Deloitte.

Identity and Access Management

Tendencia Global

Agenda

- Contexto y Tendencias de CyberSeguridad
- Arquitectura Global de Identidades
- Access Management
  - Autenticación Fuerte y Adaptiva
  - Federación
  - Seguridad en APIs
- Identity Management
- Conclusiones

- Hoy en día, dados los complejos **entornos** de las Compañías, la **aceleración de nuevas tecnologías** disruptivas y su **rápida incorporación** permiten que aparezcan nuevas y mayores vulnerabilidades tornando muy difícil su adecuada y oportuna administración.

Contexto Actual
Entendimiento

Actualmente, dados los complejos entornos de las Compañías, las vulnerabilidades se tornan más difíciles de administrar y las amenazas aumentan fuertemente. Para entender el desafío es importante visualizar los tres entornos de evolución que provocan la aparición de mayores riesgos:

- El **entorno del negocio** evoluciona debido a la competitividad del mercado y las necesidades de los clientes que también evolucionan, originando nuevos modelos de negocios, nuevos procesos y nuevas formas de trabajar.
- El **entorno de IT** evoluciona para soportar los nuevos modelos así como también las expectativas de los usuarios que adoptan nuevas herramientas para estar conectados y ser productivos.
- El **entorno de las amenazas** evoluciona como consecuencia de los cambios en el Negocio e IT creando nuevas vulnerabilidades y se tiene mayor “colaboración y creatividad” para encontrar dichas vulnerabilidades y explotarlas.

Contexto Actual

Desaparecieron las Fronteras - Aparecieron nuevas tecnologías

Redes Sociales

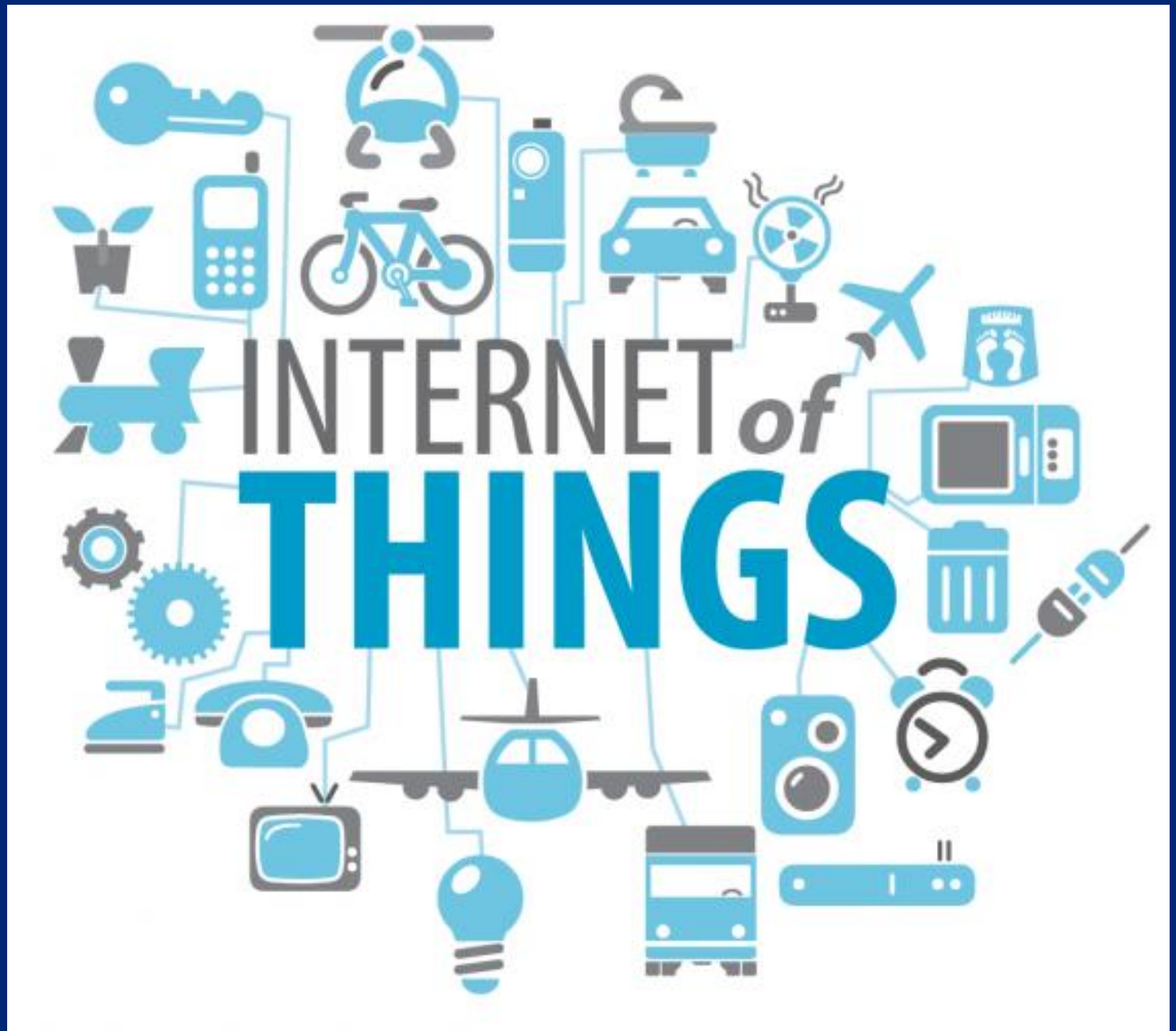
BYOD

Cloud

Mobile

Streamming

Contexto futuro



Cyber riesgos
Preocupación de los CFOs’

- Los cyber ataques se han instalado en la lista de los riesgos que más preocupan a los CFO (según la encuesta de Deloitte CFO SignalsTM) .
- Hace cuatro años cuando se lanzó la encuesta, los cyber- riesgos eran raramente mencionados, cuando hoy día son citados rutinariamente.
- Los CFO se encuentran cada vez más preocupados por los cyber ataques.
- Ese cambio en el modo de pensar tiene su correlación en la frecuencia y costos de los cyber ataques.

3,5 Millones de dólares es el costo promedio de una filtración de información

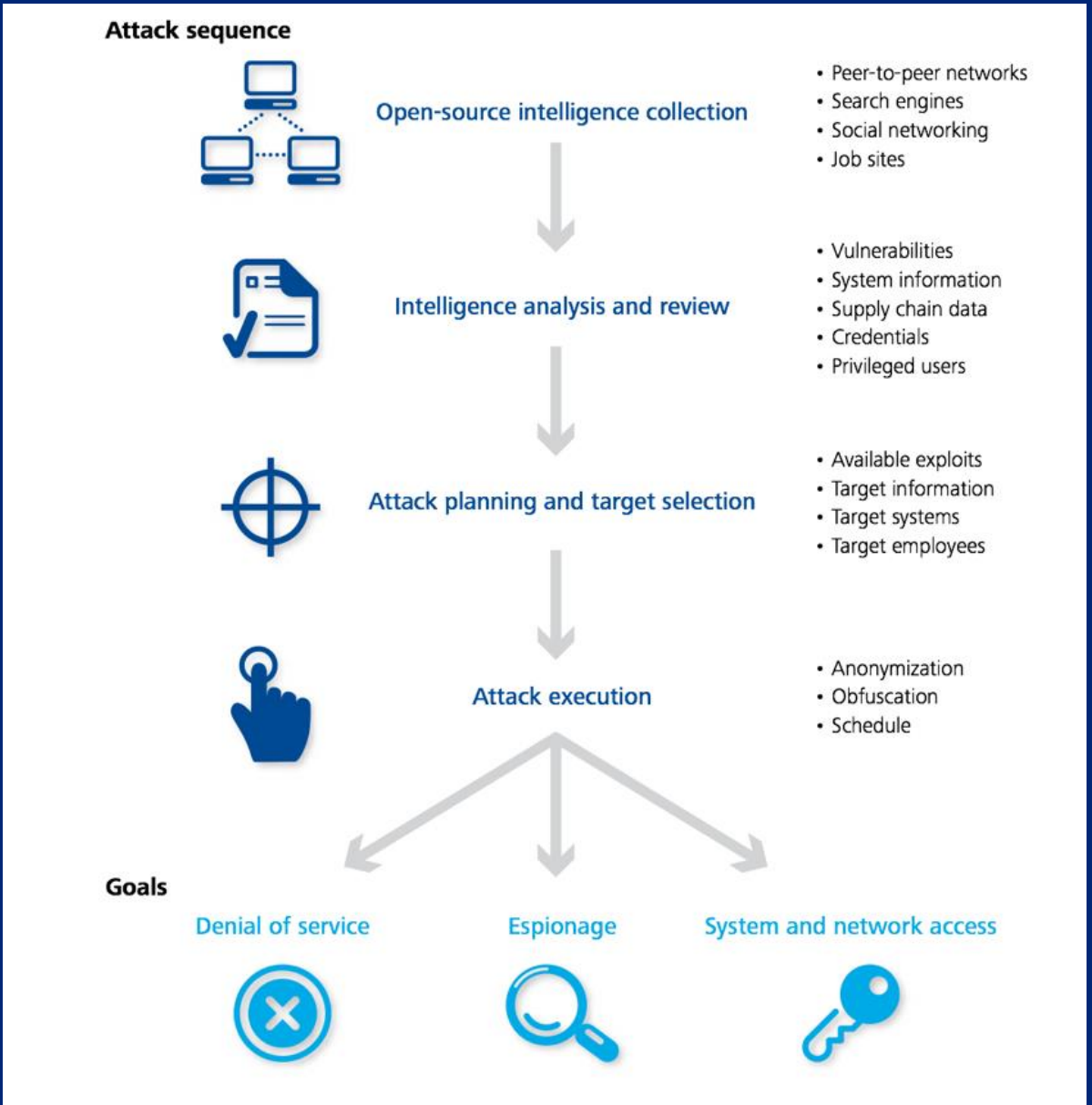
Más que el año anterior **15%**

22% Es la probabilidad que una Compañía sufra una filtración material (10.000 registros o más) en los próximos **24** meses

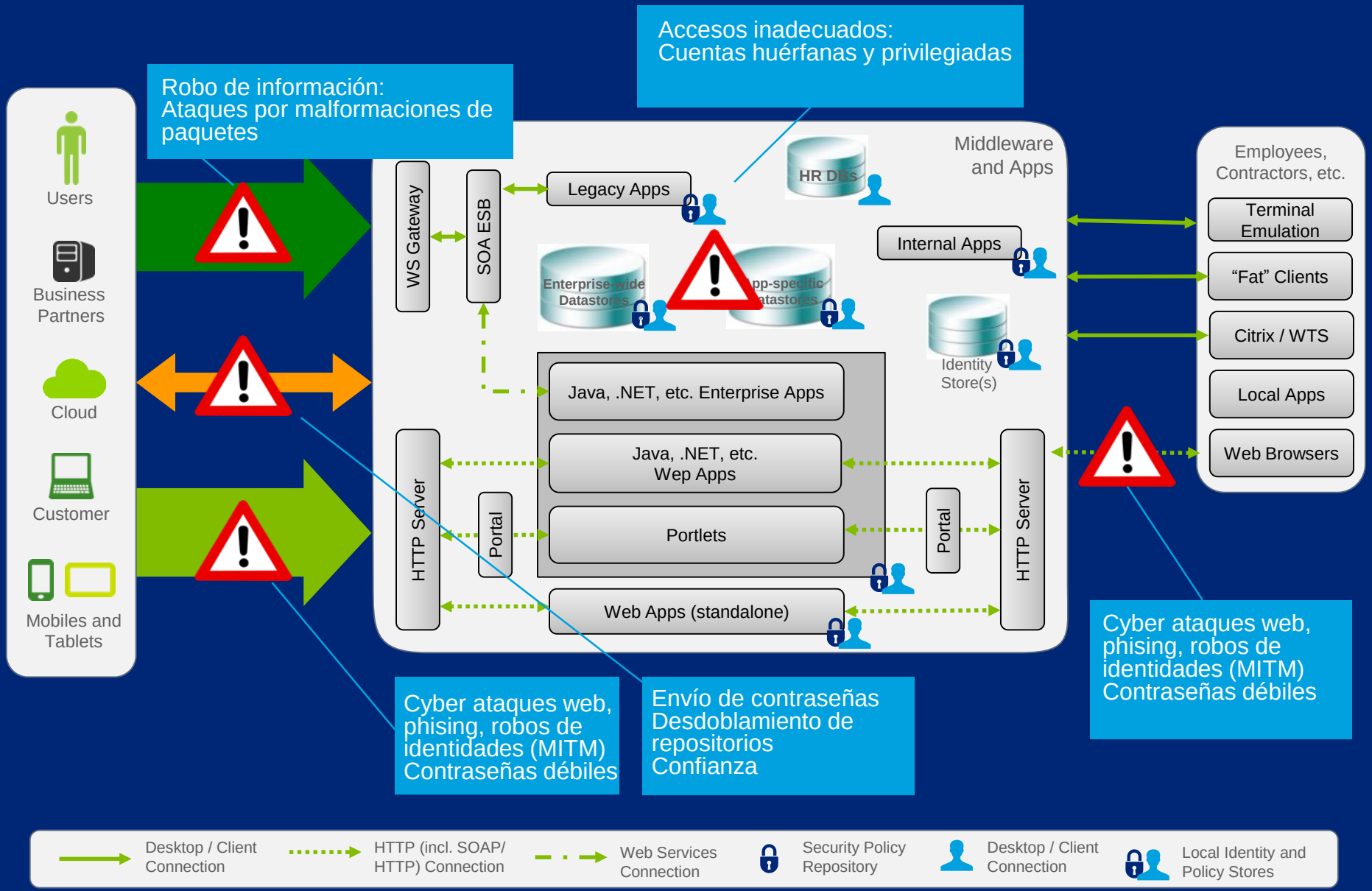
Ponemon Institute’s “2014 Cost of Breach: Global Analysis”

Cyber seguridad

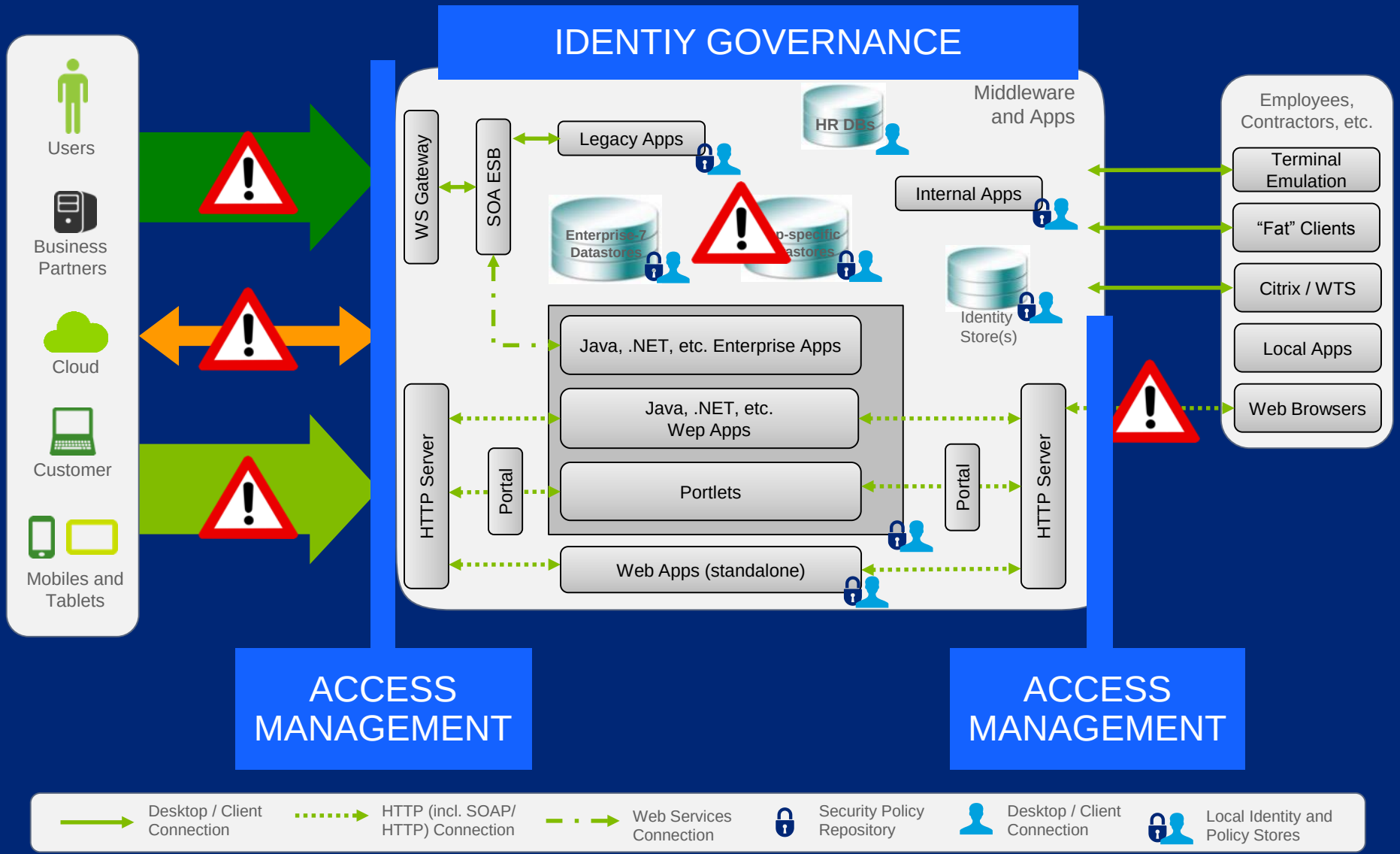
Se focalizaron los ataques



Arquitectura Global de Identidades



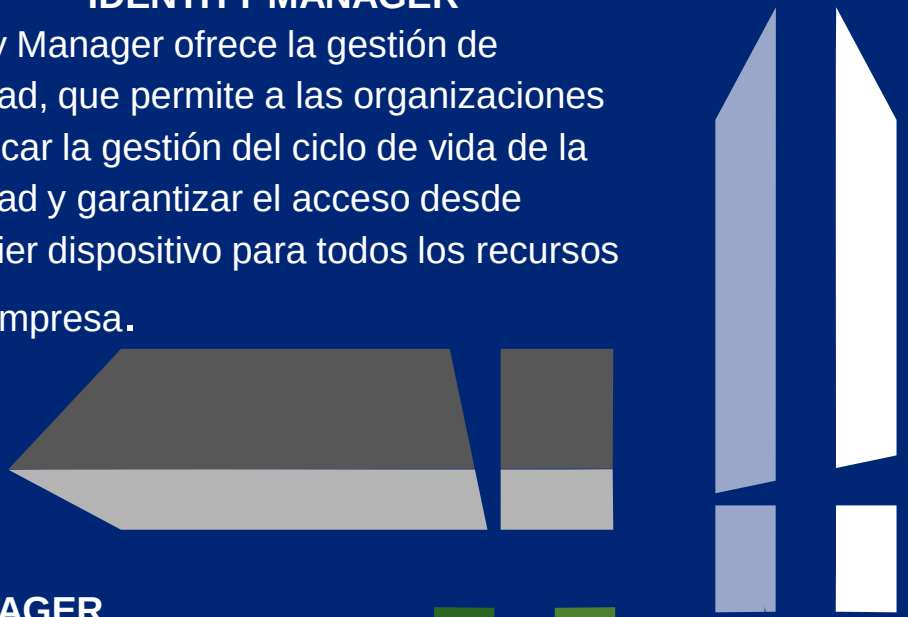
Arquitectura Global de IAM



Módulos IAM

IDENTITY MANAGER

Identity Manager ofrece la gestión de identidad, que permite a las organizaciones simplificar la gestión del ciclo de vida de la identidad y garantizar el acceso desde cualquier dispositivo para todos los recursos de la empresa.



La solución permite a los administradores de IT trabajar en los sistemas de la empresa sin exponer contraseñas administrativas. Específicamente administra, controla y graba todas las actividades de los administradores con privilegios en los distintos ambientes.

USUARIOS PRIVILEGIADOS

ACCESS MANAGER

Es la solución de seguridad encargada de proteger aplicaciones, datos, servicios web y servicios basados en nube. Construido en una arquitectura moderna entrega la flexibilidad para implementar una solución completa brindando autenticación, inicio de sesión único, autorización, federación, inicio de sesión social y móvil, propagación de identidad, y autentificación basada en riesgos y autorización en el perímetro de la red.

GOVERNANCE

Fortalece la gestión de los roles y simplifica el proceso de gestión del ciclo de vida de roles y certificación de acceso. Permite la realización de actividades de descubrimiento de accesos a través de minerías de roles.

Plataforma de Identidades Extendida

- Asegurar las aplicaciones de la Compañía y los datos en los dispositívos móviles.
- Asegurar los servicios de accesos para la Economía de APIs.
- Servicios de identidad para y en la nube.
- Automatización de Identidades y Gobierno Empresarial.

Access Management
Framework General

Authentication

Intelligent Risk Based Authentication

Integrated Strong Authentication

Authorization

Real Time

External Security Policies

Mobile and API

RESTful Interfaces

API Management

Federation

Standards Based

Social

Platform

Common Policy Model

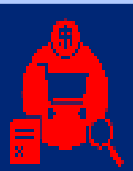
Standards Bases Approach

Scalable High Availability and DR

Authentication Plugin Framework

Cloud Apps

Desktop Apps



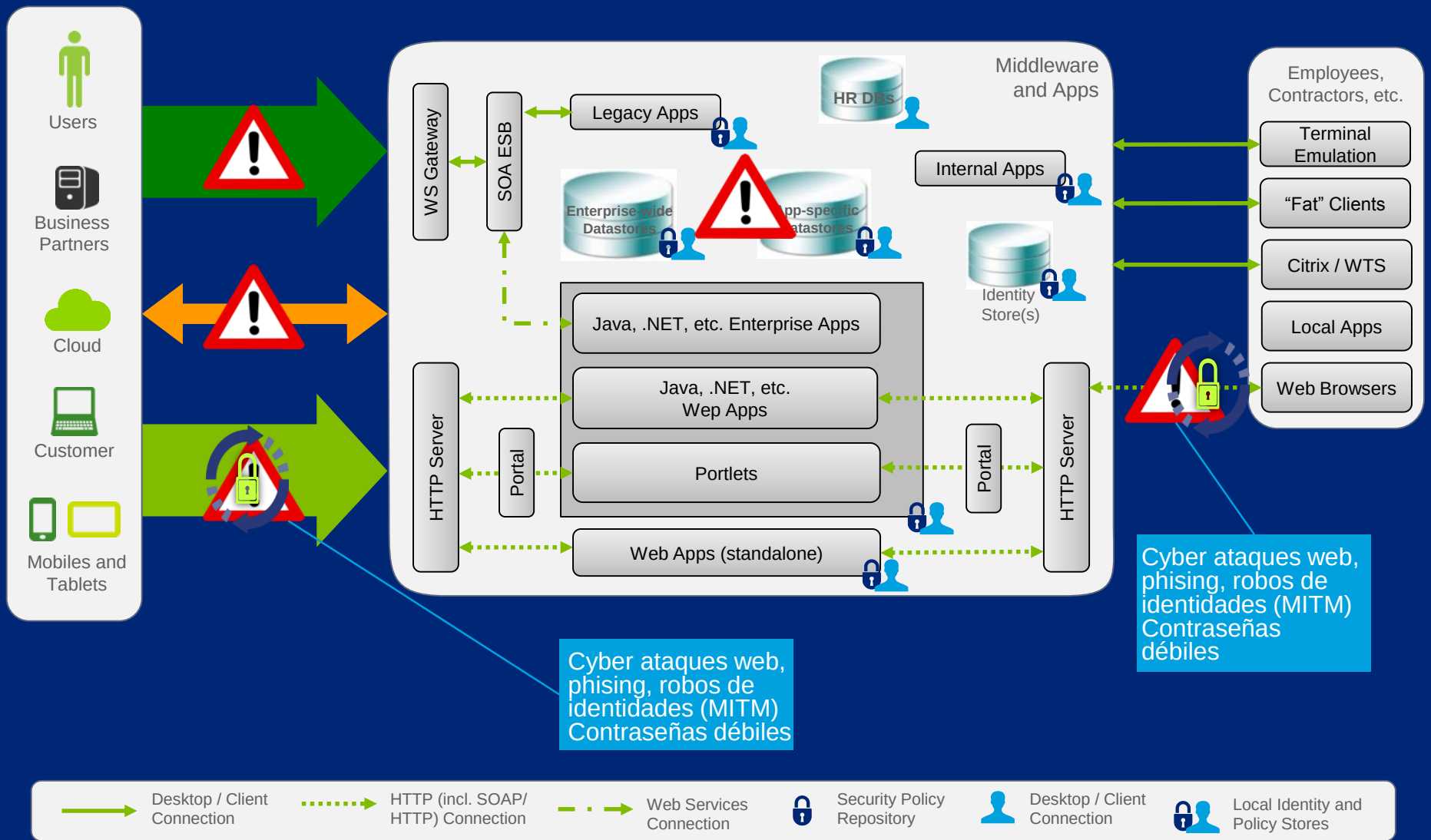
Enterprise Apps

Mobile Apps

Access Management
Características generales

- Simplifica el Web Single Sign On (WebSSO).
- Posibilita mejoras en la autenticación y autorización.
- Administración de Políticas centralizada.
- Administración avanzada de sesiones.
- Administración centralizada de agentes.
- Administración nativa de contraseñas.
- Integración con esquemas de autenticación de Windows.
- Auditoría y registración de eventos.

Tendencia
Autenticación Fuerte y Adaptiva



Access Management
Adaptive Access Management

El acceso adaptativo básicamente permite mejorar los esquemas de autenticación y evitar la ocurrencia de fraudes.

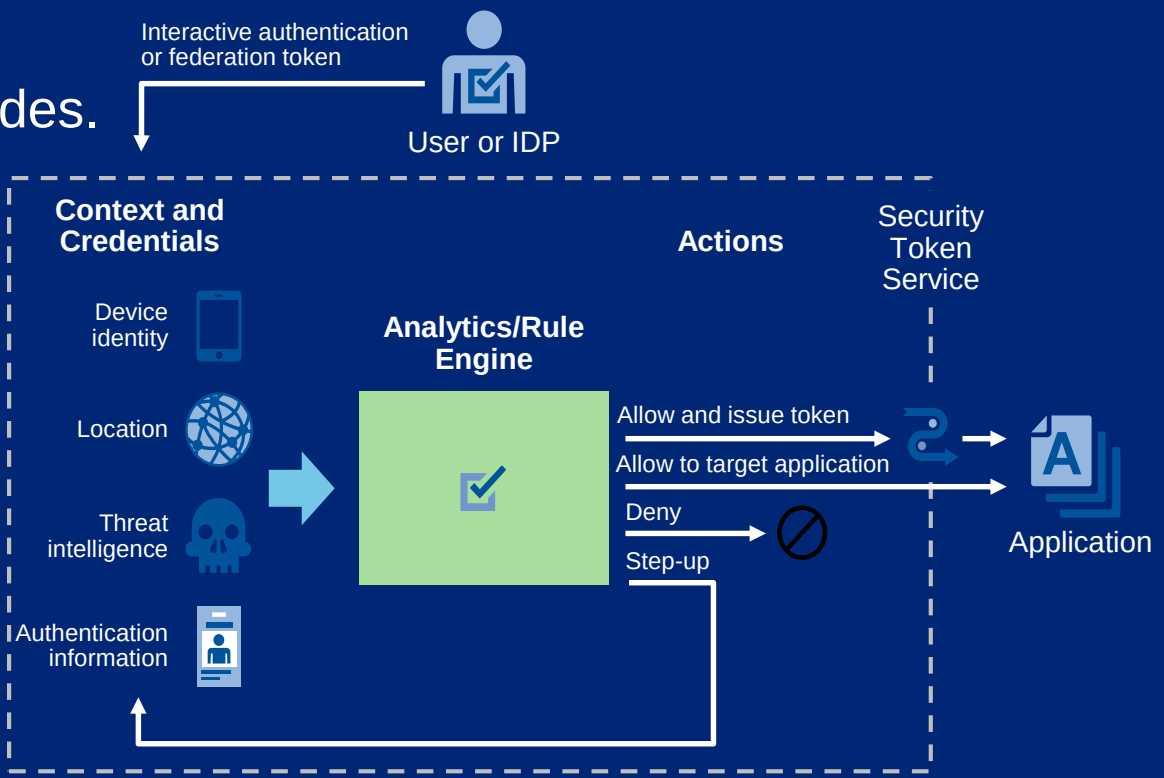
- Incrementa la seguridad en la autenticación de usuarios (dispositivos virtuales, Knowledge-Based Authentication, OTP, device fingerprint, etc).
- Métodos de desafío basados en riesgos.
- Administración de políticas centralizado.
- Análisis y correlación de eventos.
- Integración con IAM.

Acces Management

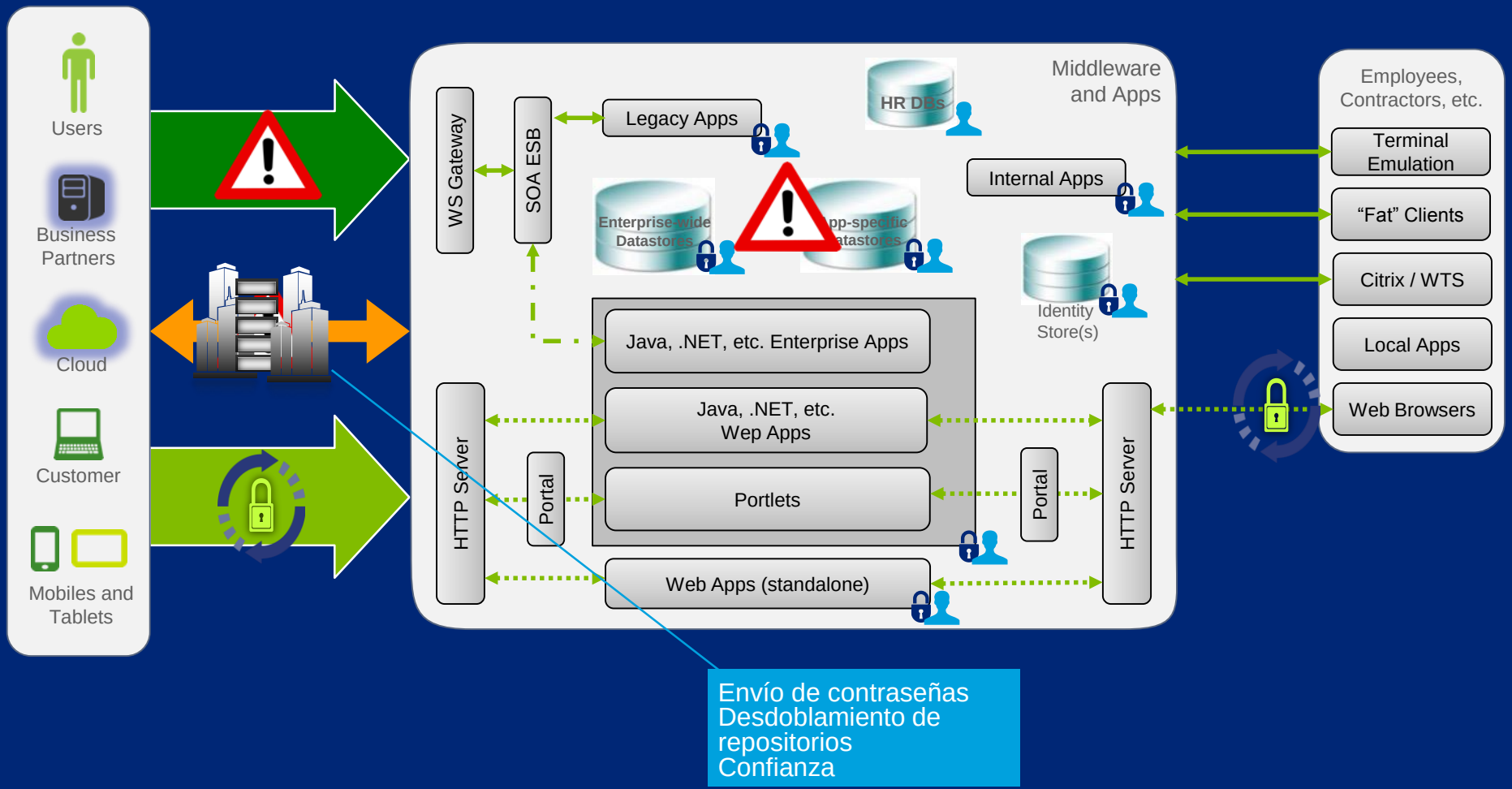
Adaptive Access Management

Otras Características:

- Auto-learning, crea un perfil base del usuario y detecta anomalías en base al mismo.
- Motor de Políticas configurable.
- Herramienta de análisis de fraudes.
- Tableros de indicadores.
- Disparador de alarmas.
- Reportes.



Federación



Access Management

Federación

Permite autenticar usuarios entre distintos dominios y/o compañías a través de tokens o “assertions”, sin tener que exponer las contraseñas o todos los atributos de la identidades.

Permite compartir algunos atributos entre distintos dominios/Compañías

Identity Provider	Service Provider
• Autentica a los usuarios • Mantiene la custodia de las identidades • Comparte atributos de la identidad (opcionalmente)	• Acepta tokens o assertions del IP • También se lo denomina Relying Partner • Permite el ingreso a la aplicación

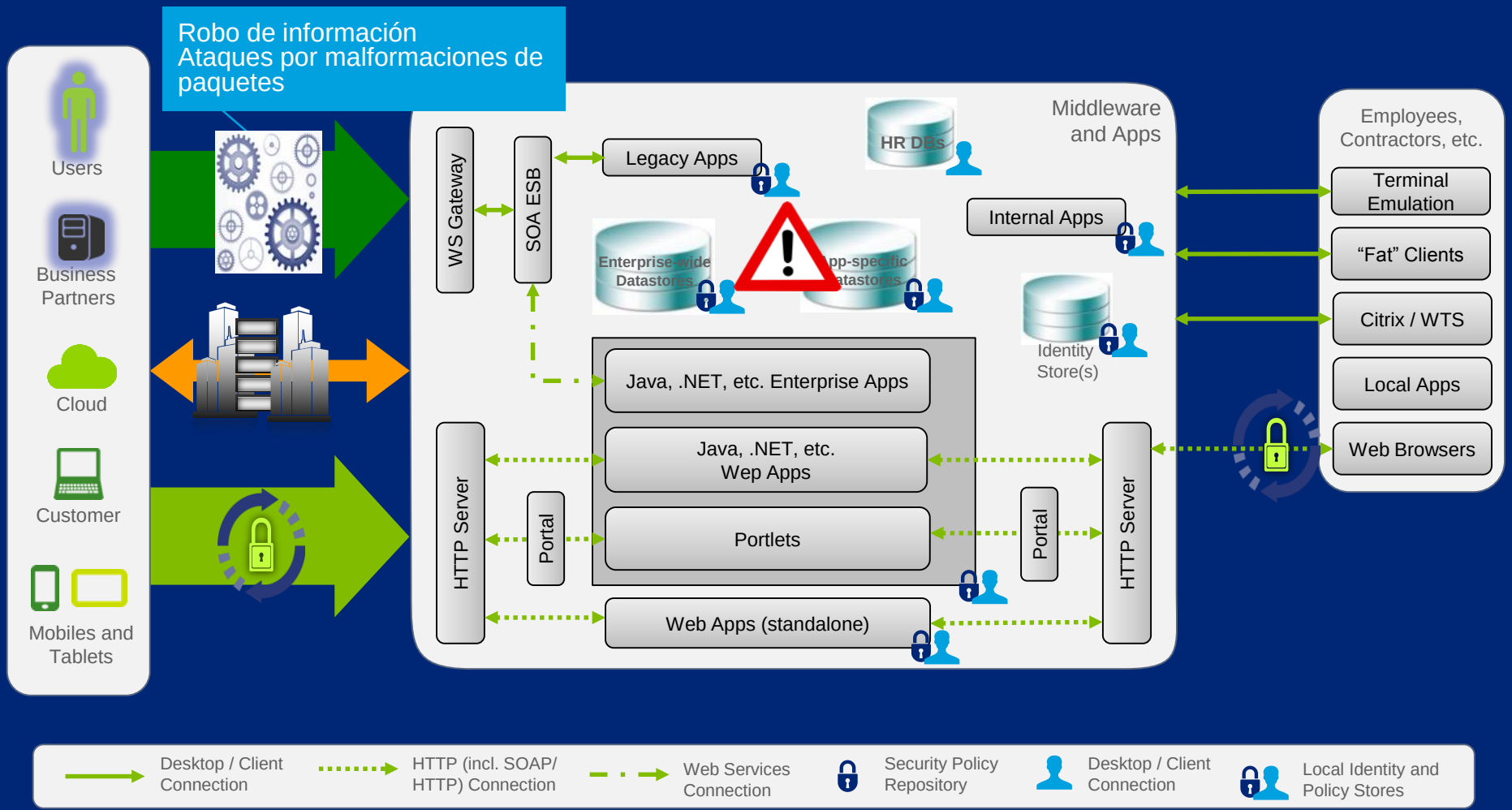
Access Management

Federación

Beneficios
• Facilidad para los usuarios (sso) • Minimizar los costos de administración de usuarios. • Permitir nuevos negocios y aplicaciones. • Integración con Socios de Negocio. • Mitigar riesgos.

Limitaciones
• Cumplimiento. • Aplicaciones y protocolos existentes. • Estructuras Organizacionales. • Capacidades del Socio de Negocio.

API Management
Tendencia



Acces Management
Seguridad en APIs

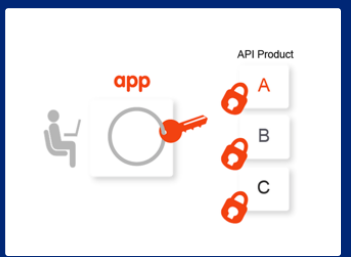
Los vectores de ataque más comunes pueden dividirse en las siguientes tres categorías:

Parámetros

- Explotan los datos enviados dentro de las APIs, incluyen URL, parámetros de querys, HTTP Headers, y/o contenido POST.

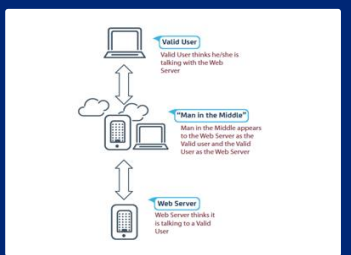
Identidad

- Explotan las debilidades en la autenticación, la autorización y registro y seguimiento de sesiones.



Man-in-the-middle

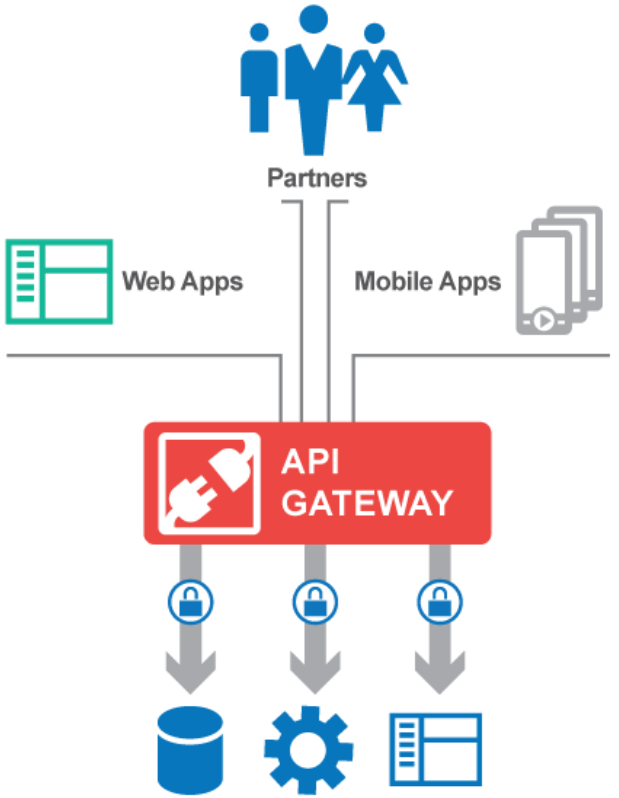
- Interceptan mensajes legítimos de transacciones y explotan los datos que no se encuentran firmados y/o encriptados.



Acces Management

API Gateway Security

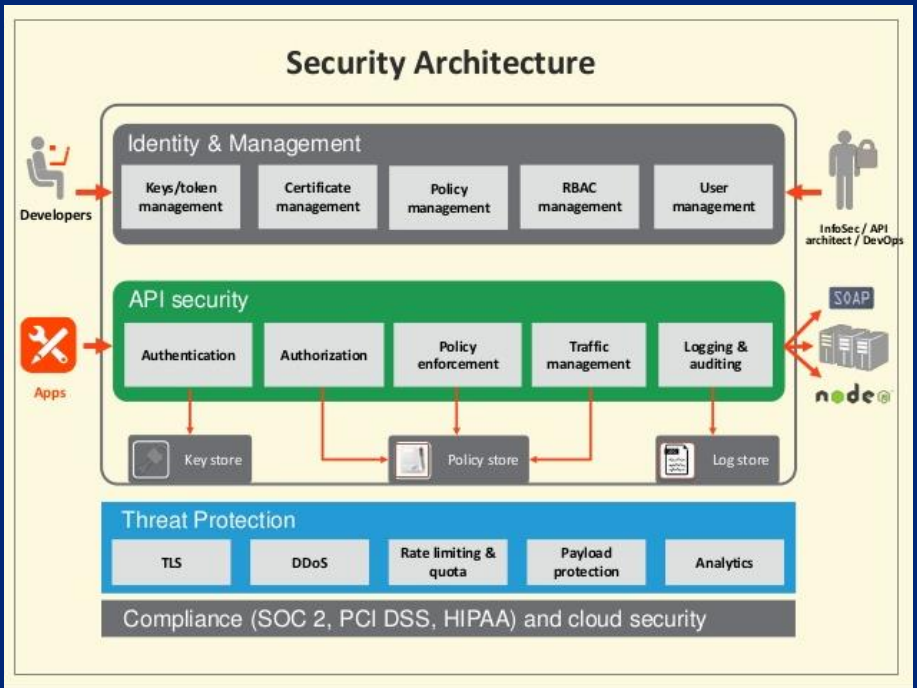
Permite la administración, desarrollo, implementación y operación de APIs incrementando la seguridad y el cumplimiento regulatorio a través de capacidades de autenticación, autorización y auditoría. Posibilita a las Compañías estandarizar las APIs y el servicio de entrega con seguridad, performance y alta disponibilidad.



Acces Management

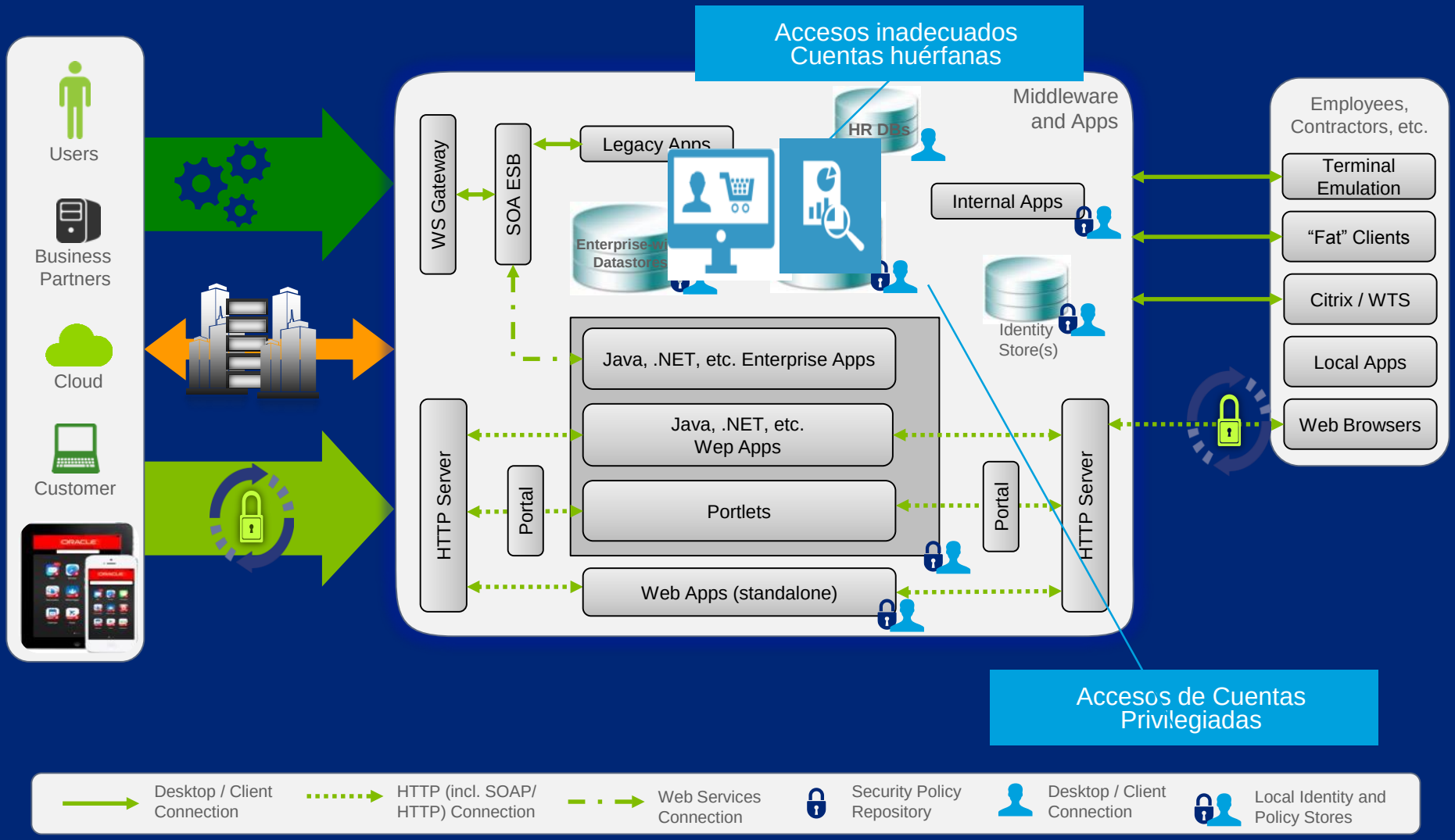
API Gateway Security

Características:



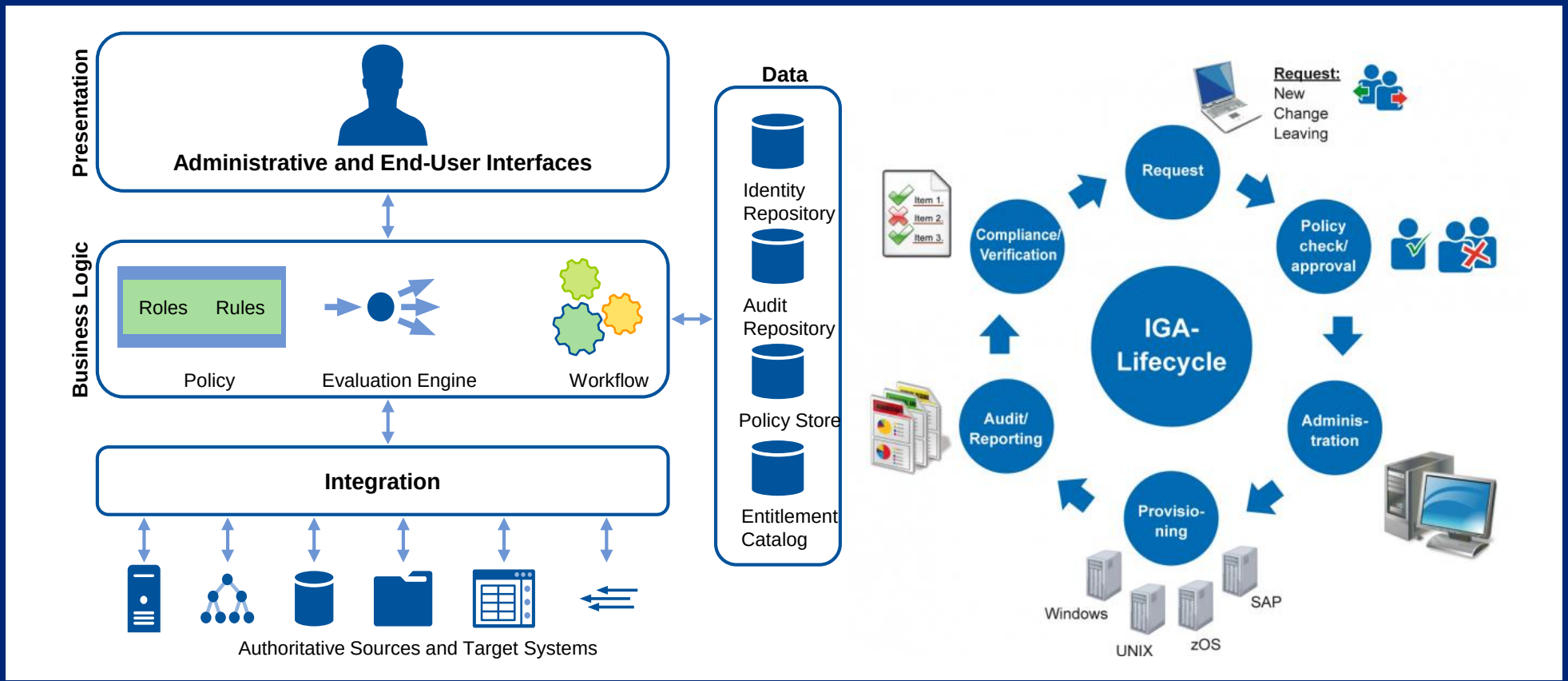
- Autenticación y autorización (protocolos como SAML, Oauth, XACML, etc.)
- Securización de los mensajes (SSL, encripción.)
- Protección ante ataques (DoS, mensajes malformados, sqlinjection, etc.)
- Orquestación, mediación y transformación de mensajes.
- Integración con servicios de cloud, mobile e identidades sociales.
- Análisis y monitoreo.

Identity Governance



Identity Manager
Funcionalidad

Identity Manager automatiza la administración de los usuarios en los recursos de la Compañía. Permite administrar todo el ciclo de vida de las personas, desde el ingreso hasta la salida.



Identity Manager
Principales Características

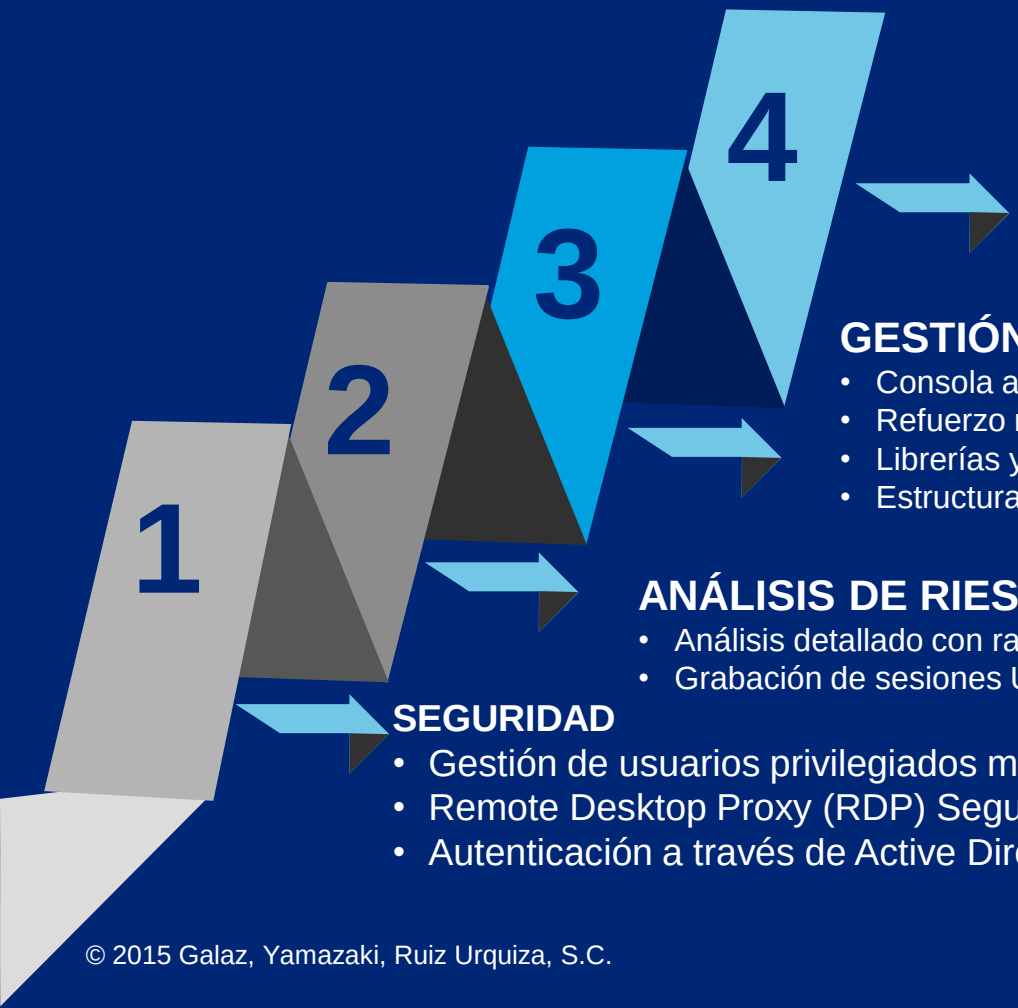
1. **Repositorio central de identidades**
2. **Autogestión (contraseñas y accesos)**
3. **Conectores**
4. **Workflows de autorización**

Role Management
Principales Características

- **Ciclo de vida de roles**
- **Minería de roles**
- **Segregación de funciones**
- **Certificación de accesos**

Usuarios privilegiados

Mediante las siguientes funcionalidades, la solución de gestión de usuarios privilegiados permite conocer las actividades realizadas por usuarios con privilegios administrativos en los recursos de la empresa:



AUDITORIA Y REPORTES
- Servicio de auditoría de Windows.
- Filtrado automático de datos para cumplimiento continuo.
- Notificaciones automáticas.
- Flujos de trabajo.
- Restricciones ACL.

GESTIÓN DE POLÍTICAS
- Consola administrativa WEB.
- Refuerzo mediante políticas y grupos de WINDOWS.
- Librerías y comandos reutilizables.
- Estructura de reglas heredada.

ANÁLISIS DE RIESGO
- Análisis detallado con rating de riesgo por código y color.
- Grabación de sesiones UNIX, Linux y Windows.

SEGURIDAD
- Gestión de usuarios privilegiados multiplataforma.
- Remote Desktop Proxy (RDP) Seguro.
- Autenticación a través de Active Directory y LDAP.

- Las Compañías y sus CxO están luchando batallas de **larga duración**, con **múltiples frentes de ataques** y donde la **victoria es difícil de medir.** Para tener alguna oportunidad de ganar estas CyberGuerras, como CxO se deben entender determinadas realidades…

Cyber Seguridad
Realidades

1. **SU RED DE INFORMACIÓN VA A SER COMPROMETIDA**
   Desafortunadamente, es inevitable que su Cía. sea atacada. Si opera una red de información, no es posible tener cero riesgo y 100% de seguridad.

2. **LA SEGURIDAD FÍSICA Y LA CYBERSEGURIDAD SE ENCUENTRAN MUY VINCULADAS**
   Mientras que amenazas como espionaje, robo de propiedad intelectual, fraudes, ciberterrorismo pueden involucrar filtraciones de seguridad, las mismas pueden originarse con un acceso físico.

3. **LOS DAÑOS POR CYBER RIESGOS VAN MÁS ALLÁ DE LO ECONÓMICO**
   Mientras que el costo promedio de una filtración de seguridad puede estar bien documentado, los efectos a largo plazo sobre la reputación de la Compañía y la Marca pueden incrementar dicho costo. Muchas Compañías están considerando la contratación de Cyber Seguros para limitar dichos costos.

4. **TODO NO PUEDE SER PROTEGIDO DE LA MISMA FORMA**
   Después de todo, cada pieza de información no es de la misma importancia. Se debe crear una categorización o jerarquía de la información de manera personalizada para la Compañía y la industria. Y en dicho proceso son los CFOs' quienes pueden tomar mejores decisiones respecto de cómo priorizar las protecciones y monitoreos.

5. **LAS DEFENSAS PROBABLEMENTE SON SUFICIENTES**
   Las Cías. continúan invirtiendo fuertemente en el aspecto de la protección de la CyberSeguridad (más FW, IDS, etc) . Las protecciones son probablemente tan buenas como se necesitan pero los hackers pueden que ya se hayan infiltrado. Se debe focalizar más en la detección y monitoreo de ataques y sus respuestas y resiliencia.

¡Muchas gracias!

Deloitte.