

No pase por alto la seguridad cuando se traslade a la nube

Ernesto Pérez, CISSP, CISM, ITIL

Sr. Solution Strategist

CA Technologies- Security & Compliance

we can





Introducción

Las organizaciones, independientemente de su tamaño y de su tipo, confían cada vez más en los servicios en la nube no sólo para funciones empresariales importantes, sino también para almacenar y procesar la información confidencial. En palabras de Gartner: “A finales del año 2016, más del 50% de las empresas habrá almacenado información confidencial en la nube pública.” Muchos se resisten a picar el anzuelo de los servicios basados en la nube ya que consideran que la seguridad no ha madurado lo suficiente y que carece de estándares establecidos.

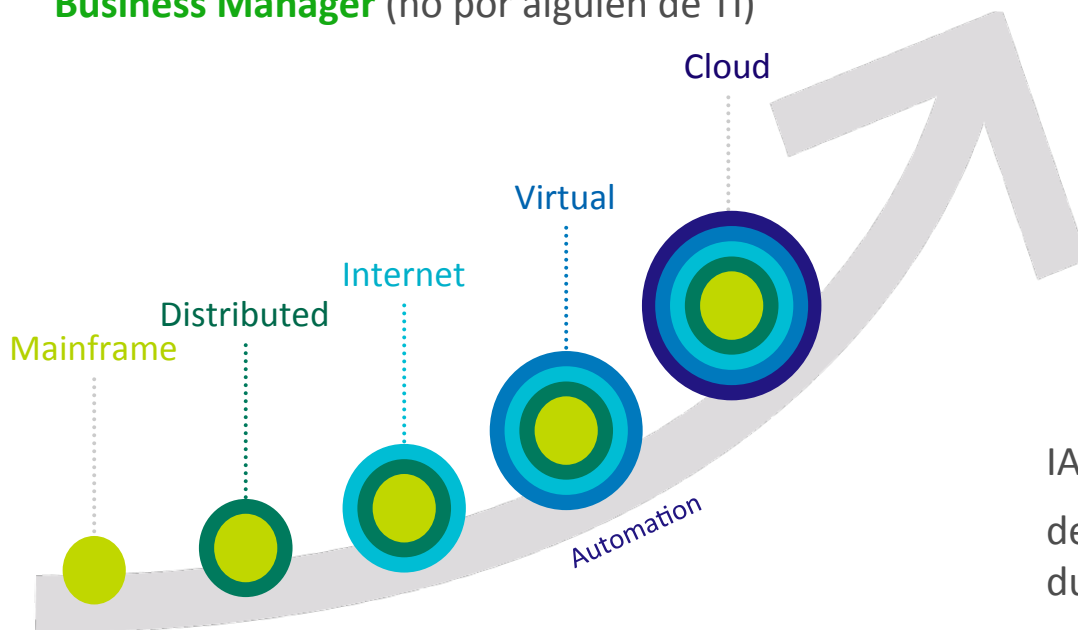
La gestión y el control de las identidades con privilegios y de los datos se han convertido en requisitos para muchas organizaciones. Se debe asegurar la reducción del riesgo de que se produzca una infracción de la confidencialidad, se contribuya a asegurar la responsabilidad de los administradores, facilite el cumplimiento e incluso, acelerar la adopción de nuevas tecnologías.

Dinámica de las tecnologías Cloud

MARKET SHIFT

34% de las adquisiciones de software de negocio será consumidas vía SaaS...

...muchas de ellas adquiridas por un **Business Manager** (no por alguien de TI)



— Sources: IDC, Ponemon, Gartner,

Nuevos Retos

Del top 5 de temas más importantes y sensitivos de las empresas para migrarse a la Nube, el tema

#1 es

IDENTITY AND ACCESS MANAGEMENT

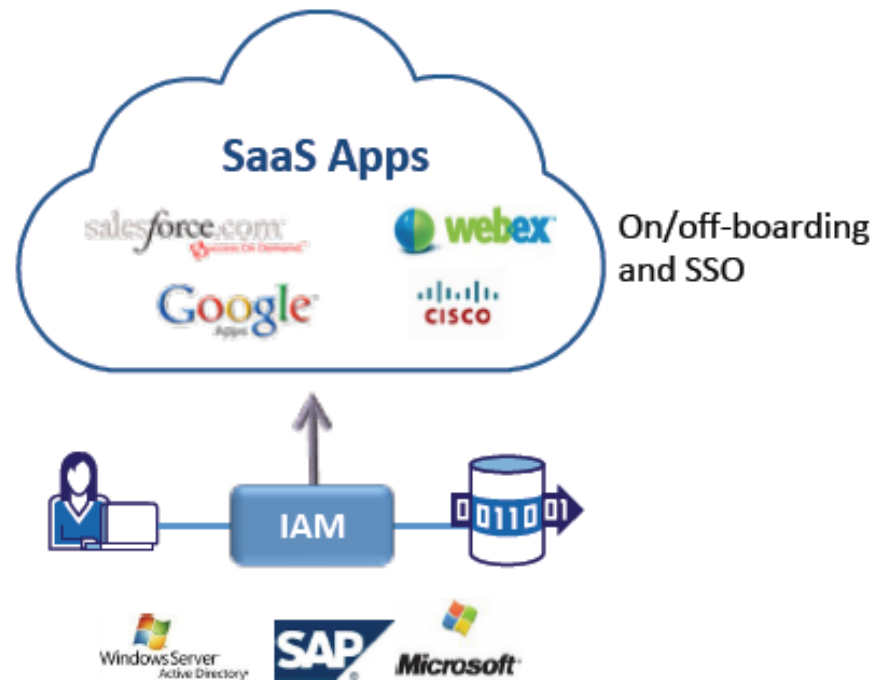
(50% de las respuestas)

Nuevos Modelos de Seguridad

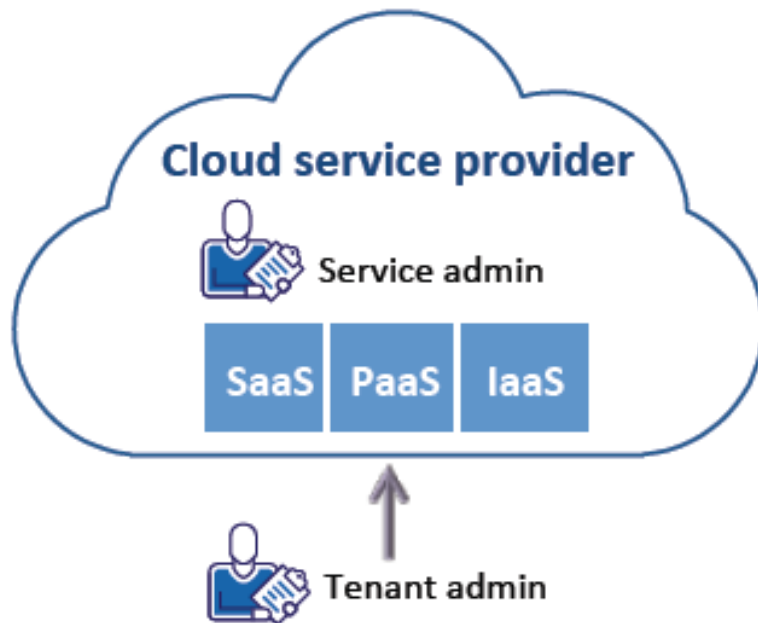
IAMaaS representará el **20%** de todas las nuevas ventas de IAM durante el periodo 2012-2013

(5% mayor que el 2011)

Extender los sistemas de seguridad de la empresa hacia la Nube



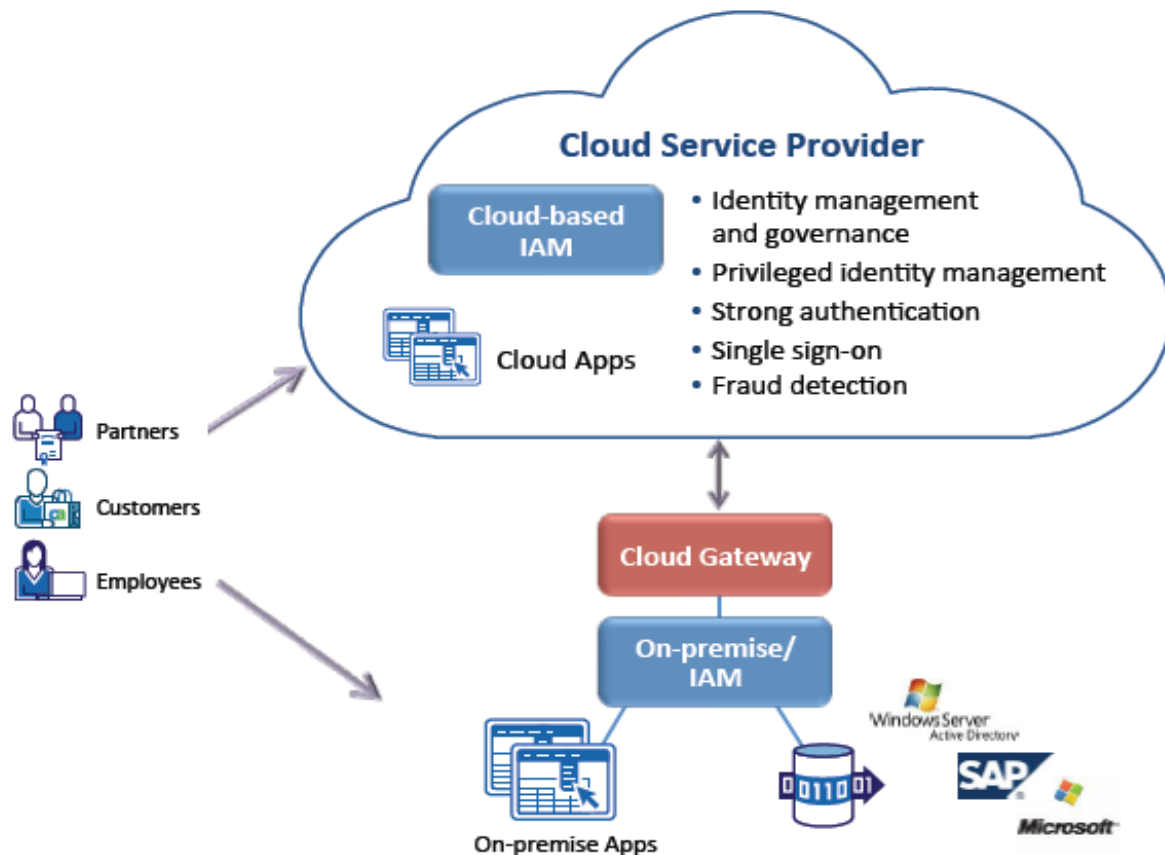
Proveer sistemas de seguridad para la nube



Cloud IAM capabilities

- Identity management and governance
- Privileged identity management
- Web access management
- Strong authentication
- Single sign-on
- Auditing/reporting
- Fraud detection/risk analysis

Entrega de sistemas de seguridad desde la nube



Tendencias y Evolución de la Seguridad : Identidades

Cloud



Redes Sociales



Datos



Mobility



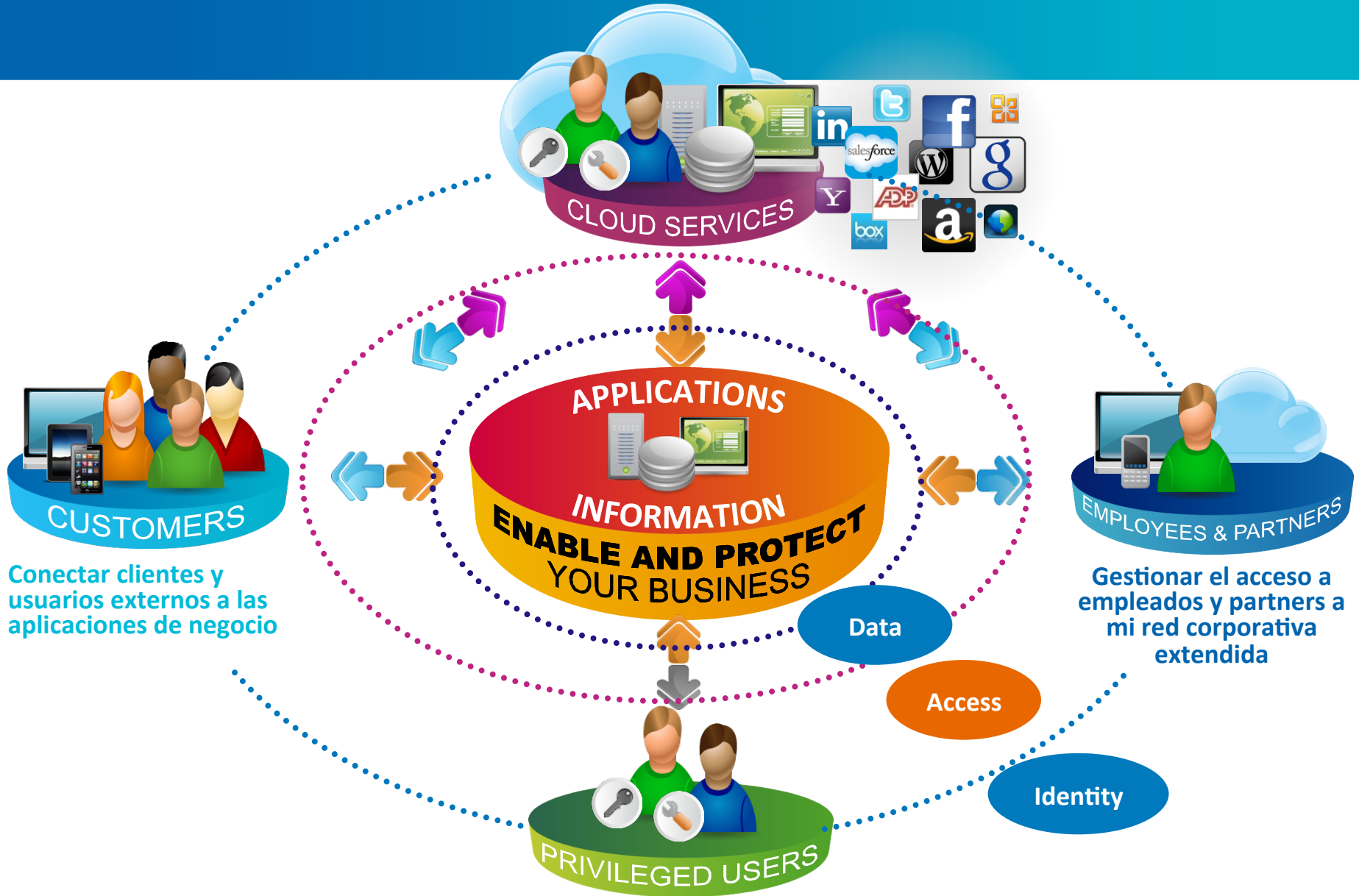
El poder del usuario



¿Cómo.....

- aseguro el acceso correcto de mis empleados y socios?
- contrato servicios en la nube que sean seguros?
- dar acceso dinámico a aplicaciones empresariales y de terceros?
- administrar multiples usernames/passwords?
- restrinjo la fuga de información sensible sin inhibir al negocio?
- puedo proteger a la empresa de manera proactiva y en línea?
- cumplo con lineamientos regulatorios y normativos al usar la nube?

Gestión de los usuarios: empleados, partners y clientes



Administración de seguridad en la nube:

Casos de Uso

AUTENTICAR USUARIOS A LA NUBE

Administración centralizada y asignación de métodos de autenticación dinámica como software tokens, biométricos o firma electrónica

OFRECER EL ACCESO A MULTIPLES APLICACIONES

Single Sign On provee un acceso único a múltiples aplicaciones/websites para una administración más sencilla pero robusta

ADMINISTRAR DINAMICAMENTE LAS IDENTIDADES

Usuarios son aprovisionados o des-aprovisionados mediante una interface fácil de usar, incluyendo self service, creación de profiles, reset de password resets y más

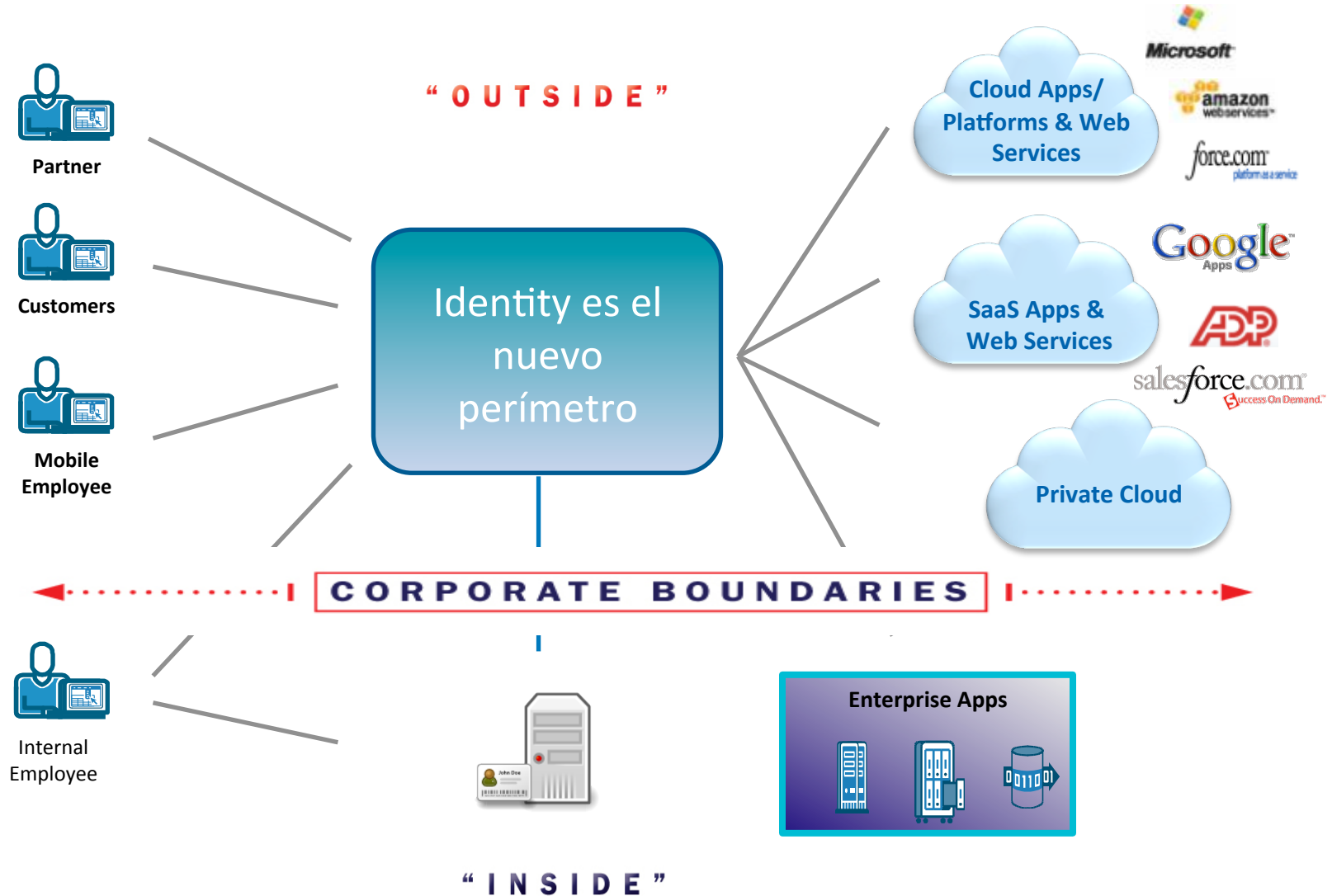
PROTEGER LA INFORMACIÓN DE LA EMPRESA

Consola única y central para realizar tareas de backup, restore y replicación de datos
Evitar fuga de información sensible y dar evidencia para temas regulatorios y normativos

ENTREGA DE APLICACIONES ONLINE SEGURAS

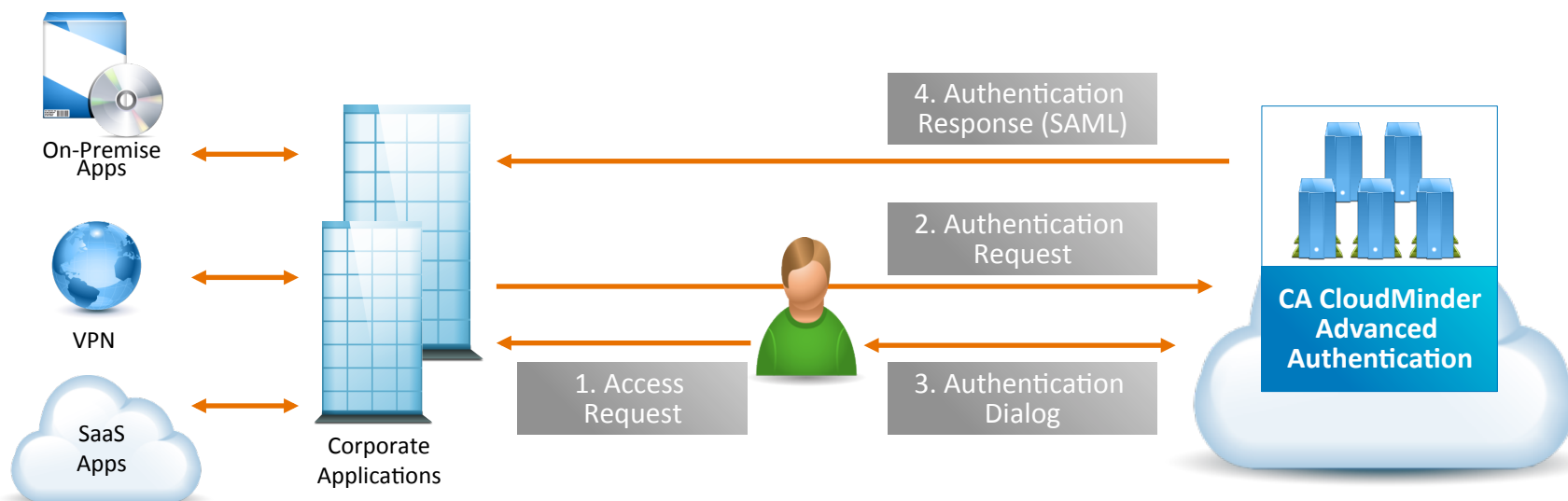
Entrega de facturación segura en línea, on demand, consumiendo lo que se use

La Nube: no es solo sobre administrar empleados... la industria habilitará a los clientes y socios vía la nube



Administración de seguridad en la nube

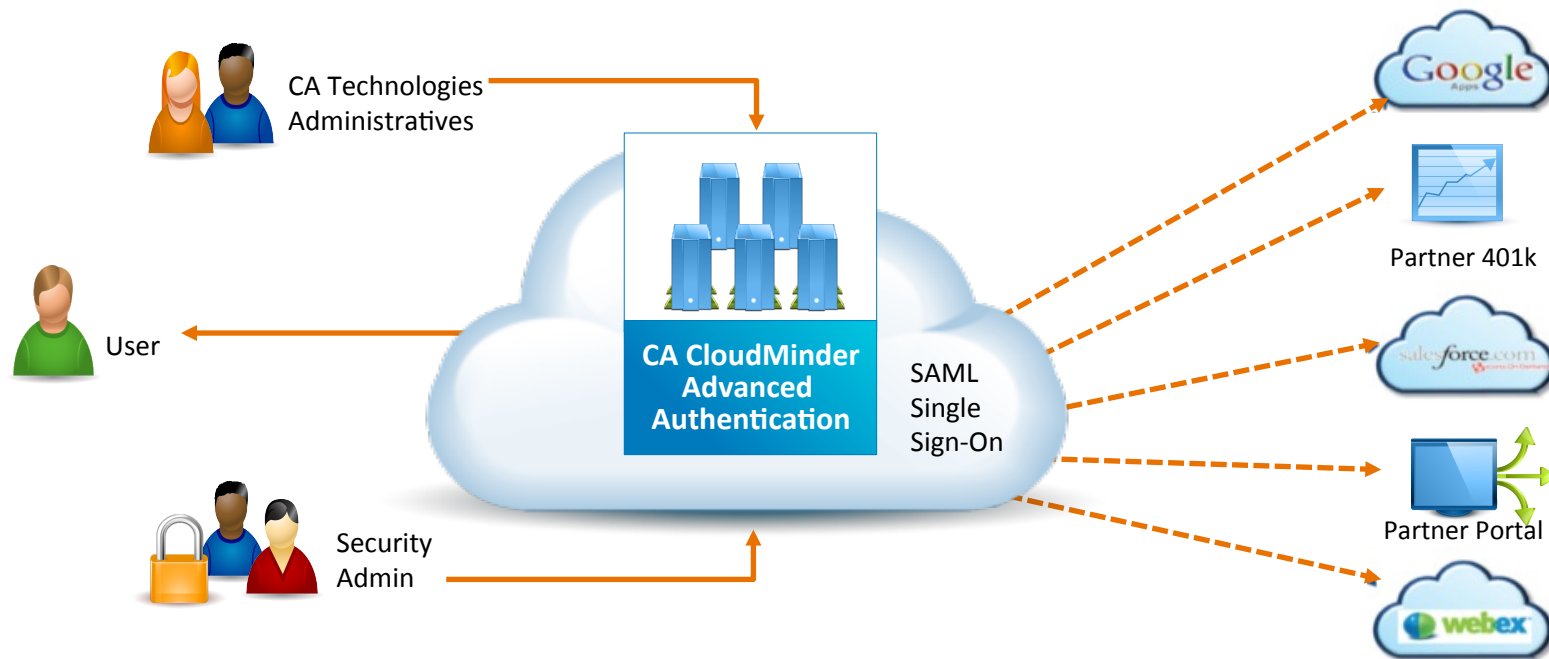
Modelo de arquitectura: Autenticación avanzada



AUTENTICACIÓN AVANZADA

- **Risk detection & prevention** : valorar un “score” de riesgo
- **Rules engine**: determinar el nivel de riesgo de la actividad mediante reglas y políticas modulares
- **Modeling engine**: ofrecer modelos operativos que “disparen” el uso de distintos tipos de autenticación dinámica según el patrón de riesgo

Administración de la seguridad en la nube: Modelo de arquitectura: Single Sign On

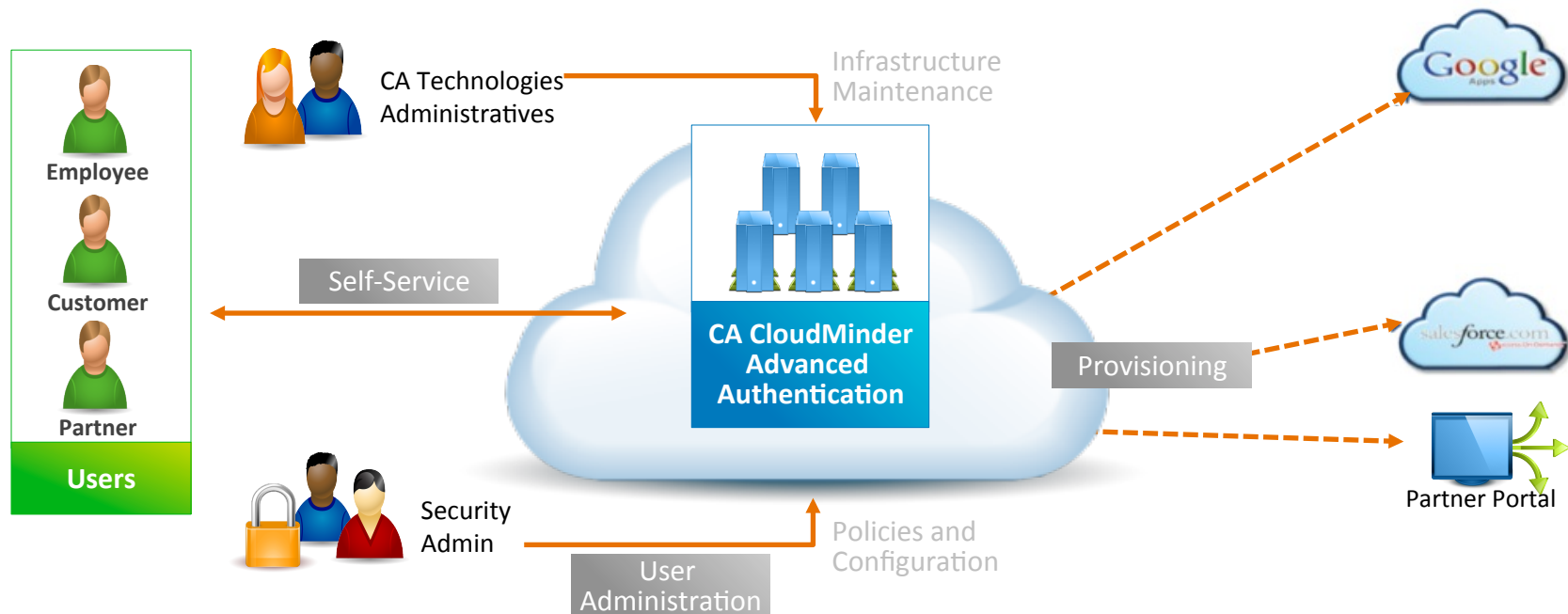


SINGLE SIGN-ON

- **SSO Federado:** SSO cross-domain apalancando el uso del protocolo estándar SAML
- **Aprovisionamiento Just-in-time:** permite a usuarios sin cuenta crear su acceso a las aplicaciones en un solo paso

Administración de la seguridad en la nube

Modelo de arquitectura: Administración de la identidad de los usuarios

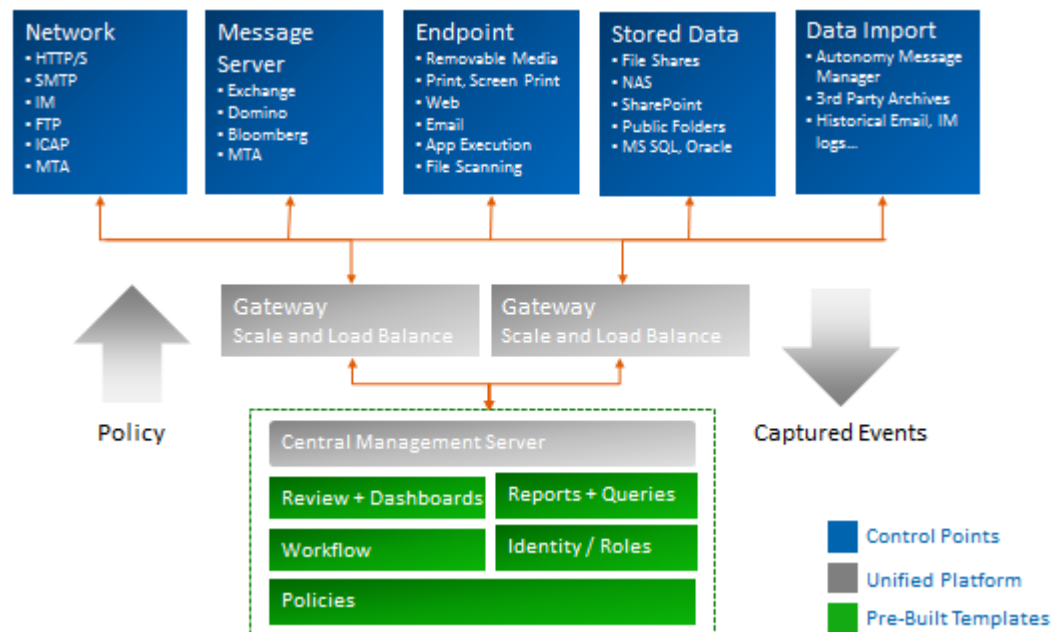


ADMINISTRACIÓN DE USUARIOS Y GESTIÓN DE ACCESOS

- **User Management** : integración con los aplicativos para proveer funcionalidades de administración de identidades en la nube
- **Provisioning**: automatiza el proceso de altas, bajas y cambios de cuentas de usuario
- **Access Request Management**: permite al usuario hacer requerimientos online, que dispara procesos de workflow de aprobación de manera automática basado en políticas definidas

Administración de la seguridad en la nube

Modelo de arquitectura: Protección de información contra fugas



DATA LOSS PREVENTION

- **Control of data** :- descubrir, analizar, inventariar, monitorear y controlar la información corporativa sensitiva para asegurar su confidencialidad, disponibilidad e integridad
- **Identity centric approach** : entender y apalancar la relación entre la gente (rol y perfil) y los datos, particularmente los sensitivos
- **Proactive**: notificación y alertamiento en tiempo real de incidentes y violaciones a las reglas y políticas corporativas

Casos de uso: "Self Service"

Home Page

The screenshot displays the Bentley Cola user interface. At the top left is the Bentley Cola logo. The top right shows the user name 'kevin mann' and a 'Sign out' link. A left-hand navigation menu is titled 'Tasks' and contains 'My Settings' (expanded to show 'Home', 'Manage My Access Requests', 'My Profile', and 'My Password') and 'My Services'. The main content area is divided into two sections: 'My Settings' and 'My Services'. 'My Settings' contains three icons: 'Request & View Access', 'My Profile', and 'My Password' (highlighted with a red box and a blue arrow pointing to the text 'Icon view Self Service'). 'My Services' contains seven application icons: 'Google Docs', 'Google Mail', 'SalesForce', 'SAP', 'SharePoint', 'WebEx' (highlighted with a red box and a blue arrow pointing to the text 'Icon view Applications'), and another 'SharePoint' icon. At the bottom, a footer area is highlighted with a red box and labeled 'Footer Modifiable' with a blue arrow. The footer text includes 'Copyright © 2011 CA. All rights reserved.' and links for 'Contact Us', 'Privacy Policy', 'About Us', and 'About Bentley Cola'.

Default End User Console

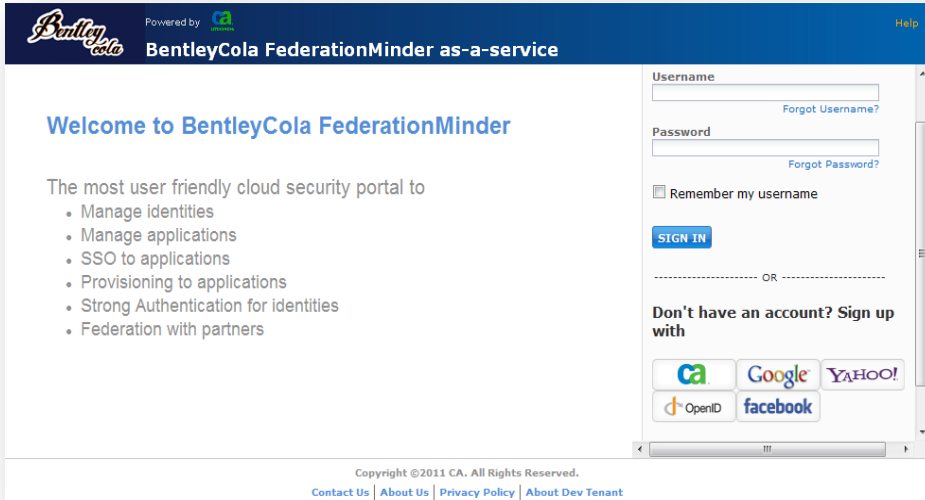
Icon view Self Service

Icon view Applications

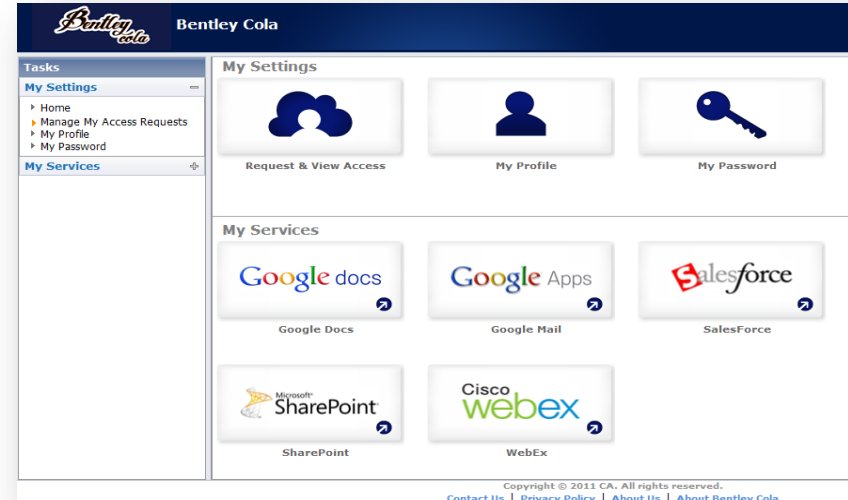
Footer Modifiable

Casos de uso: "Self Service"

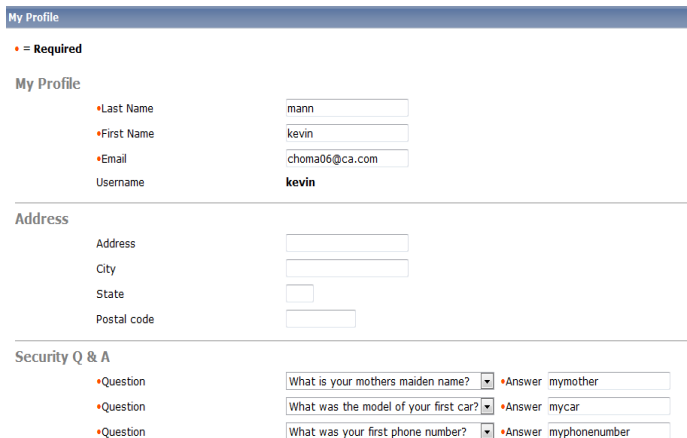
Permitir habilitar a los usuarios gestionen sus perfiles/passwords/requests



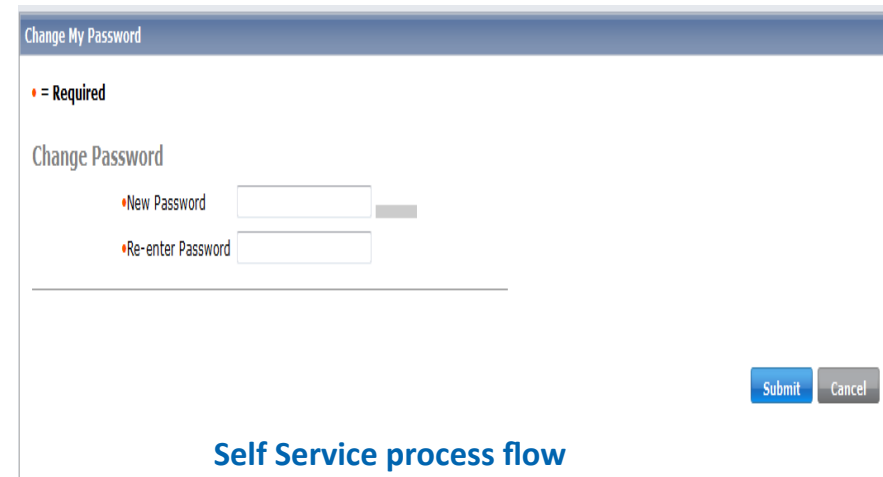
Login page



End User Home Page



Self Service process flow



Self Service process flow

Casos de uso: Suportar identidades sociales

Habilitar a los clientes con sus credenciales existentes



Forward INC.

Log in OR [Register](#)



ArcotID OTP



ArcotID PKI

or

Use your Forward INC. Account

Username :

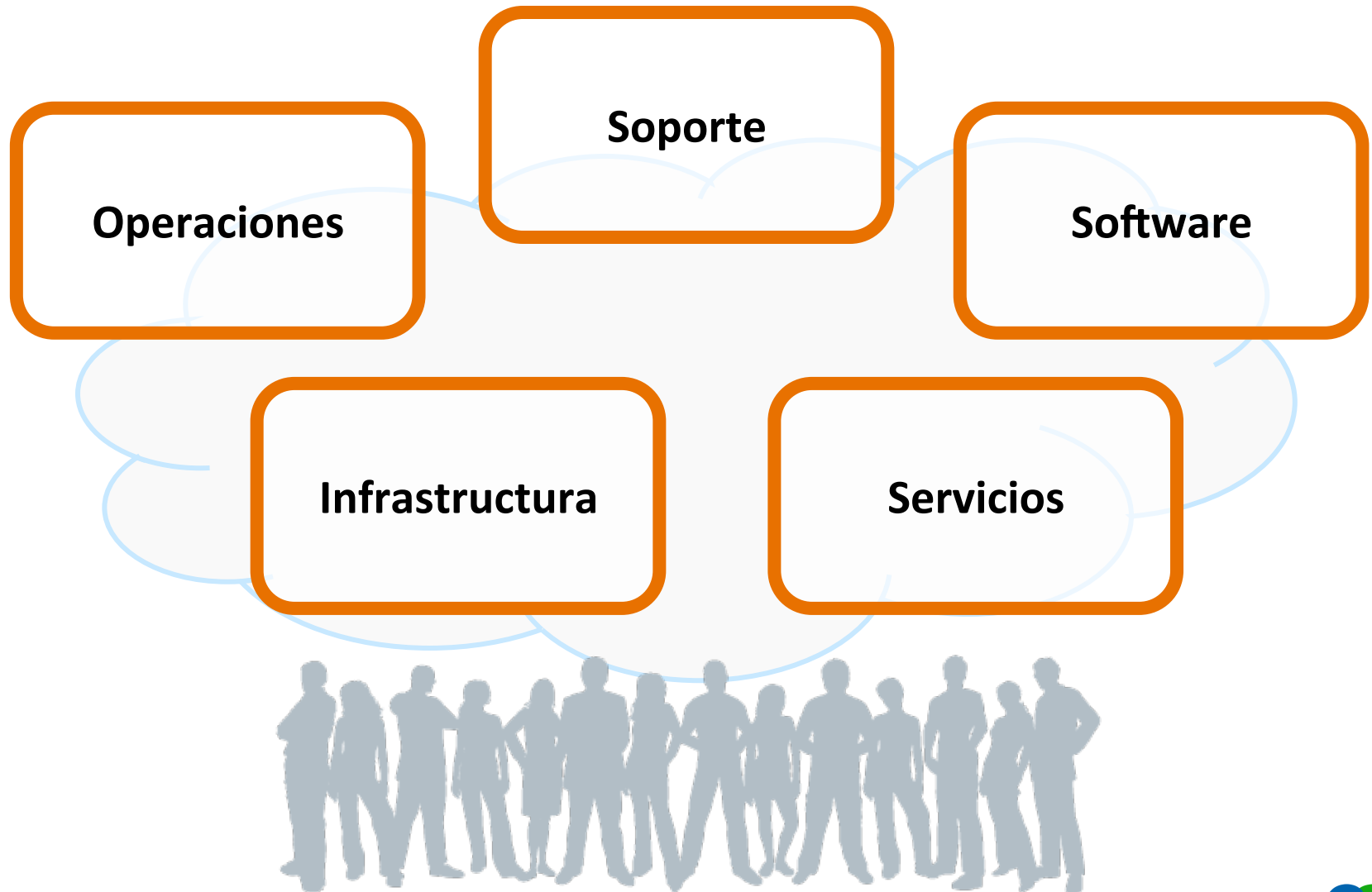
Password :

Login

[Forgot Username?](#) [Forgot Password?](#)



¿Qué debe tener un servicio provisto desde la nube?



Los administradores del Negocio querrán trabajar con uds!



Dueños del negocio

- ✓ Implementaciones y puesta en marcha mas rápidos
- ✓ Sign-ons más reducidos y simples
- ✓ Innovación de negocio



CIO

- ✓ Menores costos operativos
- ✓ Menores costos de Helpdesk
- ✓ Aumenta la confiabilidad



Audidores

- ✓ Reporteo y manejo de evidencias de manera automatizada
- ✓ Auditorías más sencillas



Security Officer

- ✓ Reducir riesgos
- ✓ Ganar “Exposure”

Beneficios

Agilidad de negocio

Ofrecer niveles de **servicio elásticos**, y con opciones de servicio **flexibles y bajo demanda** con cobertura escalable desde un portal único

Reducir riesgo y mejora de compliance

Proteger los **activos críticos desde la nube**, sin importar que los sistemas y aplicativos estén en ambientes físicos, virtuales o en la nube misma

Acelerar nuevos servicios de negocio

Ofrecer nuevos **servicios de seguridad** más rápido y efectivamente. Ser líder del mercado, aumentar el market share y la presencia regional

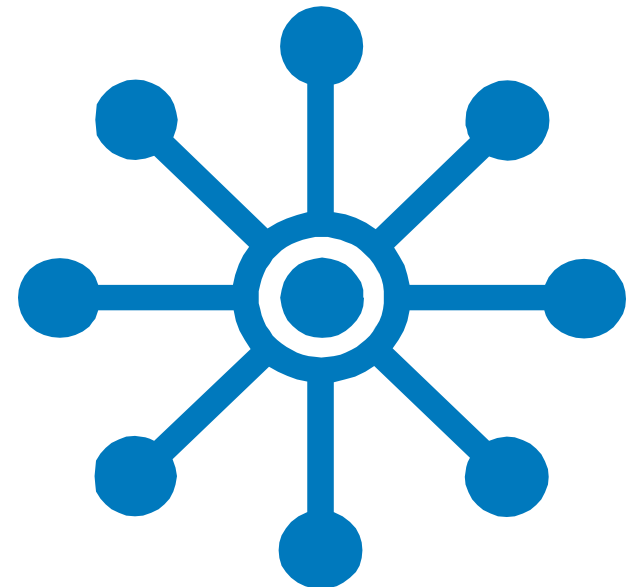
1 Establecer el modelo cloud apropiado

Considerar seriamente a IAM como un modelo de servicio

Iniciar un nuevo modelo con aplicativos basados en la Nube- agregar on-premise con el tiempo

Integrar y aumentar lo que se tiene hoy por hoy

Integrar clientes, partners, proveedores en caso de requerirse

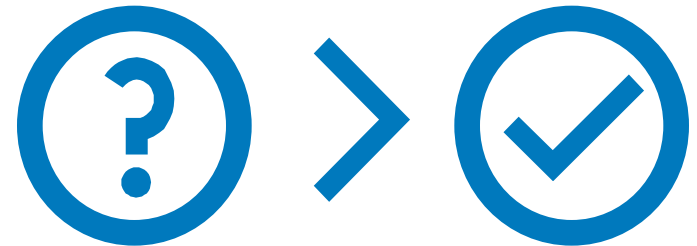


2 Evaluar cloud providers o evaluar como crear la nube propia

Identificar que proyectos son importantes para su organización para el próximo año o dos....

Evaluar proactivamente a varios proveedores de servicios en la nube enfocado en temas de identidades:

- ¿Solicita SAML a sus usuarios?
- ¿Realiza provisioning & de-provisioning de usuarios automaticamente?
- ¿Ofrece consultas a usuarios?
- ¿Accesos a bitácoras y logs?
- ¿Cuenta con servicios de Self-Service?
- ¿Es on-demand y se paga solo lo que se usa?



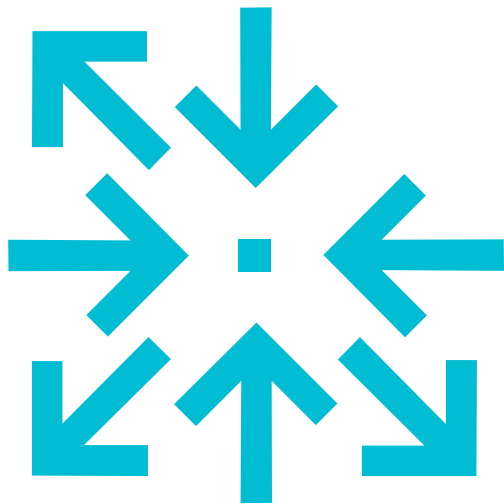
3 Contruir un catálogo

Usar proveedores que sean serios respecto a sus ofrecimientos de Identity Management en sus catálogos

Dar a los directivos varias alternativas

Definir la campaña de offering apropiada tanto a los clientes como a los empleados y partners





El Valor

- Aumentar la agilidad del negocio
- Reducir costos operativos
- Tiempos de implementación más rápidos

¿Porqué CA?

- Tecnología líder de mercado
- Experiencia de entregar servicios en la nube
- “Time-to-value” más rápido

Muchas Gracias !!!

ernesto.perez@ca.com

cel: 04455 9198 6090

Derechos

- *Copyright © 2012 CA. All Rights Reserved. All other trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. Microsoft, SharePoint and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Certain information in this publication may outline CA's general product direction. However, CA may make modifications to any CA product, software program, method or procedure described in this publication at any time without notice, and the development, release and timing of any features or functionality described in this publication remain at CA's sole discretion.*
- *CA will support only the referenced products in accordance with (i) the documentation and specifications provided with the referenced product, and (ii) CA's then-current maintenance and support policy for the referenced product. Notwithstanding anything in this publication to the contrary, this publication shall not: (i) constitute product documentation or specifications under any existing or future written license agreement or services agreement relating to any CA software product, or be subject to any warranty set forth in any such written agreement; (ii) serve to affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (iii) serve to amend any product documentation or specifications for any CA software product.*
- *This document is for your informational purposes only, and CA assumes no responsibility for the accuracy or completeness of the information contained herein. To the extent permitted by applicable law, CA provides this document "as is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised in advance of the possibility of such damages.*