



access
management

Governance | Compliance
Integration | Flexible | Auditing



WE PROVIDE IT SERVICES WITH EXCELLENCE IN QUALITY AND **PREMIUM SERVICE**

SEEKING TO BUILD REAL AND LASTING TIES WITH OUR CUSTOMERS, EMPLOYEES, AND PARTNERS.

PARTNERS:

Microsoft
Partner



Gold Cloud Platform
Gold Application Development
Gold DevOps
Gold Data Analytics
Silver Collaboration and Content



+11 YEARS

OF EXPERIENCE

+100

CUSTOMERS SERVED

+500

EMPLOYEES

**HISTORICAL
GROWTH
HIGHER THAN**

25%

PER YEAR

Our Customers



Finance



Health



Manufacture



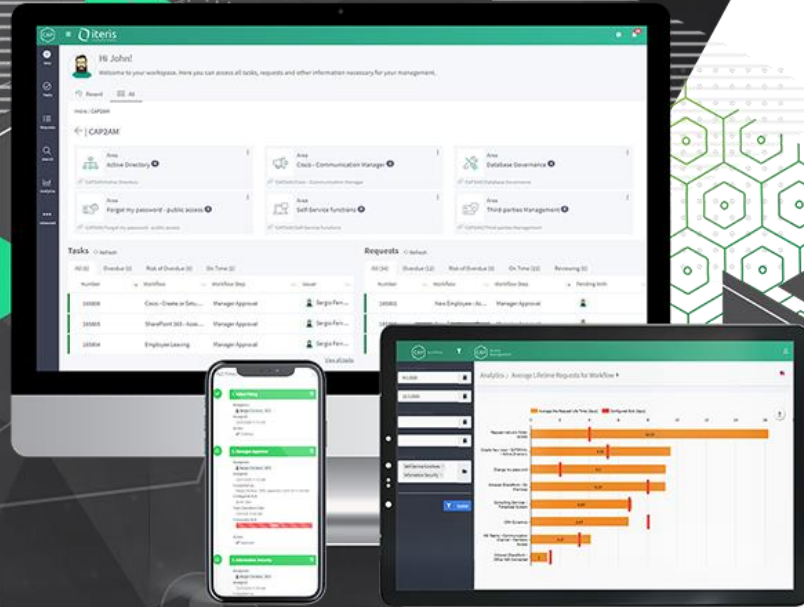
Energy



Miscellaneous



Agro
4



CAP2AM is an identity and access management platform that is quickly adopted and adaptable to the most diverse governance challenges.

We are an IGA (Identity Governance and Administration) platform, a category created by Gartner for positioning identity and access management and administration tools.

Fast Track IG&A Adoption



With CAP2AM you connect your HCM/payroll system and / or third-party management and get a better experience in managing the **Onboarding** and **Offboarding** process.

It's Identity Governance and Administration with **controls** and **agility**.

You will manage the life cycle of user **access** and **identity** (access request workflows) centrally, no matter if it is in the **cloud** or **on-premises**.

A full orchestration of the Granting and Revoking processes (cloud, on premises or both).



Manual



Automatic
(APIs)



RPA
granting



Current Priorities

Global priorities in IG&A – Identity Governance & Administration



access
management



SECURITY

Reduce risk & Mitigate
impact of a breach



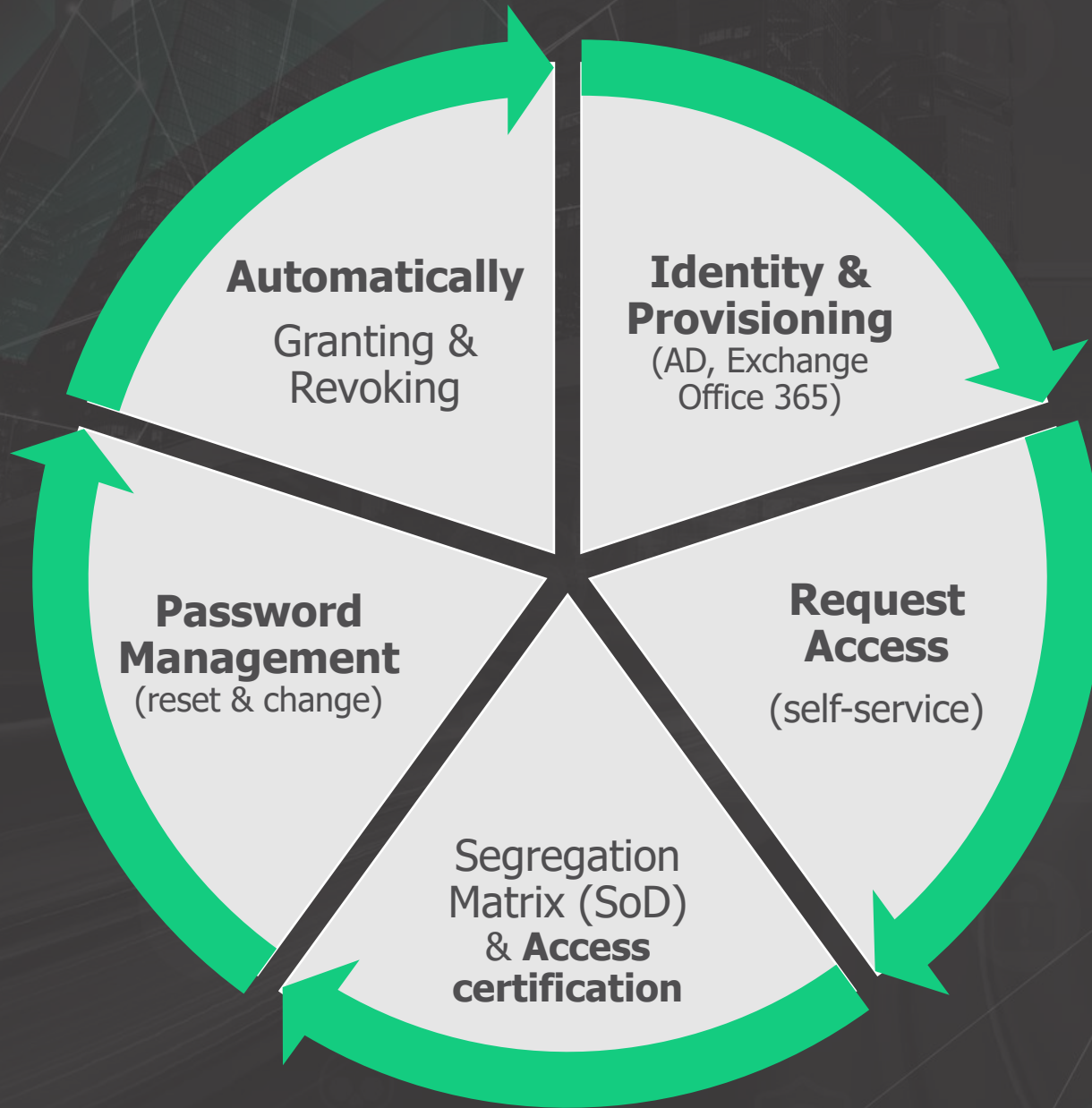
GOVERNANCE

Simplify Data Privacy &
Compliance Efforts



EFFICIENCY

Reduce operational costs,
streamline workflow & access
automation



Identity Administration and Access Management

- **Top 5** challenges tackled by **CAP2AM**
- Our modern approach aligns with IG&A trends to support our customers

Identity & Provisioning

Onboarding - Top #1 priority in terms of provisioning



access
management



Provisioning
Network users



Provisioning accounts to
**O365 / Exchange /
Google**



Access to **network
folders**



Permissions to
VPN access



Provisioning **VoIP
(Cisco)**



**Granting &
Revoking** access to
legacy applications

Identity & Provisioning

Offboarding - Top #1 priority in terms of deprovisioning



access
management



Block **network
users**



Block
e-mail accounts
(quarantine)



Revoke **network
folders access**



Revoke **VPN
Access, VoIP**
etc

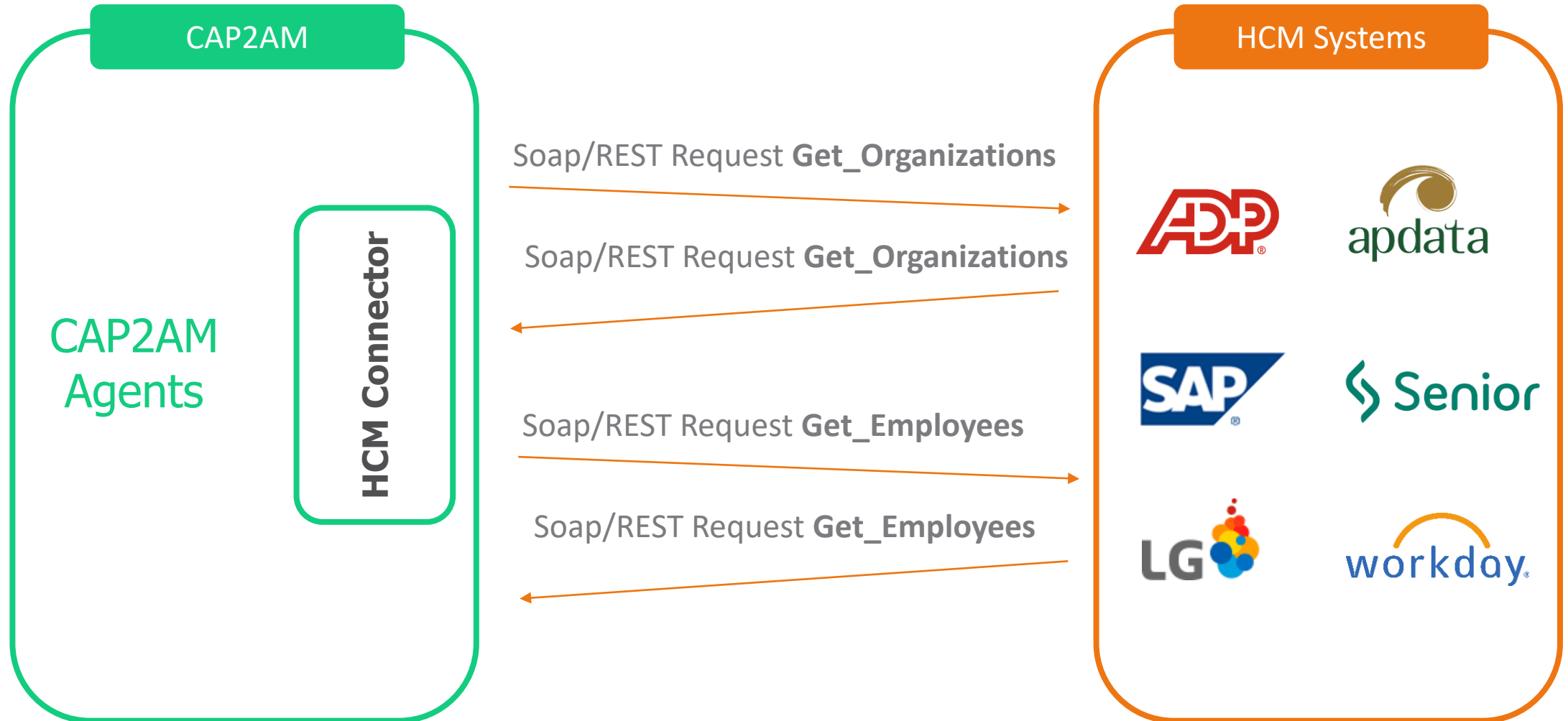


Block **access to
legacy apps**



Block **SaaS**
Accesses &
**deprovisioning
licenses**

How It Works?



CAP2AM integration with HCM



HCM Systems

HCM System (Human Capital Management) is an identity source where we receive employee data & business roles that will be used to create digital identity profiles and access roles to company resources.

This information along with other sources data is used to access administration and governance.



access
management



Email



SaaS/Cloud Apps



On-premises Apps



Data Resources



Networking

Example of New Employee Onboarding



HCM Systems



Email



SaaS/Cloud Apps



On-premises Apps



Data Resources

"Access to data resources is not needed"



Networking



New employee is created on HCM



CAP2AM receives employee data and creates and identity profile



Based on business roles and access information, access requests are created to resources

Example of Employee Change Roles



HCM Systems



Email



SaaS/Cloud Apps
"Access to CLOUD APPS is not needed"



On-premises Apps



Data Resources
"Access to data resources is needed"



Networking



Employee **changing roles**



CAP2AM receives **role changes** and **updates** the identity **profile**



Access to resources is **adjusted**

Example of Employee Leaving



HCM Systems



access management



Email



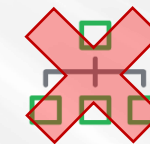
SaaS/Cloud Apps



On-premises Apps



Data Resources



Networking



Employee status is marked as **inactive**



CAP2AM receives status **update** and **revoke** all **identity access**



Access to resources is **removed** **within minutes**

Request Access Workflows

Top #2 priority in terms of IG&A



access
management



Who has
access?



Who approved
the access?



How can I
request an
access?



Who is the
access owner?



Who really had to
approve the
access?



Witch systems user
need access?



Is the user access
already valid or is
expired?

How to guarantee ecosystem management?

Centralized governance of dozens of types of accesses



access
management



NETWORKING

- Network users
- E-mail
- Biometry
- Tokens
- VoIP



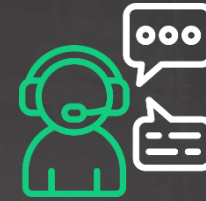
ERP

- SAP
- Oracle
- Microsoft
- Totvs
- Dynamics
- MV
- Tasy



LEGACY

- CRM
- Intranet
- Help Desk
- E-Learning



TI

- Password reset
- Network folders
- Databases
- VPN



CLOUD

- Sales Force
- Workday
- SharePoint
- ServiceNow
- Etc ...

Access Request Workflows

Empower business users



access
management



Access Request
(self-service)



LEGACY SYSTEM



Governance (Access Management)

Running World-Class IG&A

The Path to Progressive IG&A



BEST MATURITY

- 7. Error Reduction
- 8. Risk Mitigation
- 9. Focus on strategic tasks

ACCESS INTEGRATION

- 4. Measure bottlenecks
- 5. Prioritize tickets reduction
- 6. Starting automation (pareto)

ACCESS CONTROL

- 1. Access Inventory
- 2. Granting and Revoking
- 3. Centralized control

Granting and Revoking Manual Accesses

Common scenario for the starting the adoption of an Access Management system, since almost all companies already have some type of “ticketing system” related to the granting and revoking of accesses.

Additionally, is strongly recommended users accounts clean up early in the first stage of deployment, reducing the risk of unused accounts.

Connectors to keep hands-off

At this level of maturity, it is already possible to measure where the bottlenecks of the process are, in addition to being able to identify a Pareto (80/20) of the main systems and accesses.

Best of breed in IG&A Scenario

Error Reduction; Access inventory; Compliance; Reduction of manual Service Desk activities; Reduction of Audit Points; Mitigation of labor risks; Information Leak Mitigation etc.

SUCCESS CASES

Oracle IDM replacement in 3 weeks, **reduction** of **hundreds** of **tickets** and automation of new access controls.



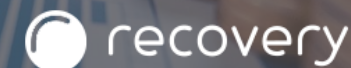
Significant reduction in password reset tickets in the **ERP (MV)** and release of the security team for activities with **higher added value**.



Granting and Revoking of thousands of accesses **integrated to SAP** and **Active Directory**, in addition to periodic re-certification of accesses.



Automation of employee **onboarding** and **offboarding**, provisioning all **O365**, **AD** and **VoIP** accounts.



In good company

Guide



raízen



TOTAL
express



SGS

rede



YASKAWA



accessstage



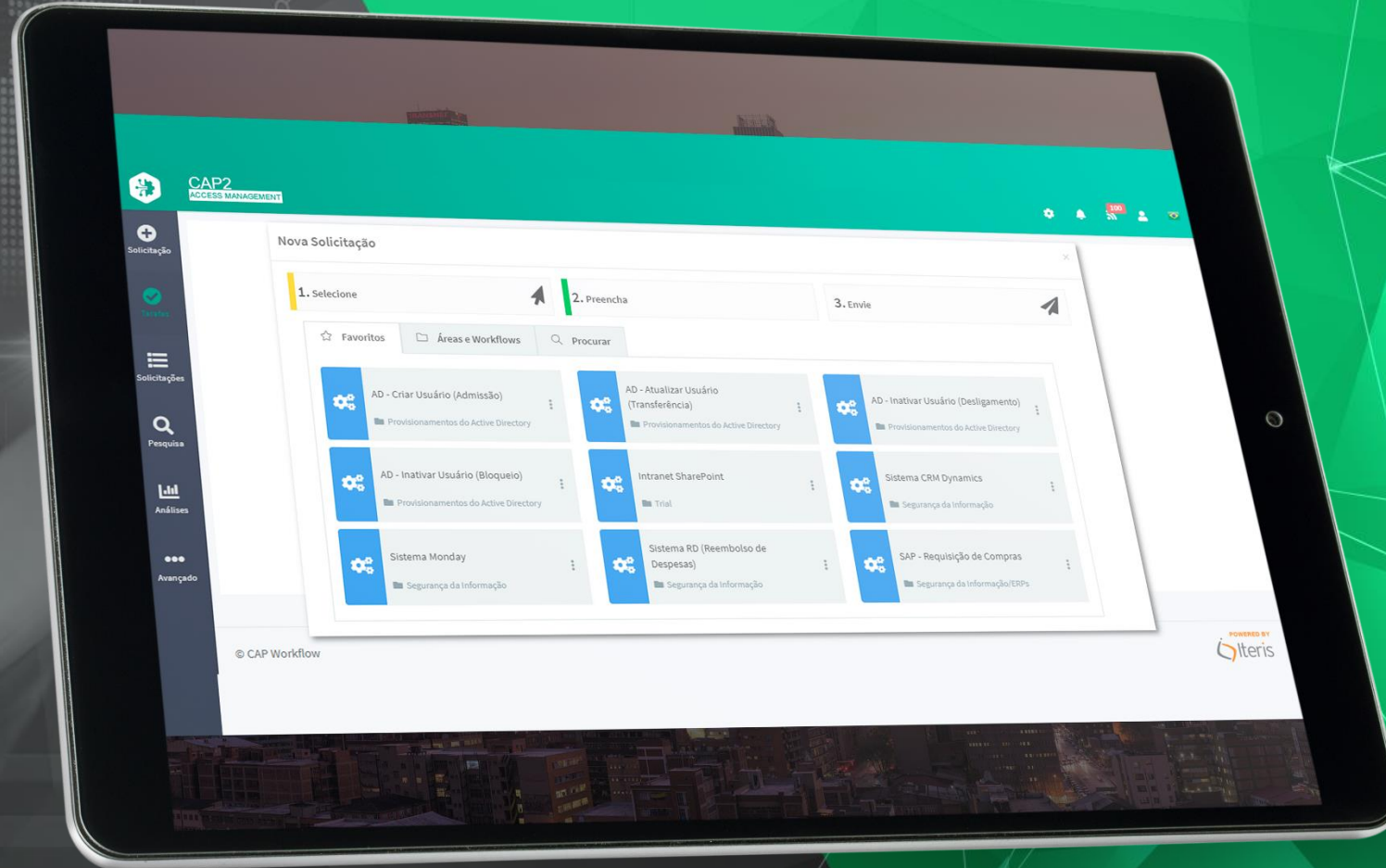
FIBRA
EXPERTS



Some Screenshots

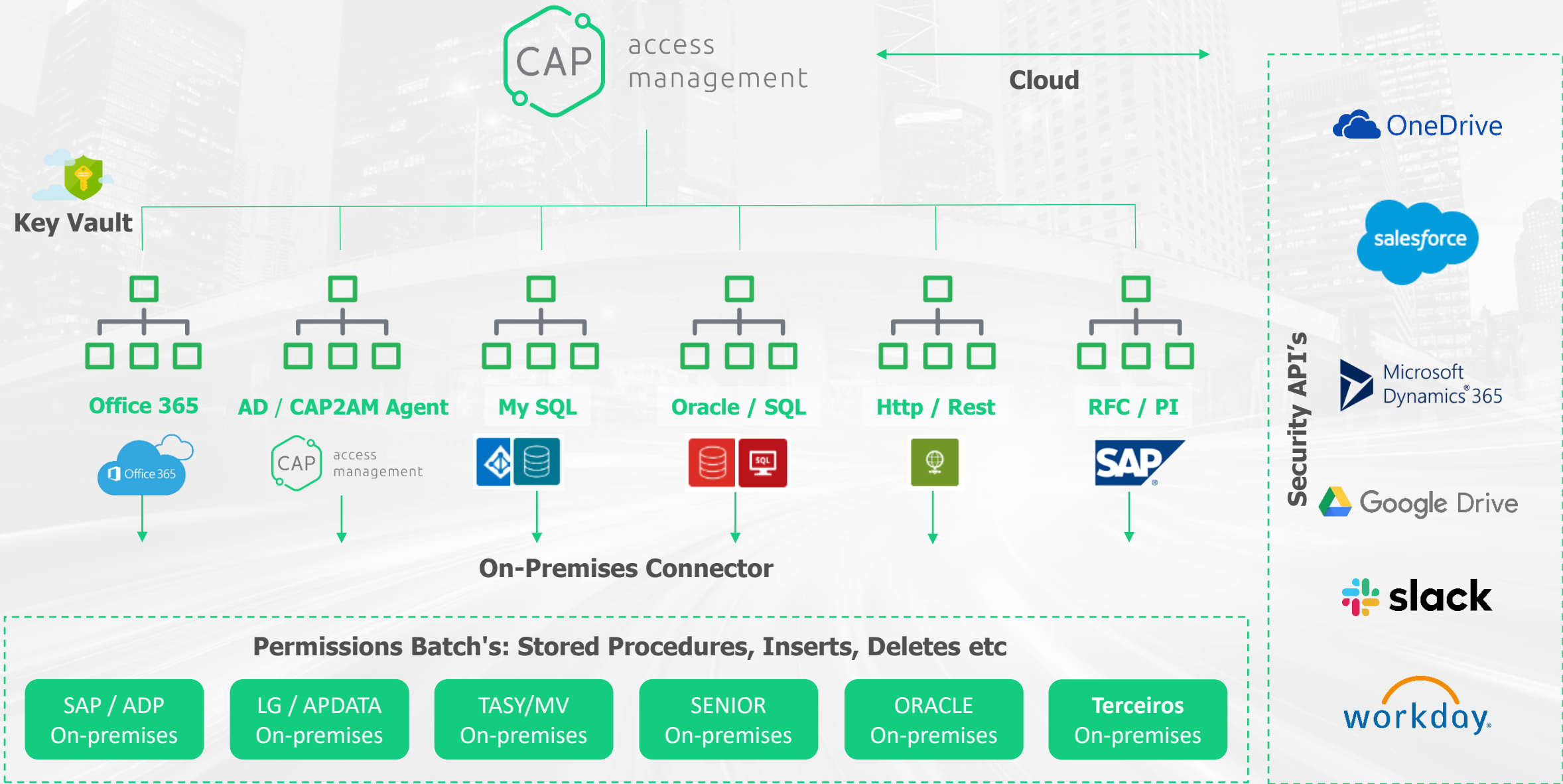


access
management



CAP2AM

Hybrid Integration



CAP2AM

Access Requests – Self-service Portal



access
management

The screenshot shows the CAP2AM self-service portal interface on a tablet. The top navigation bar is green with the CAP logo, a hamburger menu, the Iteris logo, and user settings. The main content area has a dark sidebar with navigation options: New, Tasks, Requests, Search, Analytics, and Advanced. The main area displays a welcome message for 'Hi John!' and a list of recent requests under the 'CAP2AM' tab. The requests are organized into a grid of six cards, each representing a different access area with an icon, title, and a count of requests. Below the grid, there are two sections: 'Tasks' and 'Requests', each with a 'Refresh' button and a list of filters (All, Overdue, Risk of Overdue, On Time, Reviewing) and a table of request details.

Hi John!
Welcome to your workspace. Here you can access all tasks, requests and other information necessary for your management.

Recent All

Inicio / CAP2AM


← | CAP2AM






- Area Active Directory** (4)
CAP2AM/Active Directory
- Area Cisco - Communication Manager** (1)
CAP2AM/Cisco - Communication Manager
- Area Database Governance** (1)
CAP2AM/Database Governance
- Area Forgot my password - public access** (1)
CAP2AM/Forgot my password - public access
- Area Self-Service functions** (5)
CAP2AM/Self-Service functions
- Area Third-parties Management** (1)
CAP2AM/Third-parties Management


Tasks Refresh
All (6) Overdue (0) Risk of Overdue (0) On Time (1)


Requests Refresh
All (34) Overdue (12) Risk of Overdue (0) On Time (22) Reviewing (0)





CAP2
ACCESS MANAGEMENT





Solicitação

Tarefas

Solicitações





Pesquisa

Análises


Avançado

My Tasks

10 records per page

#	Workflow	Workflow Step	Issuer	Pending since	Beneficiary	Type of Access Request	Authentication type	Recertification	Access Risk Score	Process SLA Expires In
370	CRM Dynamics	Execution	Sérgio Ferreira	10/27/2020 2:26 PM	Ellen Sanchez de Oliveira - EOI (ellen.oliveira@iteris.com.br)	Revoke	Windows	365	High	10/28/2020 9:26 AM 
371	Intranet SharePoint - On Premises	Execution	Sérgio Ferreira	10/27/2020 2:26 PM	Ellen Sanchez de Oliveira - EOI (ellen.oliveira@iteris.com.br)	Grant	Windows	0	Regular	10/28/2020 9:26 AM 
372	Request network folder access	Manager Approval	Sérgio Ferreira	10/27/2020 2:28 PM		Grant	Windows	180	Regular	10/28/2020 9:28 AM 
373	AD - Disable User (Spot Block)	Manager Approval	Sérgio Ferreira	10/27/2020 2:29 PM		Revoke	Windows		Low	10/28/2020 9:29 AM 

© CAP Workflow

POWERED BY
Iteris

CAP2AM

Customizable Forms and Approvals steps (Access Workflows)



access
management

The screenshot displays the CAP2 ACCESS MANAGEMENT web application interface. The top navigation bar is green and contains the CAP2 logo, the text 'CAP2 ACCESS MANAGEMENT', and several icons for settings, notifications (100), user profile, and a flag. A dark blue sidebar on the left contains icons for 'Solicitação', 'Tarefas', 'Solicitações', 'Pesquisa', 'Análises', and 'Avançado'. The main content area shows a form for user access management, titled 'Sérgio Ferreira'. The form includes a 'Fields' section with the following fields: 'User name (login)*' (text input: iteris\demo), 'Employee ID*' (text input: 4564654646), 'Reason*' (dropdown menu: Vacation / Férias), 'Authentication type' (dropdown menu: Windows), 'Access Risk Score' (dropdown menu: Low, with subtext: Very High | High | Regular (function) | Low | Very Low), and 'Re-certification' (text input: 180, with subtext: Number of day to re-certificate/re-validate this access.). Below the fields is an 'Observations' section with a text area. At the bottom right of the form are three buttons: 'Save', 'Cancel', and 'Send'.

CAP2 ACCESS MANAGEMENT

Sérgio Ferreira

Fields

User name (login)* iteris\demo

Employee ID* 4564654646

Reason* Vacation / Férias

Authentication type Windows

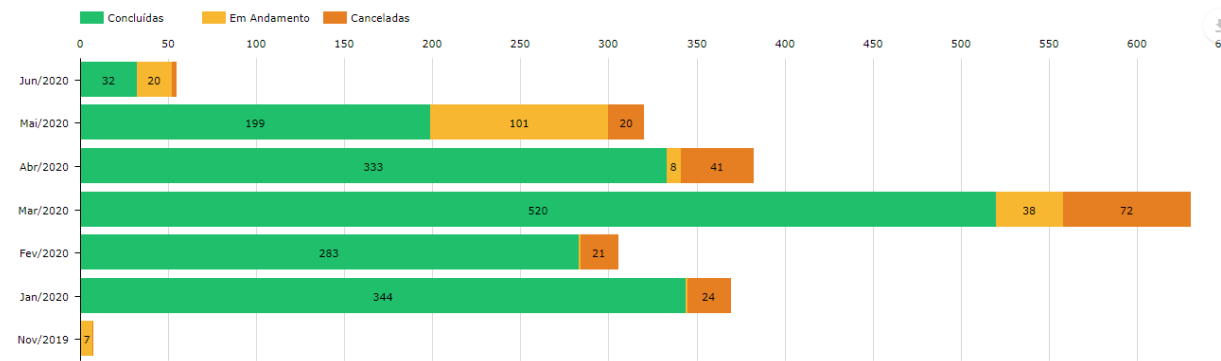
Access Risk Score Low
Very High | High | Regular (function) | Low | Very Low

Re-certification 180
Number of day to re-certificate/re-validate this access.

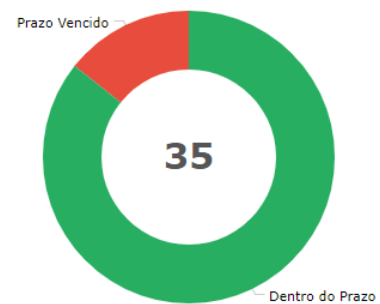
Observations

Save Cancel Send

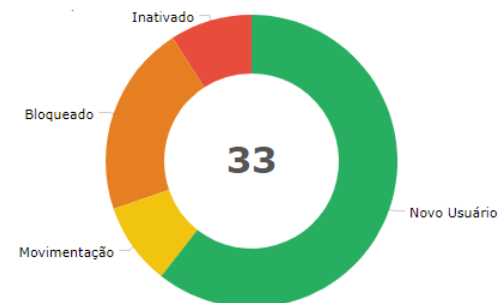
Quantidade de Solicitações por Status



Solicitações por Prazo



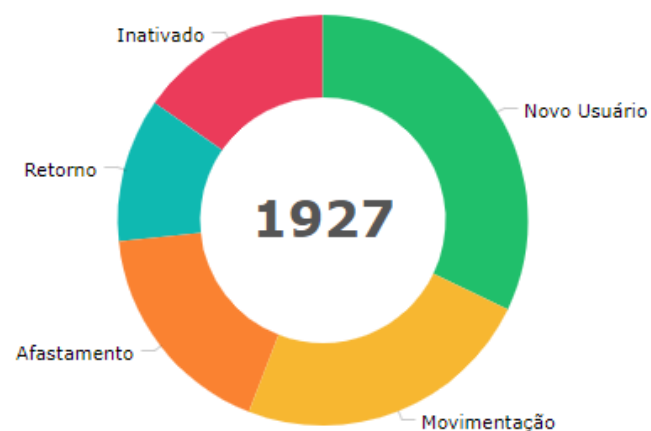
Active Directory



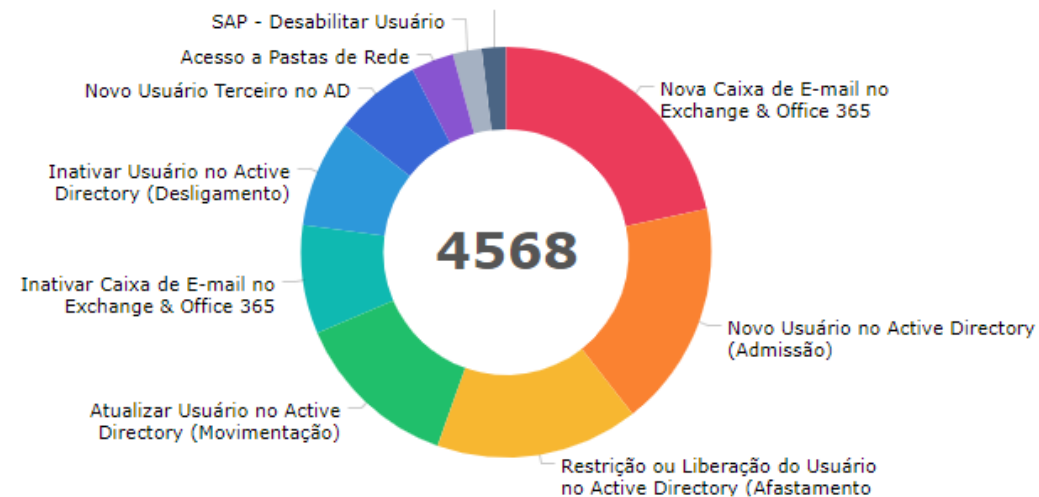
SAP



Active Directory



Solicitações por Workflow



CAP2AM

Access Timeline



Employee ID

4418

Beneficiary Name

Start Date

4/1/2019

End Date

4/11/2019

Export Update

CAP2
ACCESS MANAGEMENT

Analytics / CAP2AM - Access Inventory ▶

Copy Excel PDF Print

10 records per page

Search all columns:

Showing 1 to 3 of 3 records

Request ID	Beneficiary	System/Application	Type of Access Request	Role	Assigned	Comments
Matrícula 4418						
173	willian.silva	AD - Blocking Users (Leaving)	Revoke	Employee leaving	04/10/2019 8:40 AM	
172	willian.silva	AD - Change Roles (new Role)	Grant	Change Roles	04/10/2019 8:35 AM	
171	willian.silva	AD - Onboarding Users (Contracting)	Grant	New User Profile	04/10/2019 8:51 AM	

Previous 1 Next

© CAP Workflow

powered by
iteris



access
management

Governance | Compliance
Integration | Flexible | Auditing

Visit our website!

<https://www.cap2am.com>



The information contained herein is CONFIDENTIAL and protected pursuant to Brazilian Law 9,279 / 96 and other applicable legal provisions, and its reproduction or use, even partially, by third parties not authorized by Iteris, is expressly forbidden.

powered by
iteris
a software company