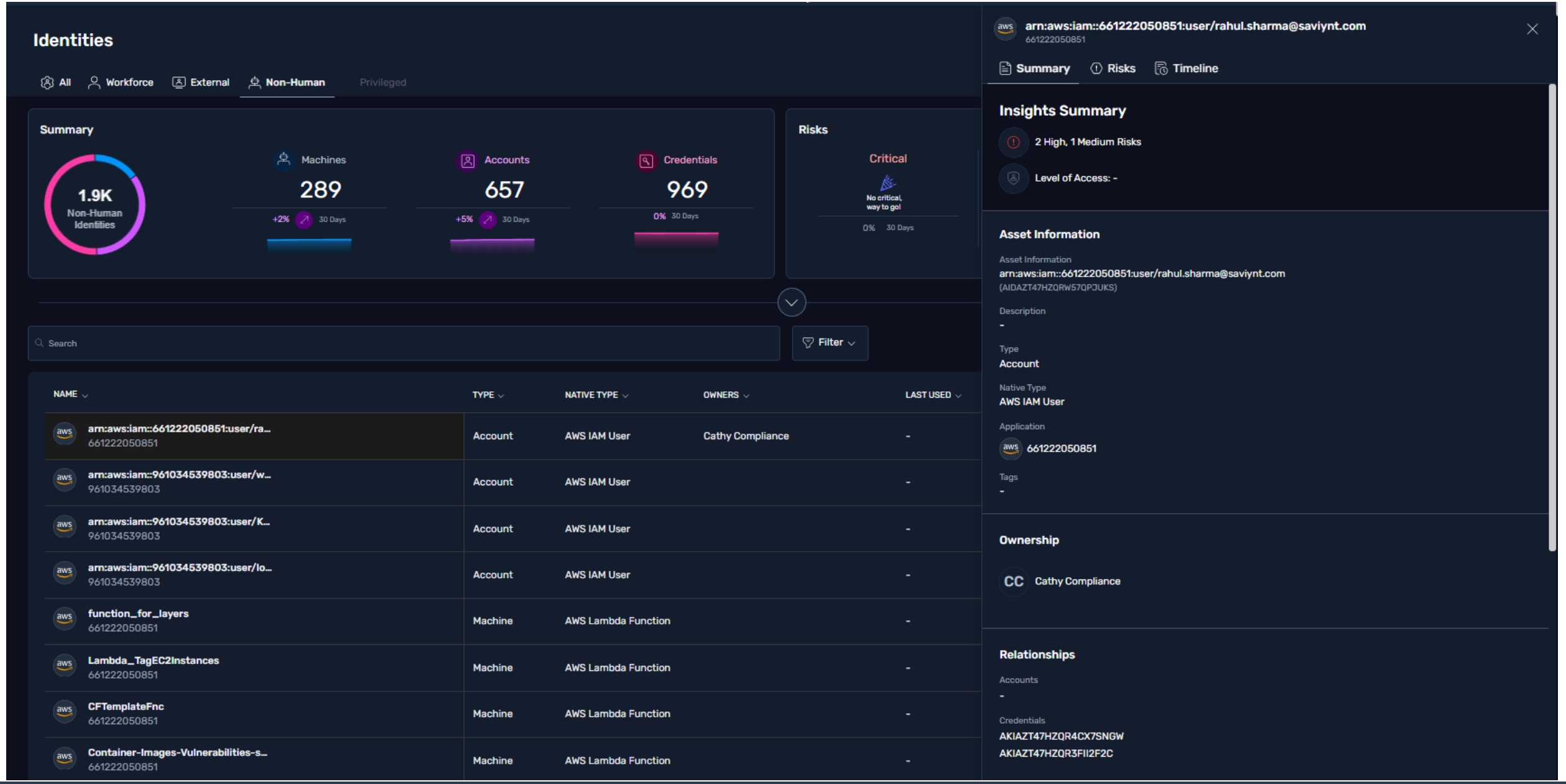
Count by Department

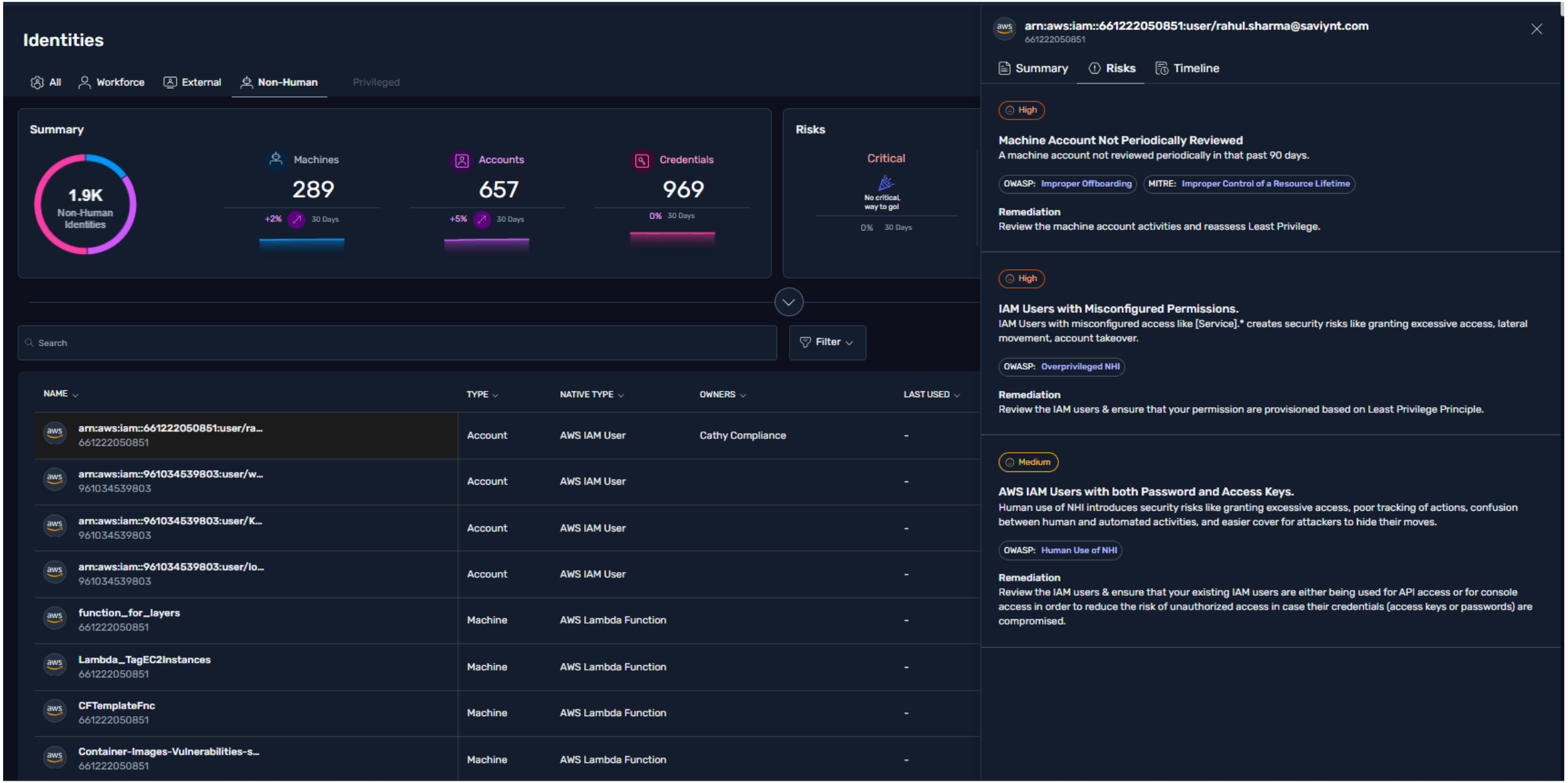
Finance	135	-11.2%
IT	60	+7.1%
Healthcare	6	0%

Findings

- **Deprovision** Access for 31 Inactive Workforce Users
- **Review** 1 Active Workforce Users with Inactive Managers
- **Review** 0 Inactive certifiers found in Access Reviews
- **Mitigate or Remediate** open SoD Violations for 18 Workforce users
- **Review** 771 users not certified for more than 3 months


Sam Taylor
Financial Manager
7 Resources
1 Roles
7 Accounts
111 Entitlements
Summary
Access
Access Comparison
Timeline
Search by application, account, entitlement, etc.
Expand All
Past 1 Year
Sort
Filter
02 Sept 2025
Access Added
Out-Of Band Access
Application
Sav4SavREST
Access Type
Account(1),Entitlement(1)
18 Aug 2025
Access Added
SOX Critical,SYS Critical,Out-Of Band Access
Application
Microsoft EntraID
Access Type
Account(1),Entitlement(3)
29 Jul 2025
Access Added
Out-Of Band Access
Application
Sav4SavREST
Access Type
Account(1),Entitlement(1)
24 Jul 2025
Access Added
Application
SAP
Access Type
Accounts(1), Entitlements(1)
Access Removed
Application
SAP
Access Type
Accounts(1), Entitlements(1)


Identities
All
Workforce
External
Non-Human
Privileged
Summary
1.9K
Non-Human Identities
Machines
289
+2% 30 Days
Accounts
657
+5% 30 Days
Credentials
969
0% 30 Days
Risks
Critical
No critical, way to go!
0% 30 Days
Search
Filter
NAME
TYPE
NATIVE TYPE
OWNERS
LAST USED
arn:aws:iam::661222050851:user/ra...
661222050851
Account
AWS IAM User
Cathy Compliance
-
arn:aws:iam::961034539803:user/w...
961034539803
Account
AWS IAM User
-
arn:aws:iam::961034539803:user/K...
961034539803
Account
AWS IAM User
-
arn:aws:iam::961034539803:user/lo...
961034539803
Account
AWS IAM User
-
function_for_layers
661222050851
Machine
AWS Lambda Function
-
Lambda_TagEC2Instances
661222050851
Machine
AWS Lambda Function
-
CFTemplateFnc
661222050851
Machine
AWS Lambda Function
-
Container-Images-Vulnerabilities-s...
661222050851
Machine
AWS Lambda Function
-
arn:aws:iam::661222050851:user/rahul.sharma@saviynt.com
661222050851
Summary
Risks
Timeline
Insights Summary
2 High, 1 Medium Risks
Level of Access: -
Asset Information
Asset Information
arn:aws:iam::661222050851:user/rahul.sharma@saviynt.com
(AIDAZT47HZQRW57QPJUKS)
Description
-
Type
Account
Native Type
AWS IAM User
Application
661222050851
Tags
-
Ownership
CC
Cathy Compliance
Relationships
Accounts
-
Credentials
AKIAZT47HZQR4CX7SNGW
AKIAZT47HZQR3FII2F2C


Identities
All
Workforce
External
Non-Human
Privileged
Summary
1.9K
Non-Human Identities
Machines
289
+2%
30 Days
Accounts
657
+5%
30 Days
Credentials
969
0%
30 Days
Risks
Critical
No critical, way to go!
0%
30 Days
Search
Filter
NAME
TYPE
NATIVE TYPE
OWNERS
LAST USED
arn:aws:iam::661222050851:user/ra...
661222050851
Account
AWS IAM User
Cathy Compliance
-
arn:aws:iam::961034539803:user/w...
961034539803
Account
AWS IAM User
-
arn:aws:iam::961034539803:user/K...
961034539803
Account
AWS IAM User
-
arn:aws:iam::961034539803:user/lo...
961034539803
Account
AWS IAM User
-
function_for_layers
661222050851
Machine
AWS Lambda Function
-
Lambda_TagEC2Instances
661222050851
Machine
AWS Lambda Function
-
CFTemplateFnc
661222050851
Machine
AWS Lambda Function
-
Container-Images-Vulnerabilities-s...
661222050851
Machine
AWS Lambda Function
-
arn:aws:iam::661222050851:user/rahul.sharma@saviynt.com
661222050851
Summary
Risks
Timeline
High
Machine Account Not Periodically Reviewed
A machine account not reviewed periodically in that past 90 days.
OWASP: Improper Offboarding
MITRE: Improper Control of a Resource Lifetime
Remediation
Review the machine account activities and reassess Least Privilege.
High
IAM Users with Misconfigured Permissions.
IAM Users with misconfigured access like [Service].* creates security risks like granting excessive access, lateral movement, account takeover.
OWASP: Overprivileged NHI
Remediation
Review the IAM users & ensure that your permission are provisioned based on Least Privilege Principle.
Medium
AWS IAM Users with both Password and Access Keys.
Human use of NHI introduces security risks like granting excessive access, poor tracking of actions, confusion between human and automated activities, and easier cover for attackers to hide their moves.
OWASP: Human Use of NHI
Remediation
Review the IAM users & ensure that your existing IAM users are either being used for API access or for console access in order to reduce the risk of unauthorized access in case their credentials (access keys or passwords) are compromised.

Posture Insights

Dormant Accounts

+57.4%
Last 30 days

74
Accounts

INACTIVITY

90 Days + (1 Accounts)	1.4%
120 Days + (1 Accounts)	1.4%
Over 6 months (3 Accounts)	4.1%
Over 9 months (69 Accounts)	93.2%

Standing Elevated Access (Last 30 Days)

Shared Accounts	6	0%
User Accounts	357	+3145.5%

Active Users with Inactive Managers (Last 30 Days)

1 0%
Inactive Mangers

Manage →

1 0%
Active Users

Out-of-Band Access (Last 30 Days)

Accounts	25.2K	+3.3%
Applications	32	-3%

Top Requested Entitlements Without Descriptions

ENTITLEMENT & APP	# OF REQUESTS	
RTR_GL_JOURNAL_IMPORT_RESP (OracleEBS)	22	0%
Accounts Receivable Analyst (Accounts_Rece... (Workday)	13	0%
Accounts Payable Analyst (Accounts_Payable... (Workday)	13	0%
CN=IT-Governance and Compliance,OU=Group... (ActiveDirectory)	9	0%
CN=ADUC,OU=Groups,OU=GlobalDemo,DC=cor... (ActiveDirectory)	6	+20%

Duplicate Identities

41
-2.4% (Last 30 Days)

Orphan Accounts

43.6K
-1% Last 30 days

Inactive Roles with Active Assignments

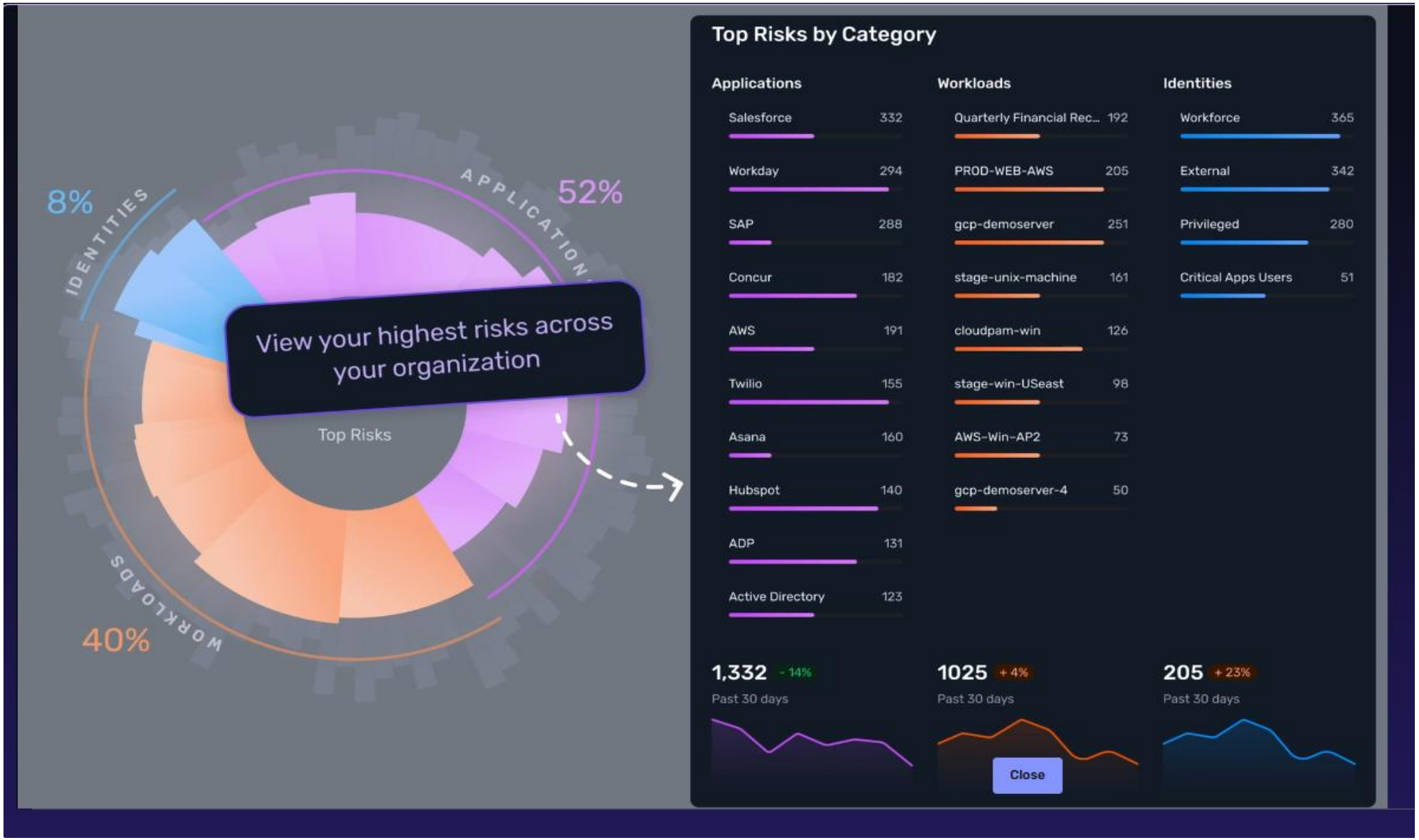
1
0% Last 30 days

Active Users Missing Birthright Assignments

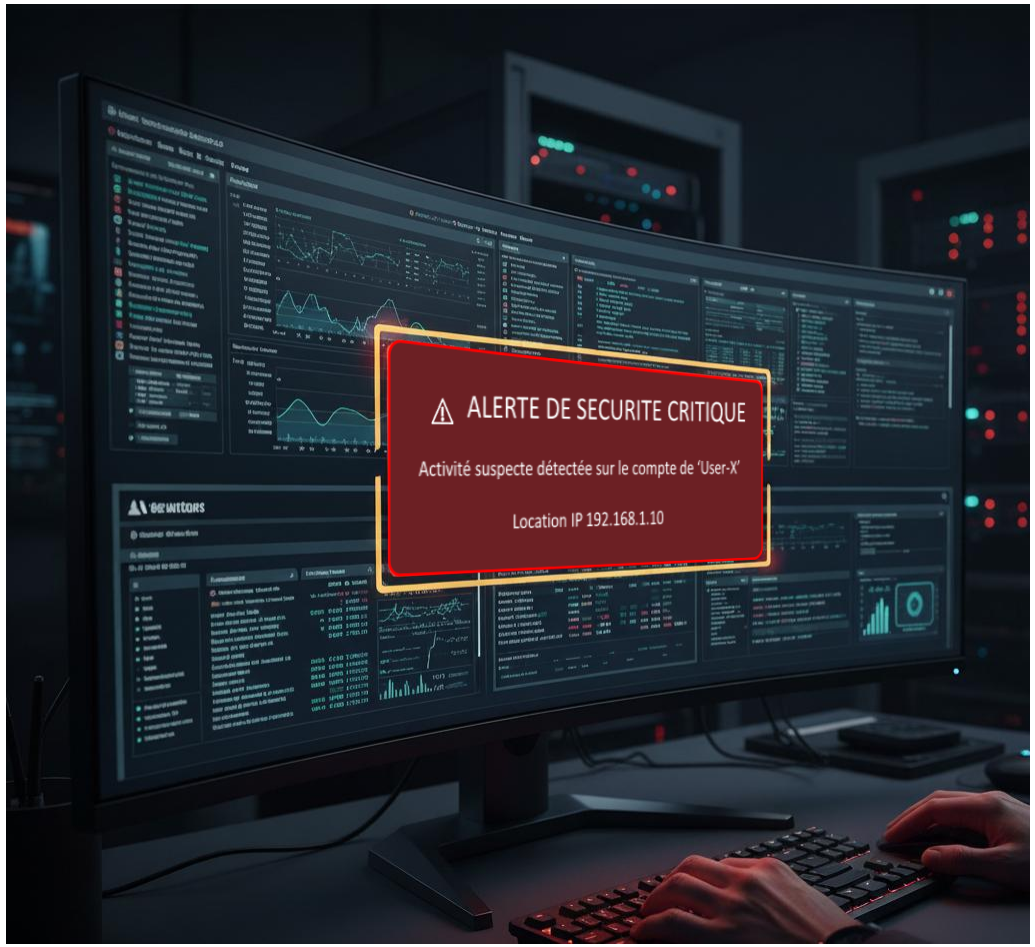
29
+26.1% (Last 30 Days)

Terminated Users with Active Access

31
+47.6% (Last 30 Days)


8%
IDENTITIES
APPLICATIONS
52%
40%
WORKLOADS
View your highest risks across your organization
Top Risks
Top Risks by Category
Applications
Salesforce 332
Workday 294
SAP 288
Concur 182
AWS 191
Twilio 155
Asana 160
Hubspot 140
ADP 131
Active Directory 123
Workloads
Quarterly Financial Rec... 192
PROD-WEB-AWS 205
gcp-demoserver 251
stage-unix-machine 161
cloudpam-win 126
stage-win-USeast 98
AWS-Win-AP2 73
gcp-demoserver-4 50
Identities
Workforce 365
External 342
Privileged 280
Critical Apps Users 51
1,332 - 14%
Past 30 days
1025 + 4%
Past 30 days
205 + 23%
Past 30 days
Close

Admin Sécurité – de l'incident à la maîtrise

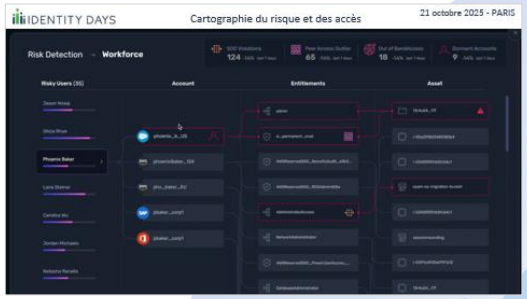


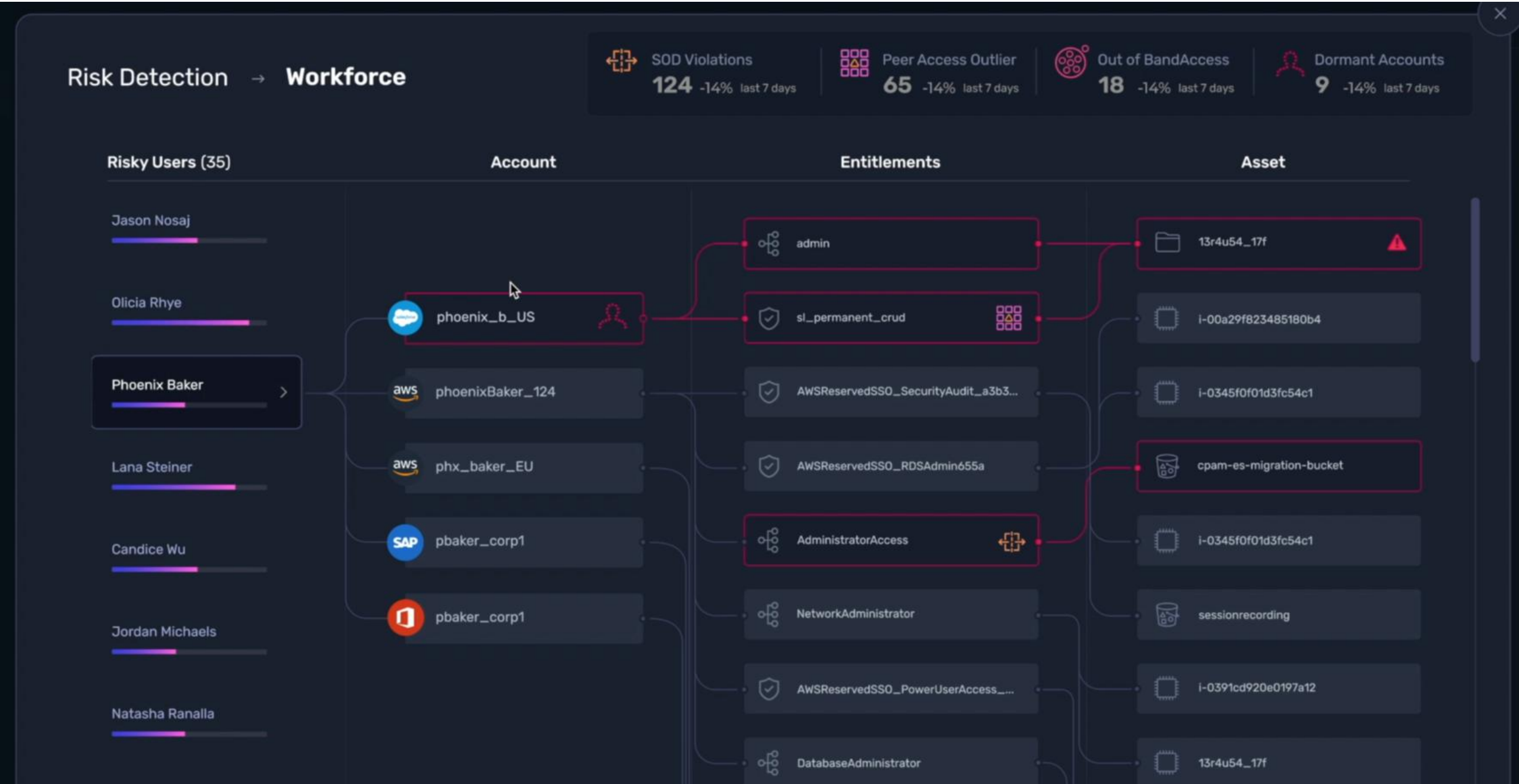
Problématique

- Qui est cet utilisateur ?
- Quel est le périmètre des dégâts potentiels ?
- Est-ce qu'il a des droits d'administration ?
- Quels sont ses droits effectifs sur tous les systèmes / applications ?

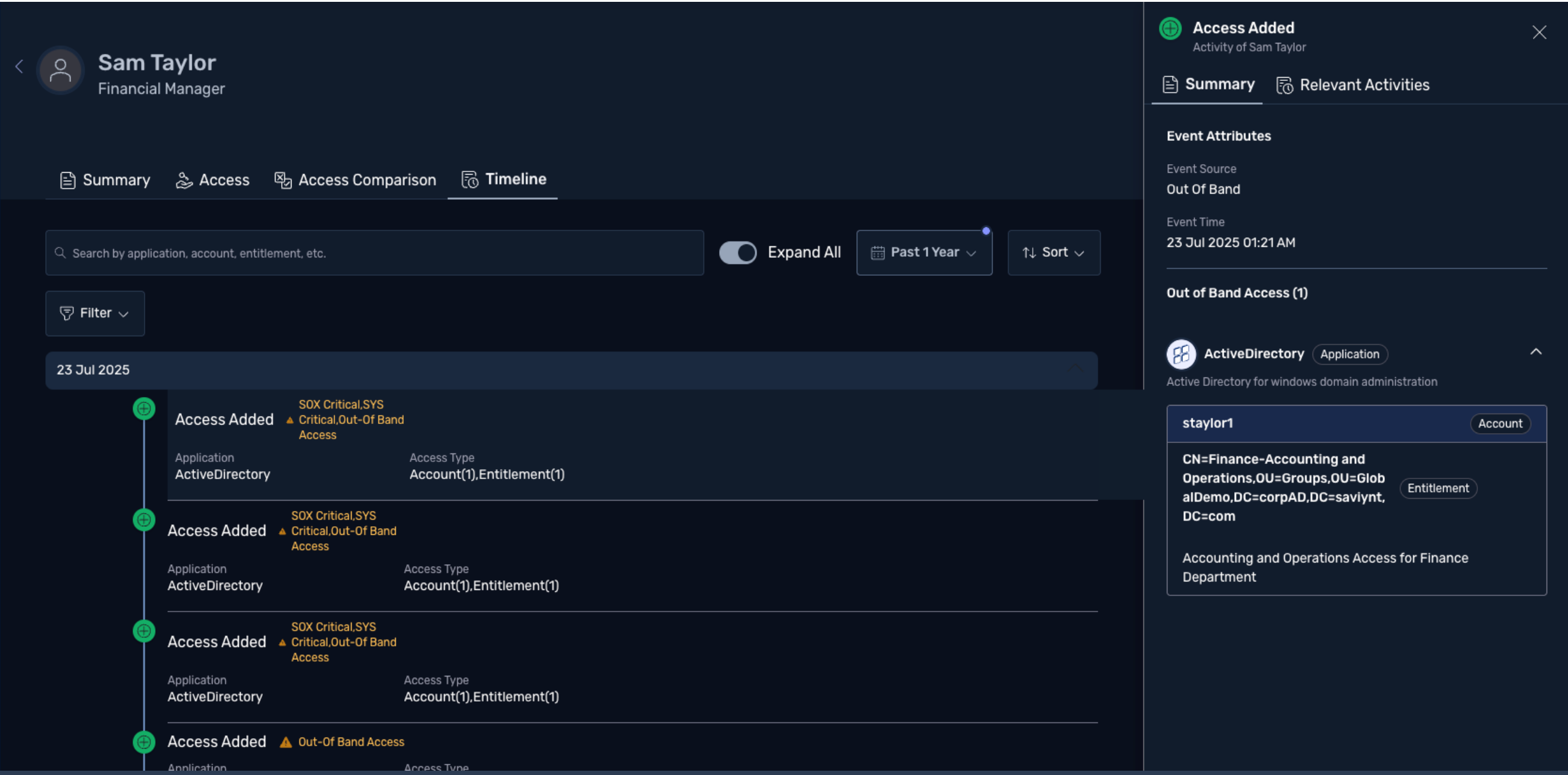
Admin Sécurité

De l’incident à la maîtrise

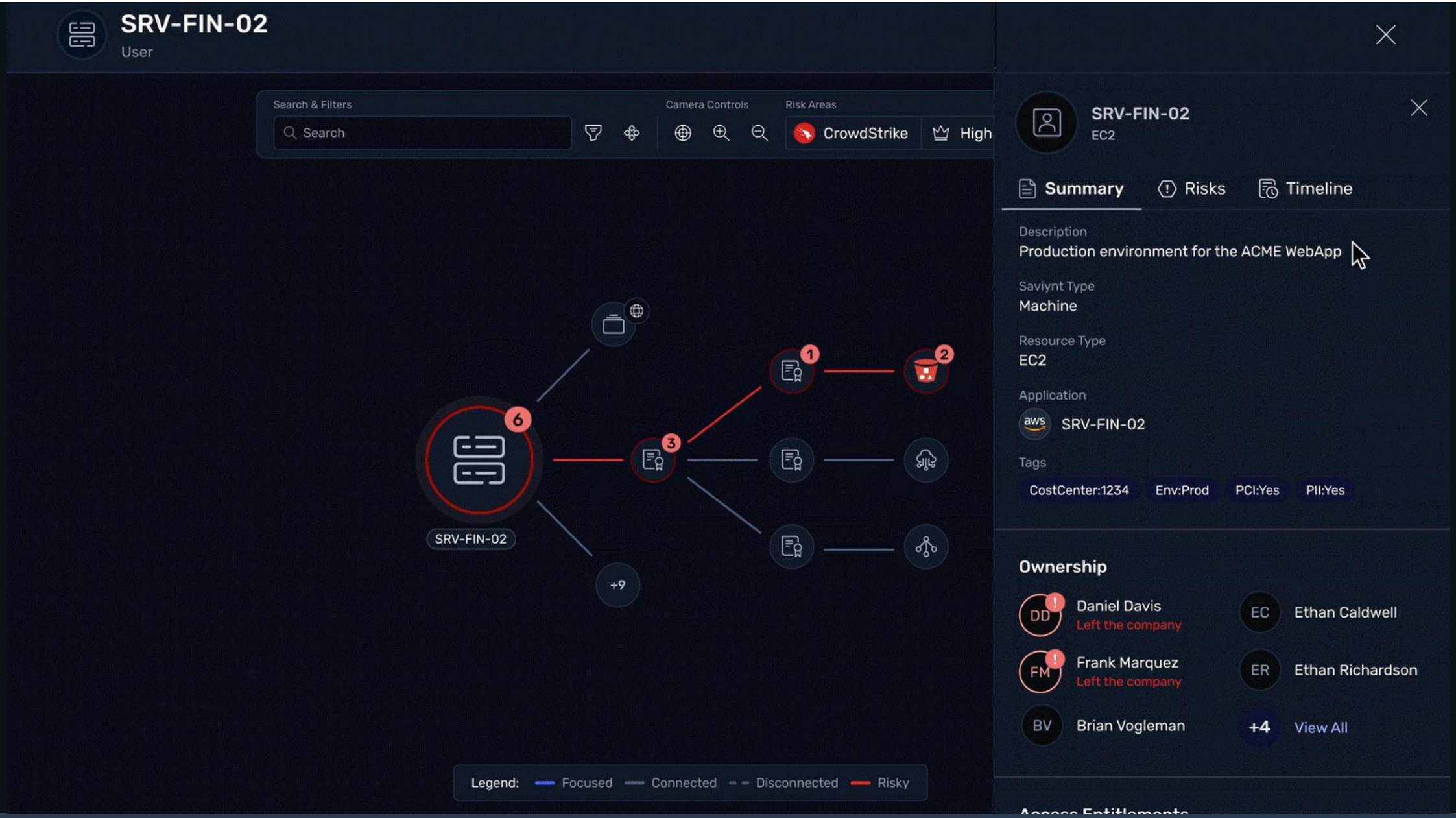



Risk Detection → Workforce
SOD Violations 124 -14% last 7 days
Peer Access Outlier 65 -14% last 7 days
Out of BandAccess 18 -14% last 7 days
Dormant Accounts 9 -14% last 7 days
Risky Users (35)
Account
Entitlements
Asset
Jason Nosaj
Olicia Rhye
Phoenix Baker
Lana Steiner
Candice Wu
Jordan Michaels
Natasha Ranalla
phoenix_b_US
phoenixBaker_124
phx_baker_EU
pbaker_corp1
pbaker_corp1
admin
sl_permanent_crud
AWSReservedSSO_SecurityAudit_a3b3...
AWSReservedSSO_RDSAdmin655a
AdministratorAccess
NetworkAdministrator
AWSReservedSSO_PowerUserAccess_...
DatabaseAdministrator
13r4u54_17f
i-00a29f823485180b4
i-0345f0f01d3fc54c1
cpam-es-migration-bucket
i-0345f0f01d3fc54c1
sessionrecording
i-0391cd920e0197a12
13r4u54_17f

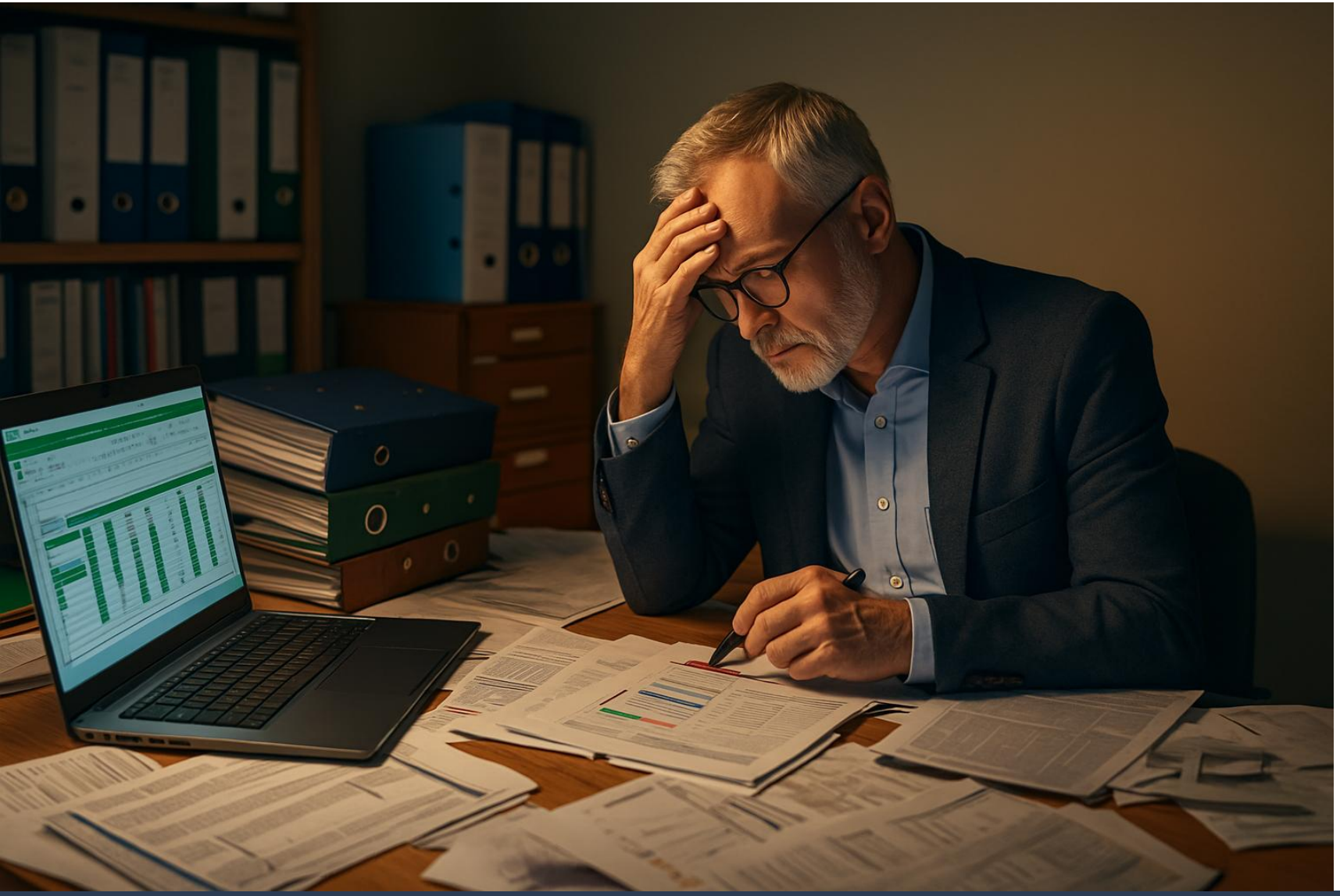
Historique des accès



Intégration avec des outils externes



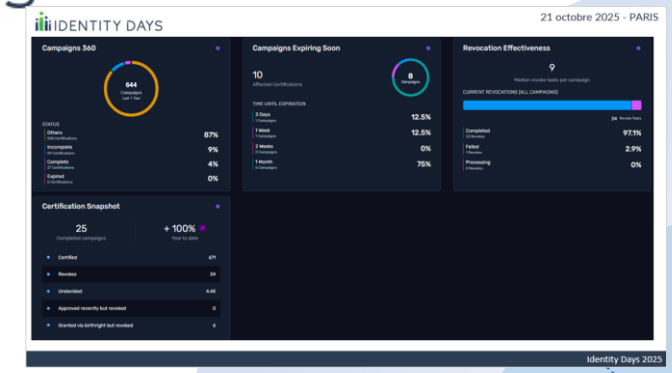
L'Auditeur - De la frustration à la preuve

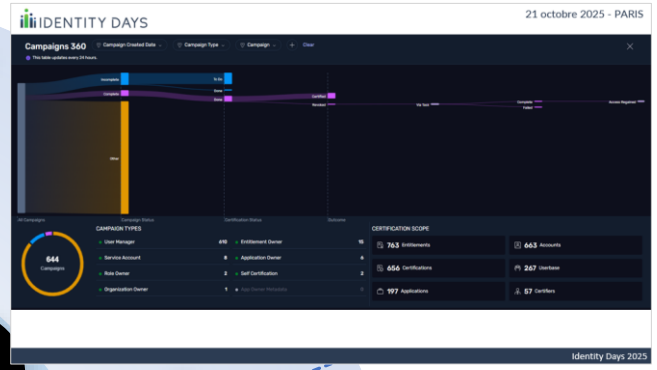


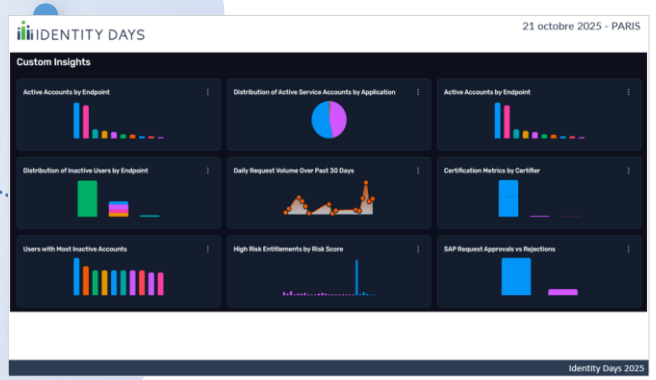
Le défi de l’Auditeur

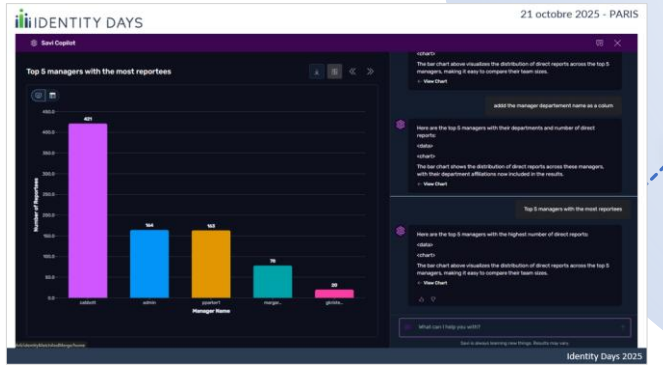
Des preuves manuelles, dispersées et incomplètes

L'Auditeur - De la frustration à la preuve









Campaigns 360

STATUS

Others 558 Certifications	87%
Incomplete 59 Certifications	9%
Complete 27 Certifications	4%
Expired 0 Certifications	0%

Campaigns Expiring Soon

10
Affected Certifications

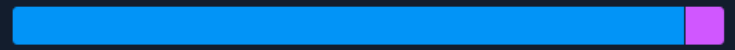
TIME UNTIL EXPIRATION

3 Days 1 Campaigns	12.5%
1 Week 1 Campaigns	12.5%
2 Weeks 0 Campaigns	0%
1 Month 6 Campaigns	75%

Revocation Effectiveness

9
Median revoke tasks per campaign

CURRENT REVOCATIONS (ALL CAMPAIGNS)



34 Revoke Tasks

Completed 33 Revokes	97.1%
Failed 1 Revokes	2.9%
Processing 0 Revokes	0%

Certification Snapshot

25
Completed campaigns

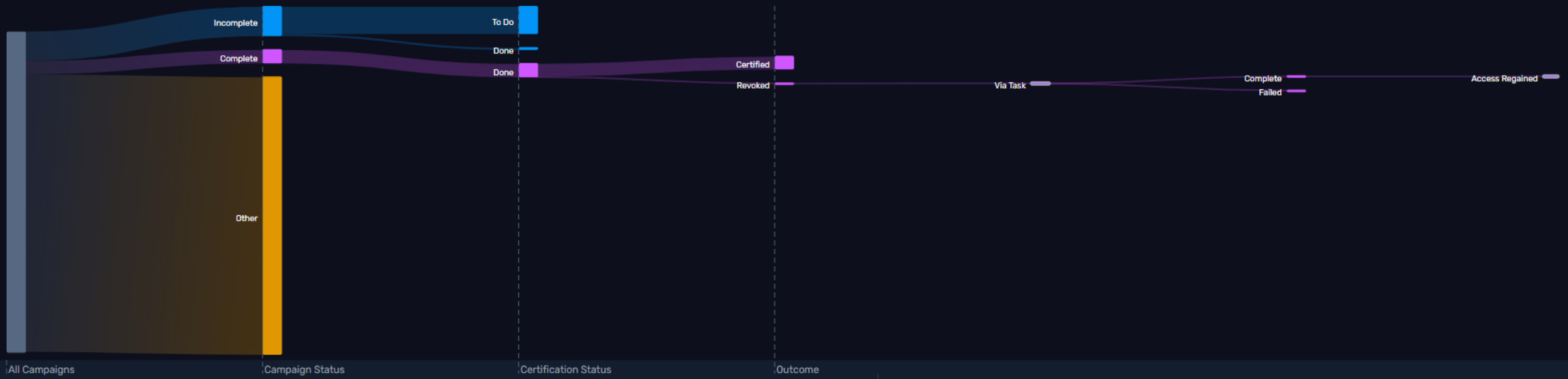
+ 100%
Year to date

Certified	671
Revokes	34
Undecided	4.4K
Approved recently but revoked	0
Granted via birthright but revoked	6

Campaigns 360

Campaign Created Date | Campaign Type | Campaign | Clear

This table updates every 24 hours.



CAMPAIGN TYPES

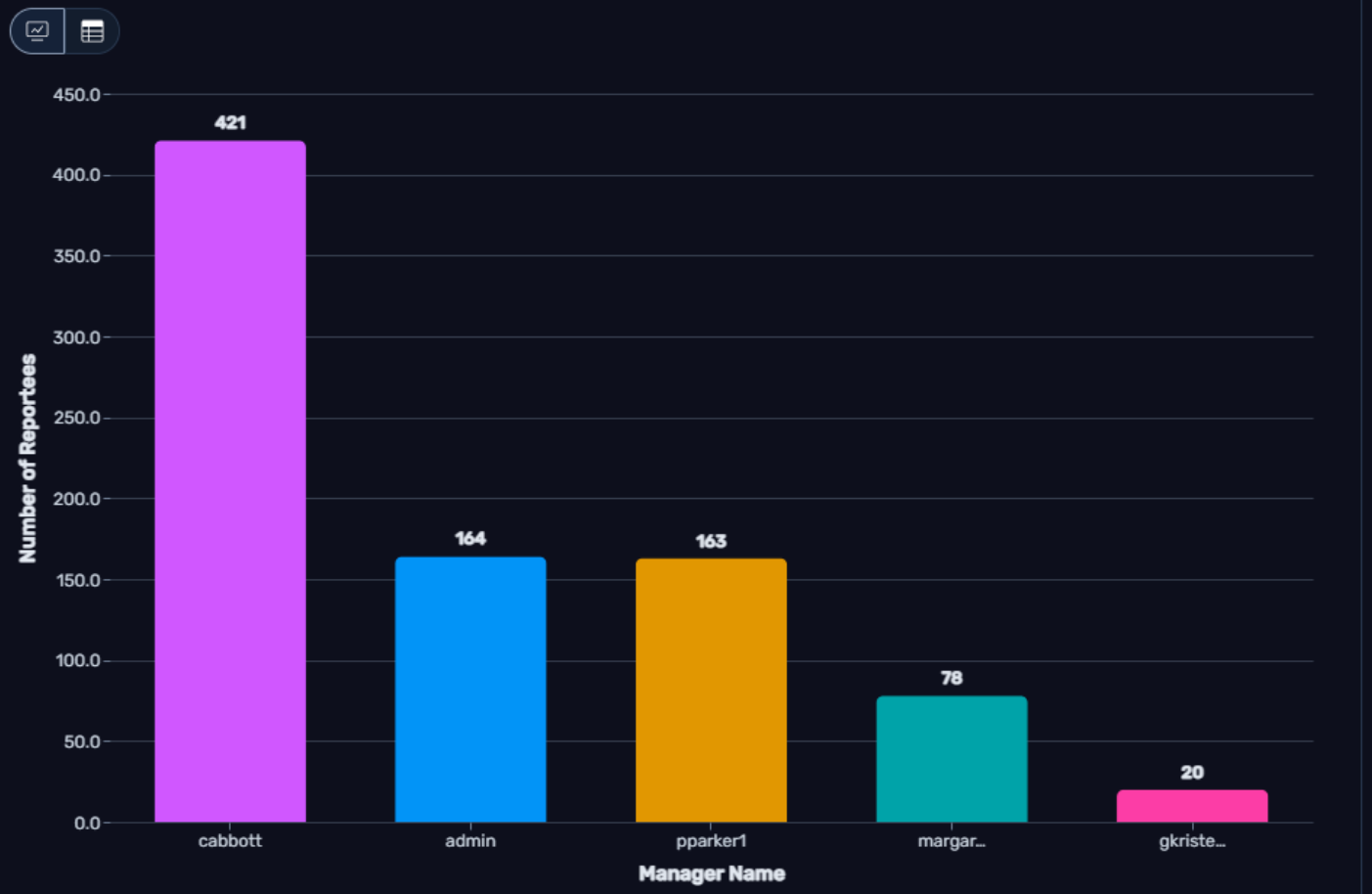
User Manager	610	Entitlement Owner	15
Service Account	8	Application Owner	6
Role Owner	2	Self Certification	2
Organization Owner	1	App Owner Metadata	0

CERTIFICATION SCOPE

- 763 Entitlements
- 663 Accounts
- 656 Certifications
- 267 Userbase
- 197 Applications
- 57 Certifiers

Savi Copilot

Top 5 managers with the most reportees



<chart>

The bar chart above visualizes the distribution of direct reports across the top 5 managers, making it easy to compare their team sizes.

← View Chart

addd the manager departement name as a colum

Here are the top 5 managers with their departments and number of direct reports:

<data>

<chart>

The bar chart shows the distribution of direct reports across these managers, with their department affiliations now included in the results.

← View Chart

Top 5 managers with the most reportees

Here are the top 5 managers with the highest number of direct reports:

<data>

<chart>

The bar chart above visualizes the distribution of direct reports across the top 5 managers, making it easy to compare their team sizes.

← View Chart

What can I help you with?

Savi is always learning new things. Results may vary.

/v6/identityMatchAndMerge/home

Custom Insights

Active Accounts by Endpoint

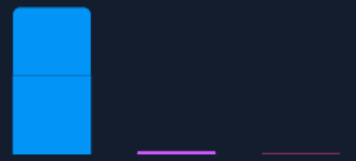
Distribution of Active Service Accounts by Application

Active Accounts by Endpoint

Distribution of Inactive Users by Endpoint

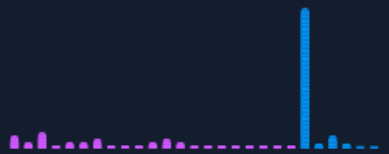
Daily Request Volume Over Past 30 Days

Certification Metrics by Certifier



Users with Most Inactive Accounts

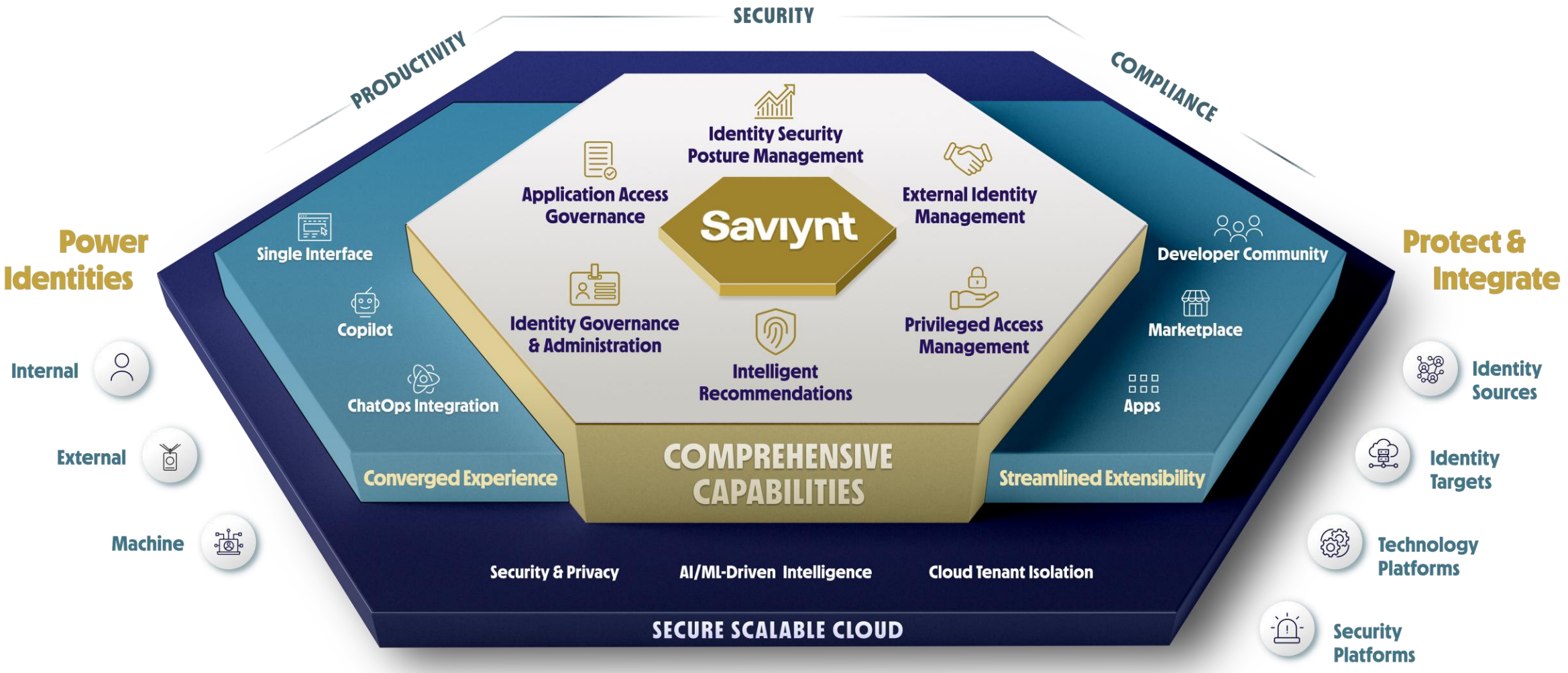
High Risk Entitlements by Risk Score



SAP Request Approvals vs Rejections

La Plateforme Convergée Saviynt

THE IDENTITY CLOUD



Découvrir et inventorier l'ensemble des identités (humaines et non humaines) et des ressources

Améliorer l'hygiène des données pour renforcer l'efficacité des contrôles de gouvernance.

Permettre aux utilisateurs métiers un accès en Self-Service aux données d'identités grâce à l'IA

Réduire les anomalies remontées par les audits en améliorant la préparation et la collecte des preuves

21 octobre 2025 - PARIS

@IdentityDays
#identitydays2025