IBM Security Forum

Soluções para um ambiente seguro

Segurança de informação com Gerenciamento de Identidades e acessos Uma poderosa combinação

Alisson Lara Resende de Campos
Certified IT Specialist – Tivoli Security Solutions
acampos@br.ibm.com

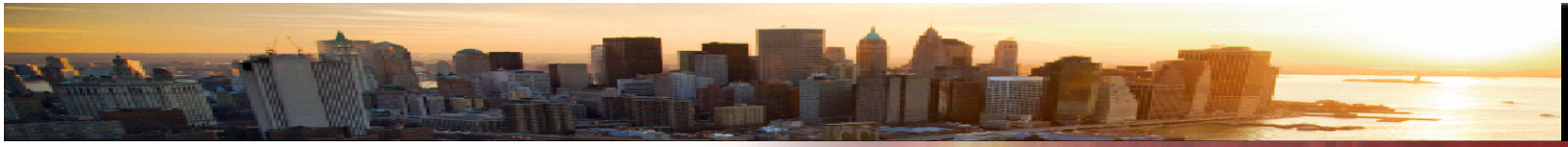
Agenda

Estratégia de segurança da IBM - objetivos

Desafios, motivação

Conceitos de IAM e o que endereça (4 As)

Soluções de segurança da IBM

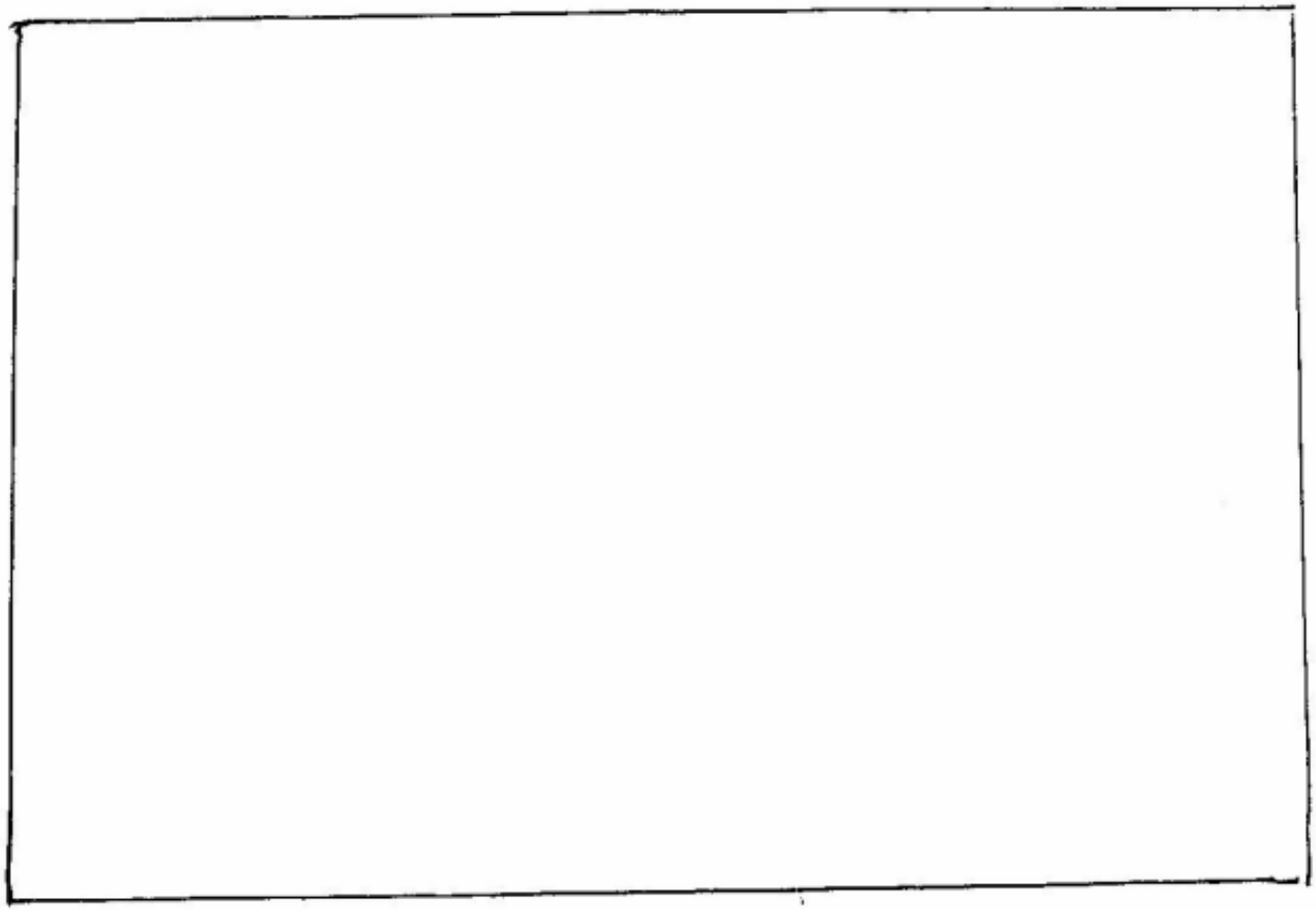


End to End Security

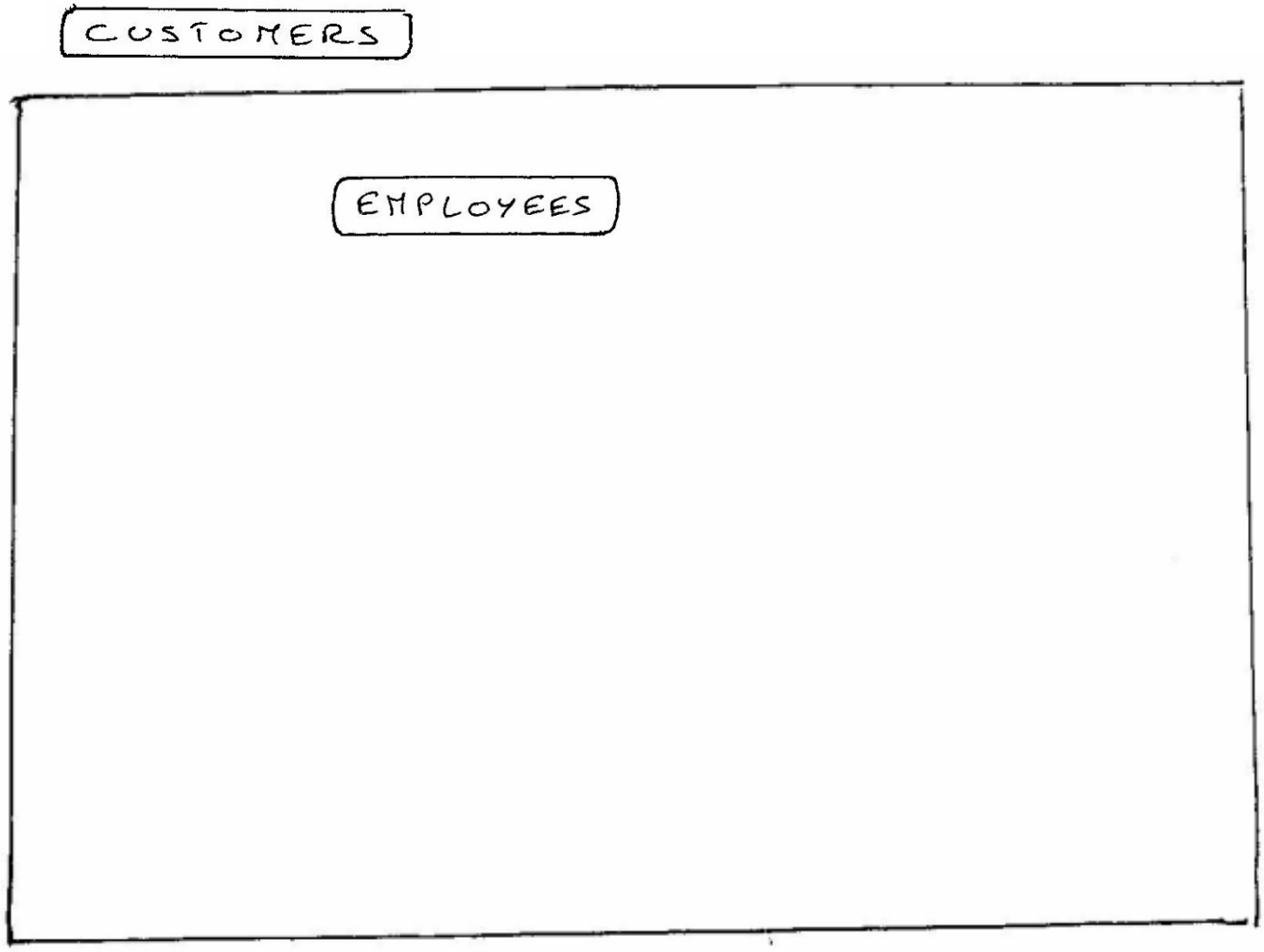
A Visão da IBM é de uma segurança tratada de forma integrada, de ponta a ponta, em todos os níveis onde a informação possa estar sob risco.

Desta forma o objetivo das nossas soluções é proteger a organização

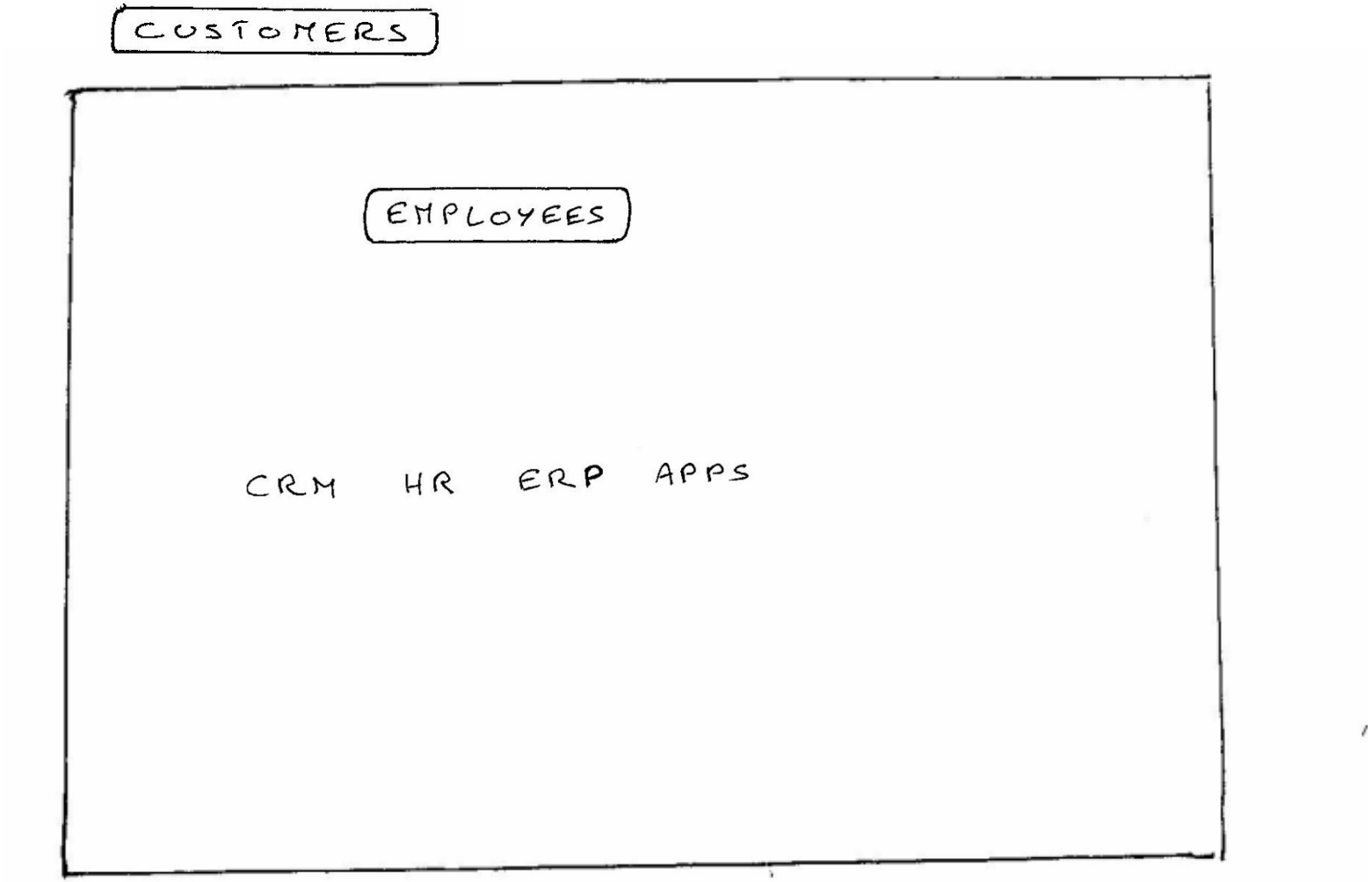
ORGANIZATION



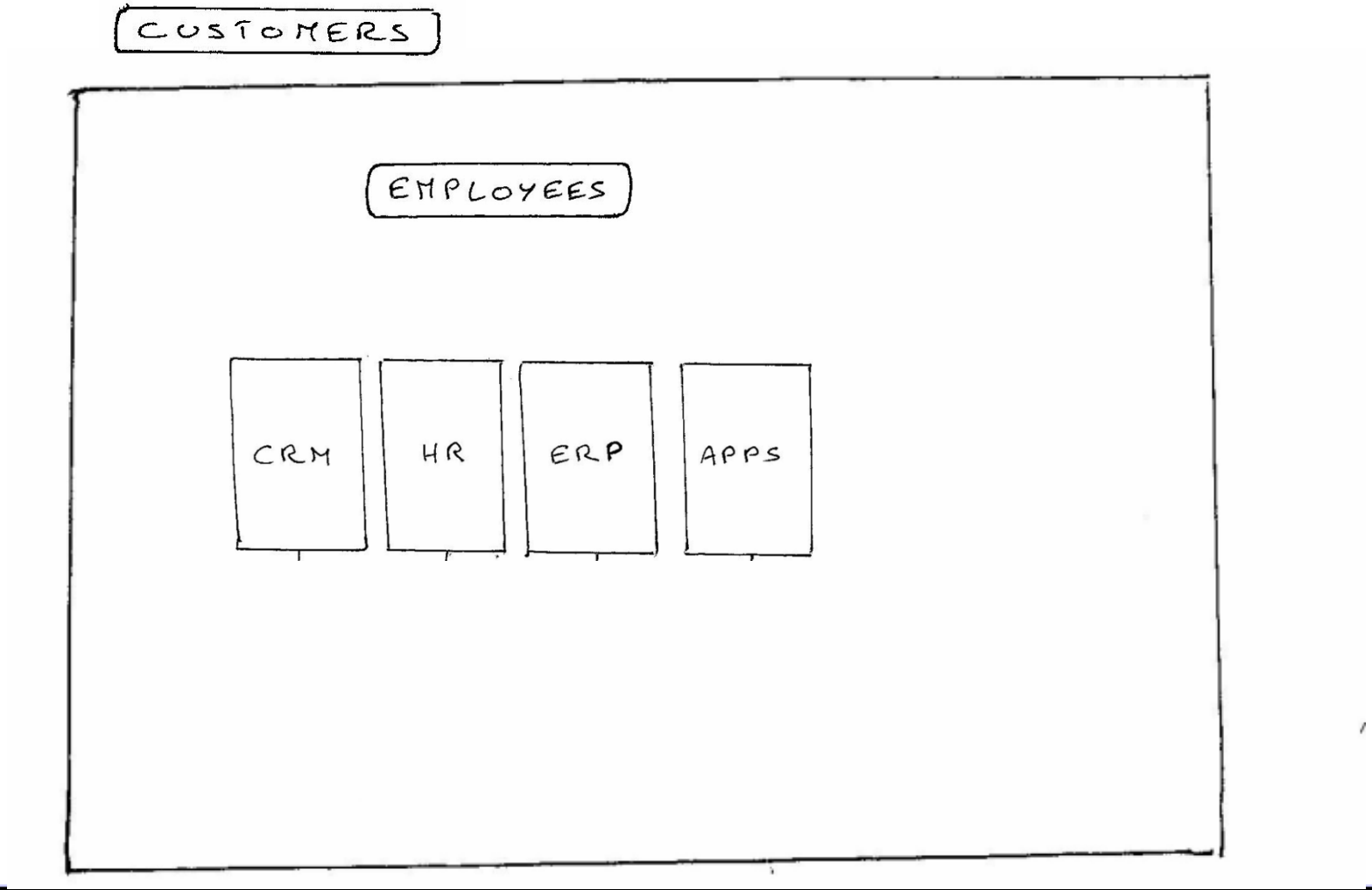
As quais possuem clientes e funcionários



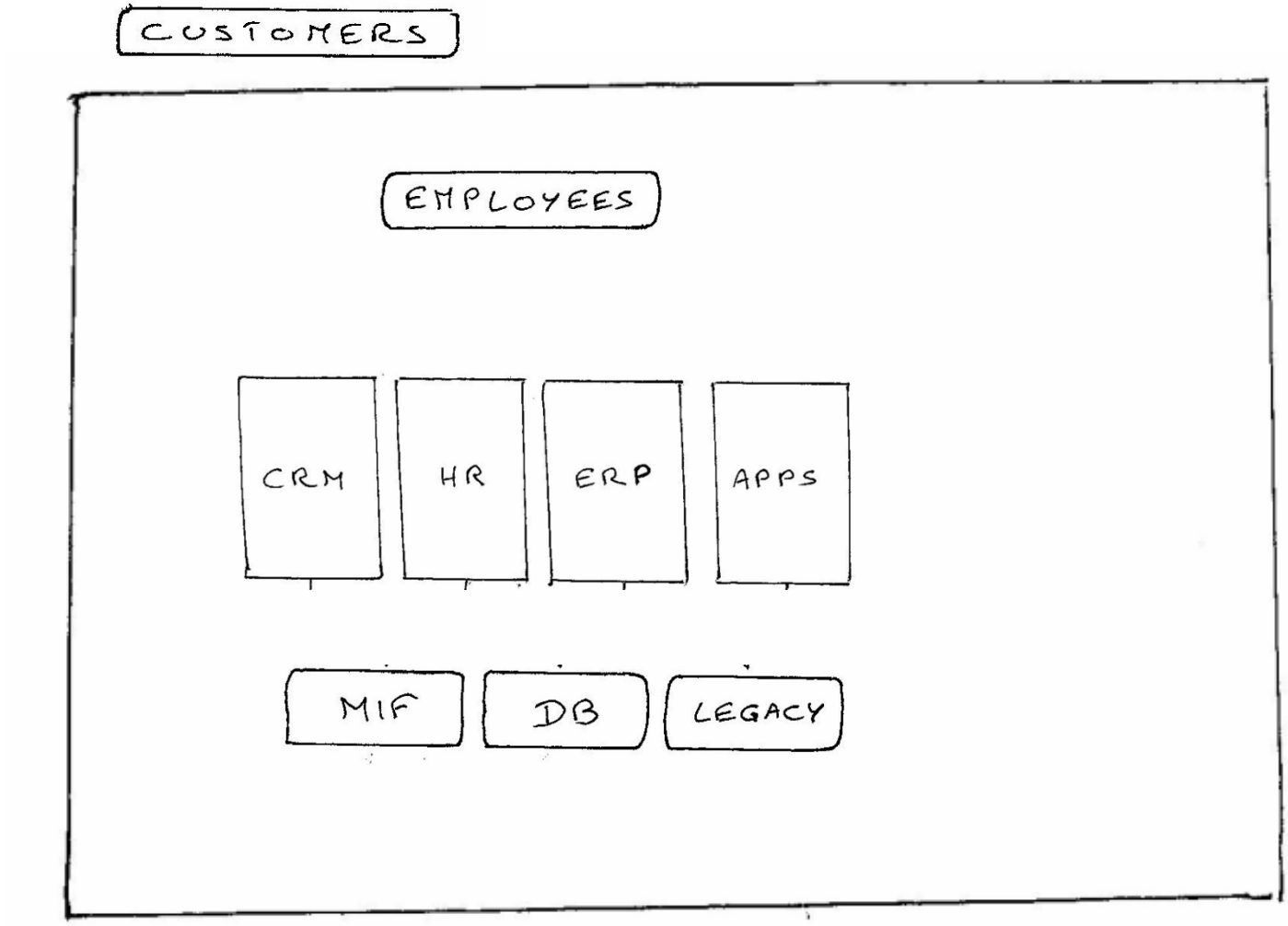
Acessando aplicações



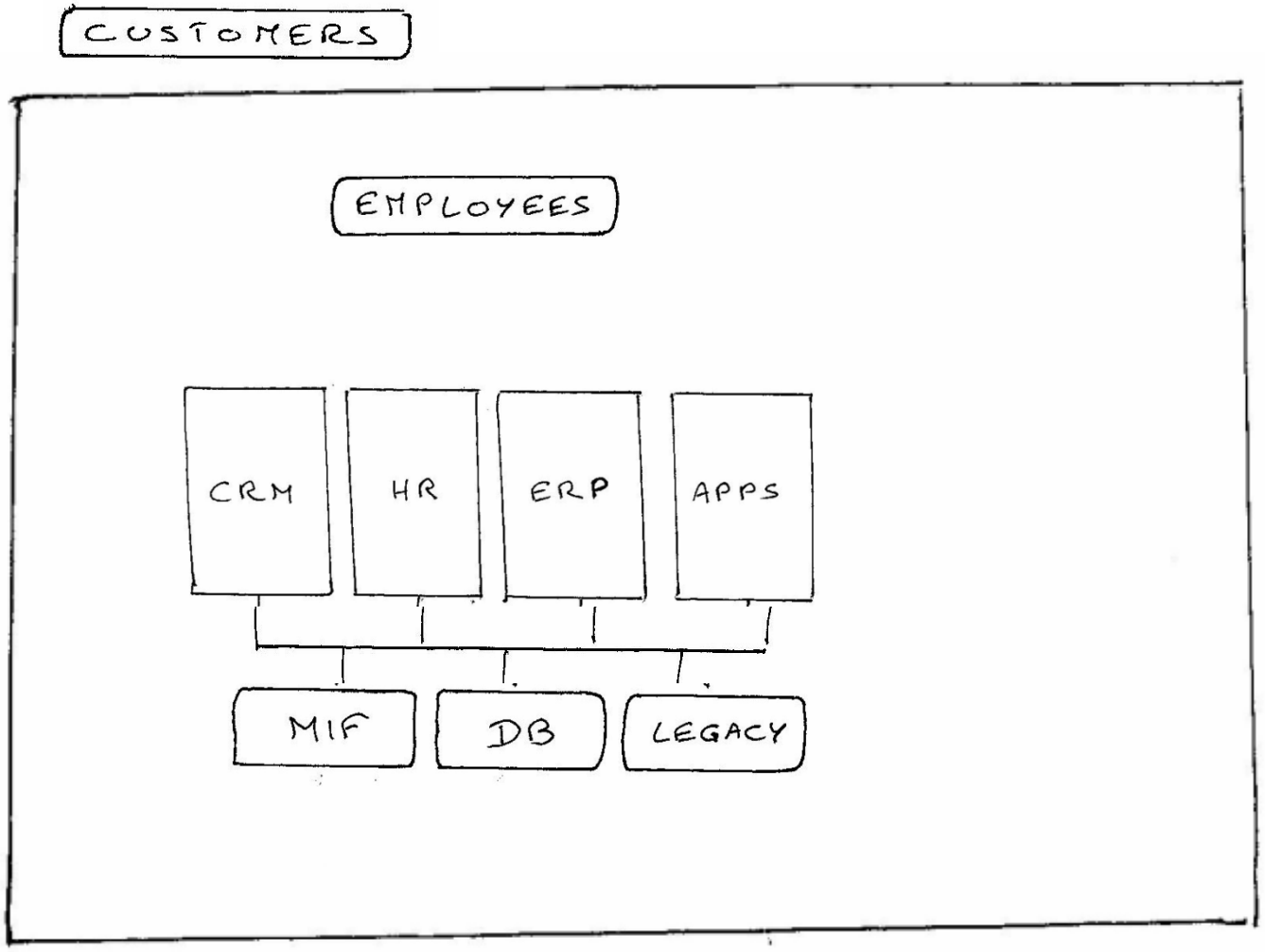
Residindo em sistemas críticos

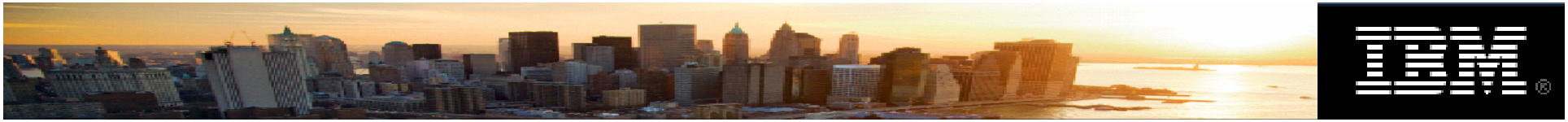


Que fazem uso corporativo de assets

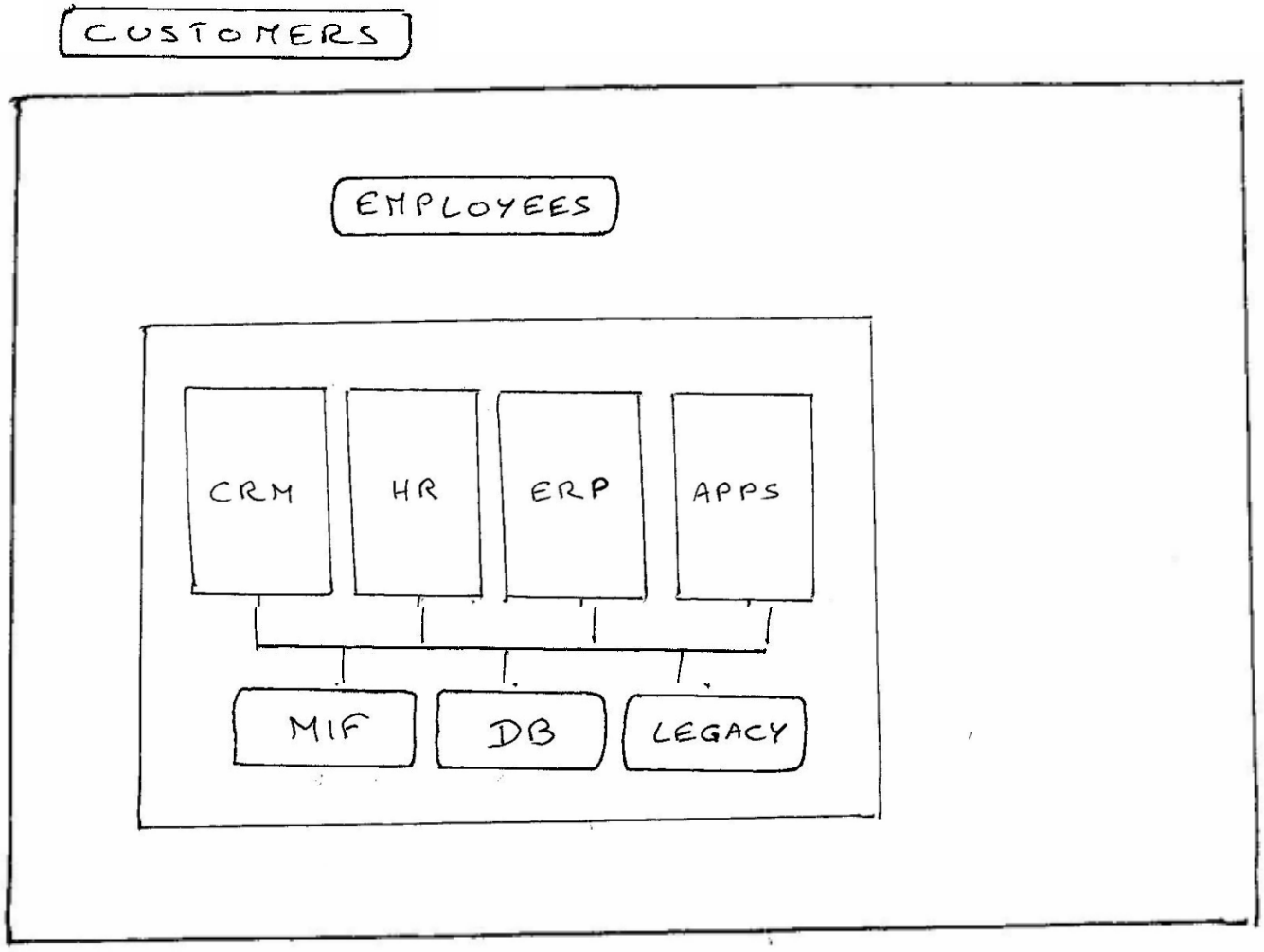


Através de rede ou Enterprise Service Bus

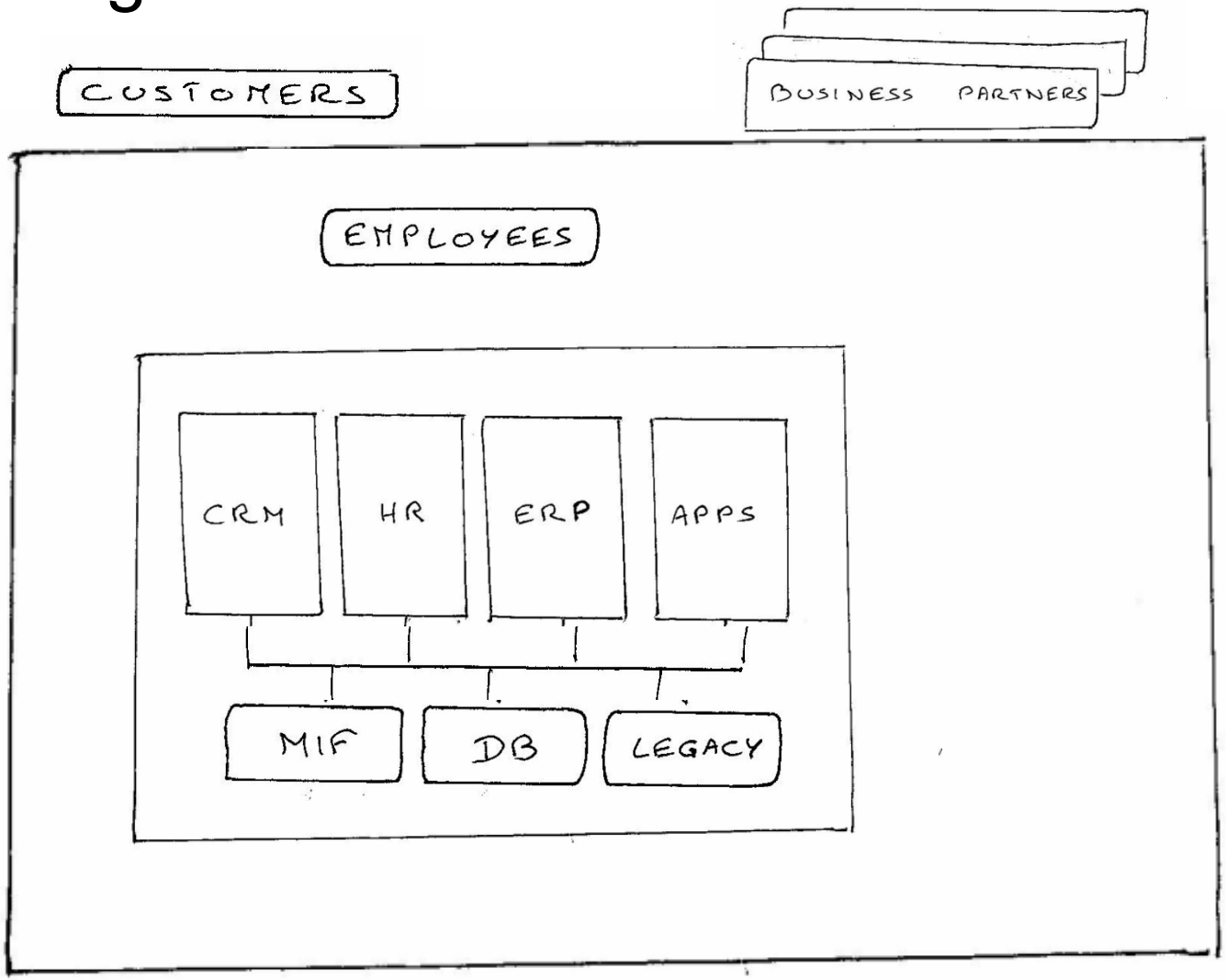




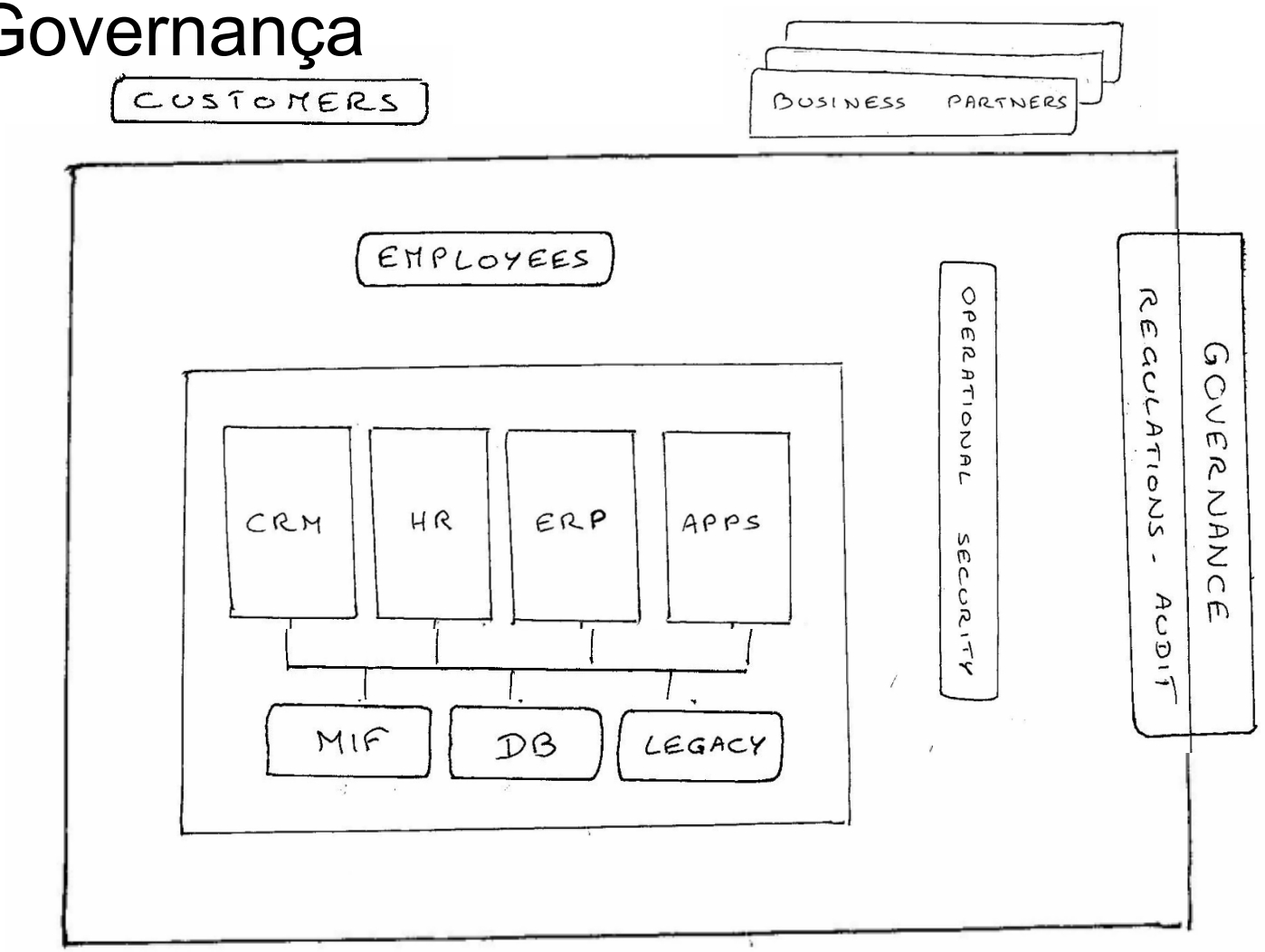
Em um data center



Interagindo com Business Partners



Levando em consideração controles, auditoria e Governança



Agenda

Estratégia de segurança da IBM - objetivos

Desafios, motivação

Conceitos de IAM e o que endereça (4 As)

Soluções de segurança da IBM

O mundo é mais perigoso do que costumava ser

Massive insider breach at DuPont
February 15, 2007
By: Larry Greenemeier

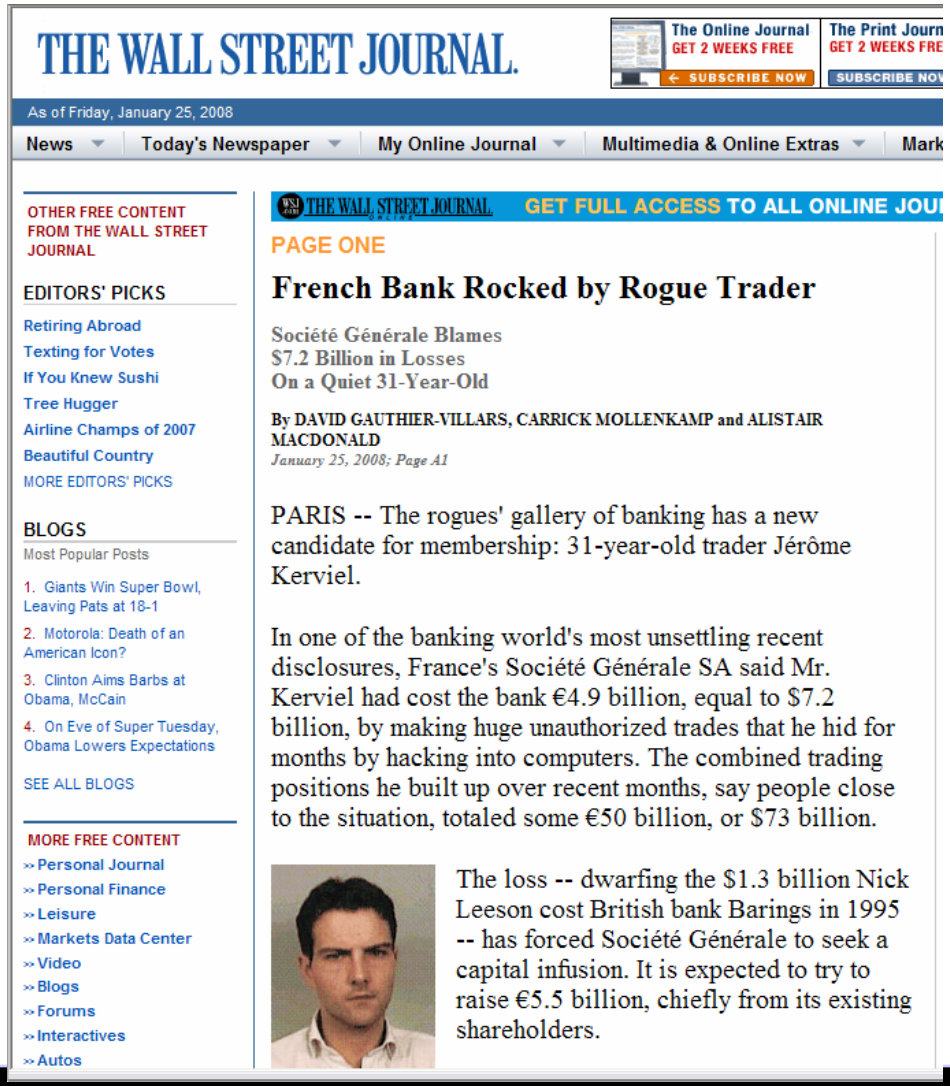
TJX data breach: At 45.6M card numbers, it's the biggest ever
March 29, 2007
By: Jaikumar Vijayan
COMPUTERWORLD

Blackberry outage widespread
February 14, 2007
By Marcia Walton
CNN

Black Friday Turns Servers Dark at Walmart, Macy's
November 25, 2006
By: Evan Schuman
eWEEK

Bill would punish retailers for leaks of personal data
February 22, 2007
By Joseph Pereira
THE WALL STREET JOURNAL.

Ameaça interna – a mais perigosa!



THE WALL STREET JOURNAL.

The Online Journal GET 2 WEEKS FREE ← SUBSCRIBE NOW | The Print Journ GET 2 WEEKS FRE SUBSCRIBE NOV

As of Friday, January 25, 2008

News | Today's Newspaper | My Online Journal | Multimedia & Online Extras | Mark

OTHER FREE CONTENT FROM THE WALL STREET JOURNAL

EDITORS' PICKS

Retiring Abroad
Texting for Votes
If You Knew Sushi
Tree Hugger
Airline Champs of 2007
Beautiful Country
MORE EDITORS' PICKS

BLOGS

Most Popular Posts

1. Giants Win Super Bowl, Leaving Pats at 18-1
2. Motorola: Death of an American Icon?
3. Clinton Aims Barbs at Obama, McCain
4. On Eve of Super Tuesday, Obama Lowers Expectations

SEE ALL BLOGS

MORE FREE CONTENT

- Personal Journal
- Personal Finance
- Leisure
- Markets Data Center
- Video
- Blogs
- Forums
- Interactives
- Autos

THE WALL STREET JOURNAL. GET FULL ACCESS TO ALL ONLINE JOU

PAGE ONE

French Bank Rocked by Rogue Trader

Société Générale Blames
$7.2 Billion in Losses
On a Quiet 31-Year-Old

By DAVID GAUTHIER-VILLARS, CARRICK MOLLENKAMP and ALISTAIR MACDONALD
January 25, 2008; Page A1

PARIS -- The rogues' gallery of banking has a new candidate for membership: 31-year-old trader Jérôme Kerviel.

In one of the banking world's most unsettling recent disclosures, France's Société Générale SA said Mr. Kerviel had cost the bank €4.9 billion, equal to $7.2 billion, by making huge unauthorized trades that he hid for months by hacking into computers. The combined trading positions he built up over recent months, say people close to the situation, totaled some €50 billion, or $73 billion.

The loss -- dwarfing the $1.3 billion Nick Leeson cost British bank Barings in 1995 -- has forced Société Générale to seek a capital infusion. It is expected to try to raise €5.5 billion, chiefly from its existing shareholders.

O problema:

- 3 grandes ameaças:
  - Erros de funcionários
  - Vazamento de informação
  - Sabotagem interna
- Fraudes internas custam US$600 Bi anualmente nos EUA

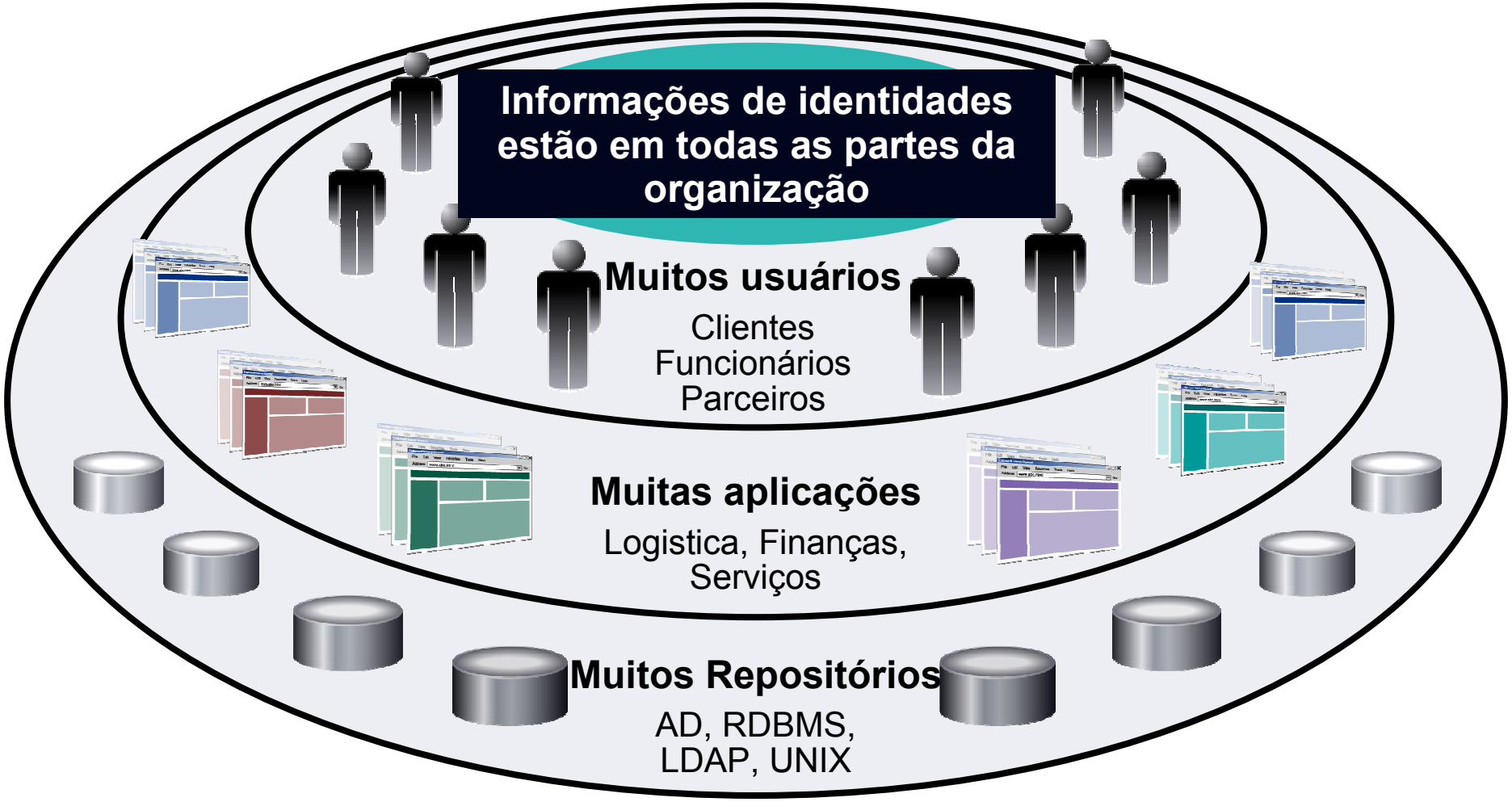
Como gerenciar:

- Maior visibilidade de contas e acessos de usuários privilegiados
- Melhorar os controles de identidades
- Automatizar o monitoramento e a auditoria

O Que é um Risco?

- Sua Marca
- Propriedade Intelectual
- Exposições Legal e Regulatória
- Informações de Clientes
- Confiança do Cliente
- Custo de Remediação
- Interrupção de Negócios
- Seu Emprego

Riscos pela complexidade de ambientes



Risco pela fragmentação

Customers

Employees

Partners

	Customer Self-Service	E-Commerce	CRM	ERP	HR	Partner Extranet	SCM
Security Layer	J_Doe 1211960	John Doe A23JJ4	John Doe	PKI Cert	John_D	Johnd	Mobile Phone
Application Layer	IBM	bea	SIEBEL	SAP	PEOPLESoft	Microsoft	ORACLE
User Store	SunONE LDAP	SQL 2000	LDAP	Oracle OID	Oracle RDBMS	Active Directory	Oracle
Operating System	Sun microsystems	Microsoft		IBM	hp invent	Microsoft	hp invent

Risco pelo gerenciamento de senhas

Tempo & Dinheiro

- Usuários frustados e reclamações relacionadas a várias senhas e complexas
- Empregados sem acesso interrompem o trabalho afetando a produtividade
- Custos associados a tarefas de reset de senhas

Segurança

- Vulnerabilidade devido ao uso de senhas fracas e falta de gerenciamento
- Dificuldade de prover segurança para aplicações críticas
- Dificuldade para integrar mecanismos avançados de autenticação nas aplicações

Regulamentações

- Necessidade de proteger dados privados e manter registros de todos os acessos para auditoria

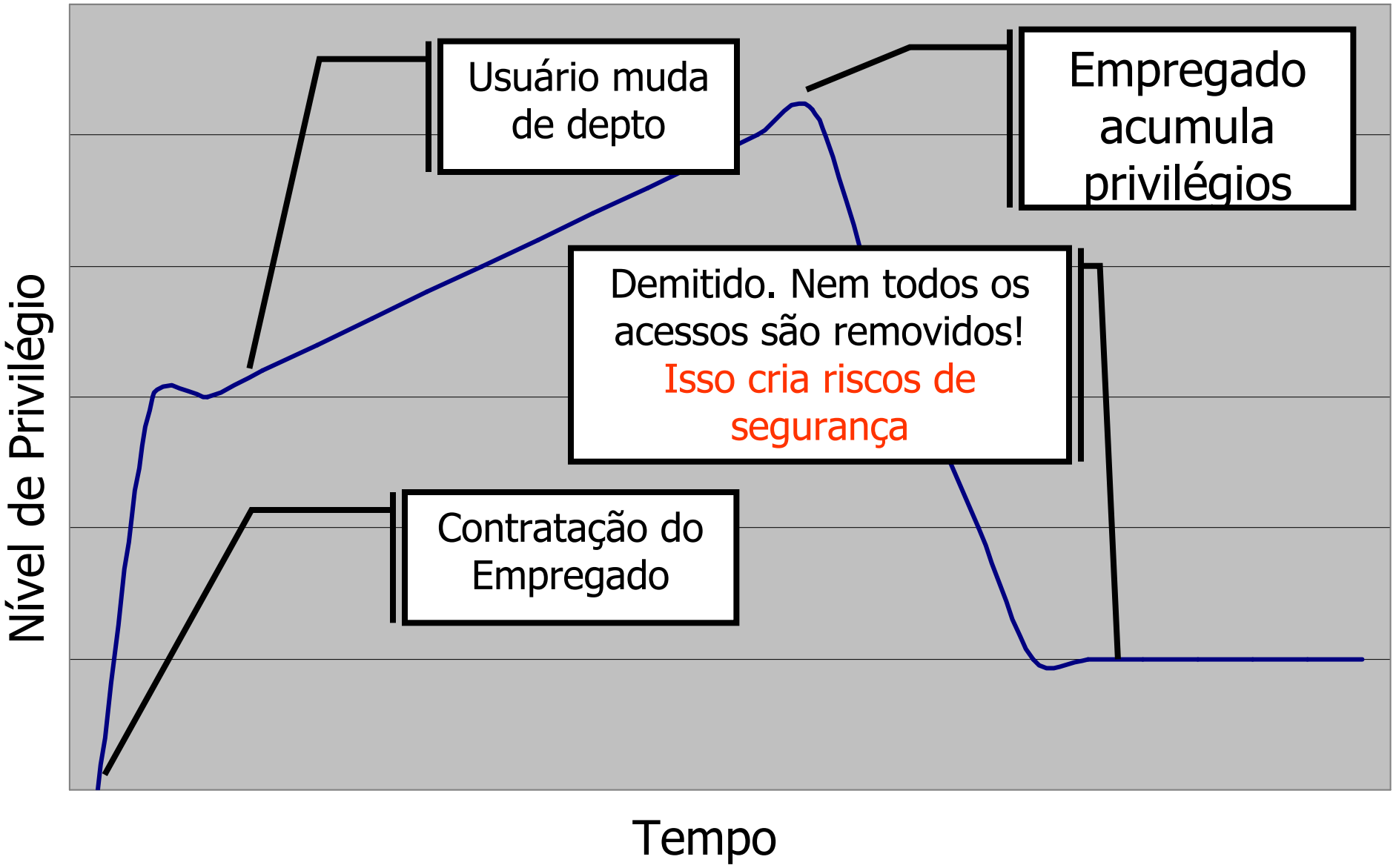
Falta de segregação

- O Administrador de Sistemas pode ver as informações dos pacientes !
- O operador de backup pode ver o *business plan* !
- O *Logging* de auditoria e as soluções de segurança podem ser desligadas !

Sys Admin

Servers

Risco pelo acumulo de privilégios



SARBOX (Seção 404)

Improper Change Management

- Lack of formal program change procedure
- Lack of understanding of system configurations
- Oversight of changes and review of change logs

Insufficient Segregation of Duties

- NOT JUST Separation of requestor, approver, implementer --Separation of developers and operators

Excessive Access to Systems / Databases

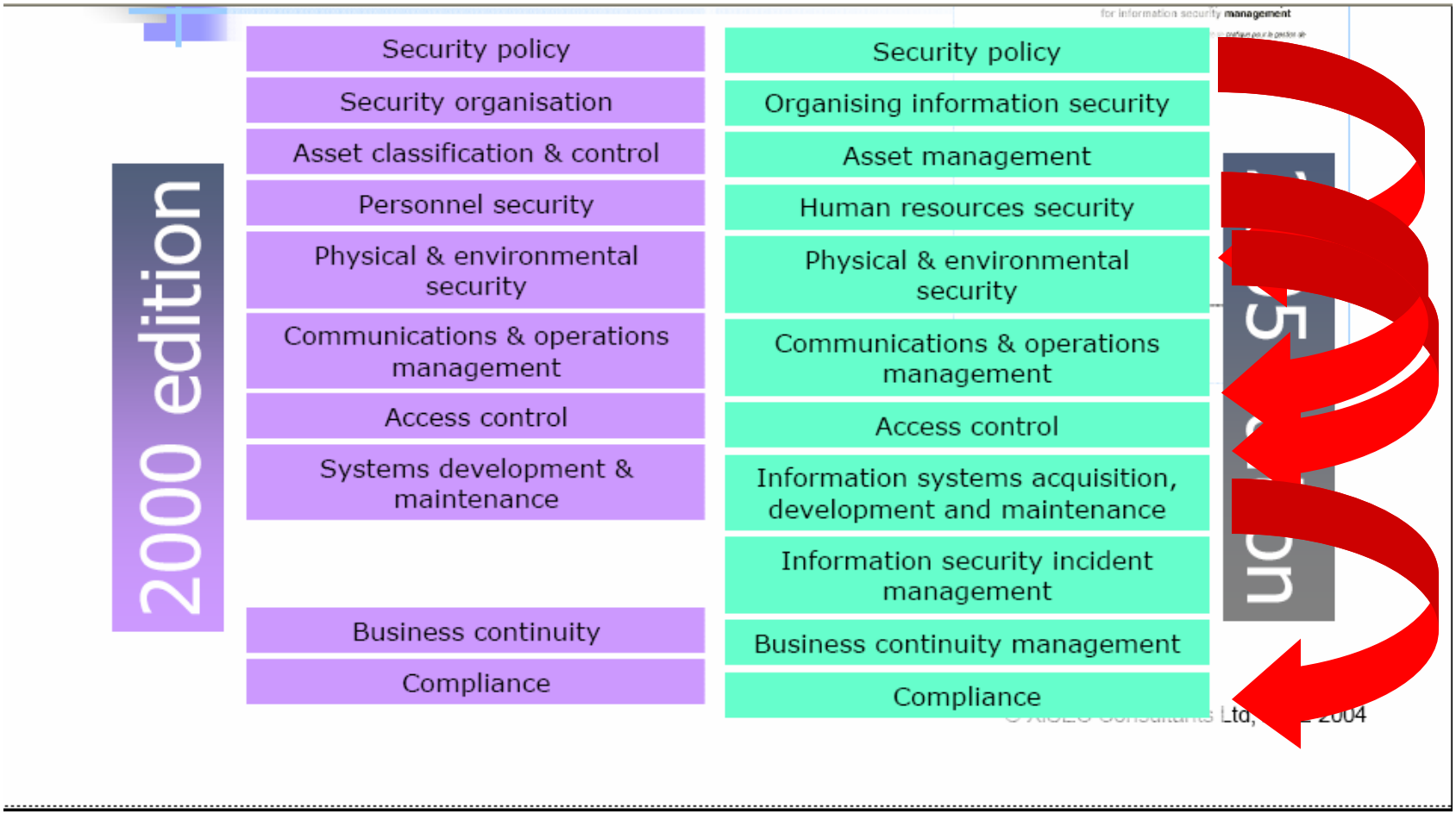
- Developer / programmer / DBA /Admin access to production environment
- Developer / programmer DBA /Admin access to production data

Lack of Access Controls

- User provisioning and administration
  - Changes in responsibilities
  - Changes in organization
  - Terminations
- No documented access policies and standards

Lack of general monitoring of the security infrastructure

IAM na ISO-27002



PCI-DSS

Construa e Mantenha uma Rede Segura	
1.	Instale e mantenha uma configuração de firewall para proteger os dados do portador de cartão
2.	Não use as senhas padrão de sistema e outros parâmetros de segurança fornecidos pelos prestadores de serviços.
Proteja os Dados do Portador de Cartão	
3.	Proteja os dados armazenados do portador de cartão
4.	Codifique a transmissão dos dados do portador de cartão nas redes públicas e abertas
Mantenha um Programa de Administração de Vulnerabilidades	
5.	Use e atualize regularmente o software ou programas antivírus
6.	Desenvolva e mantenha sistemas e aplicativos seguros
Implemente Medidas Rígidas de Controle de Acesso	
7.	**Restrinja o acesso aos dados do portador de cartão a apenas aqueles que necessitam conhecê-los para a execução dos trabalhos**
8.	**Atribua um ID único para cada pessoa que possua acesso ao computador**
9.	Restrinja o acesso físico aos dados do portador de cartão
Acompanhe e Teste Regularmente as Redes	
10.	Acompanhe e monitore todo o acesso aos recursos da rede e dados do portador de cartão
11.	Teste regularmente os sistemas e processos de segurança
Mantenha uma Politica de segurança	
12.	Mantenha uma política que atenda à segurança da informação para funcionários e prestadores de serviços

Agenda

Estratégia de segurança da IBM - objetivos

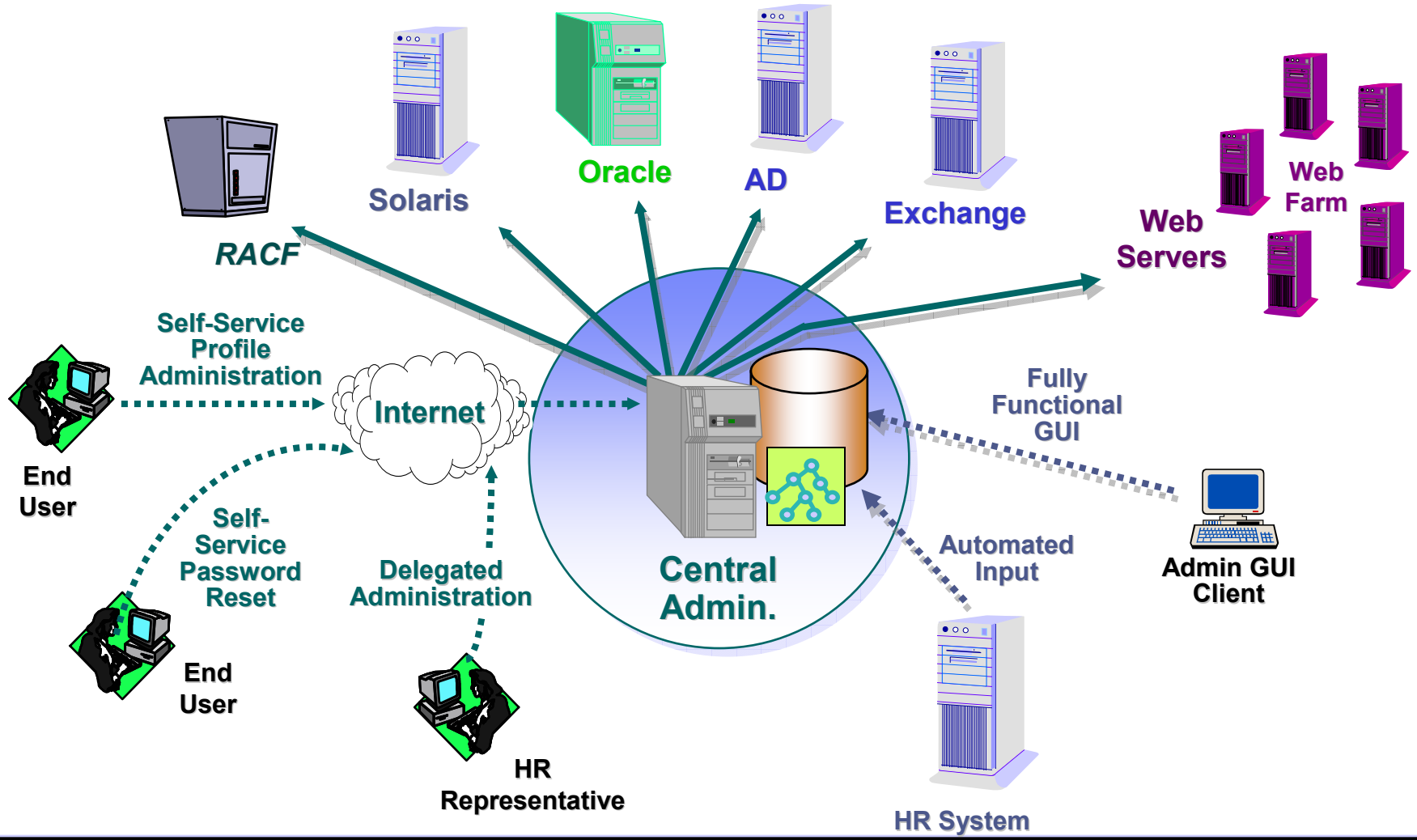
Desafios, motivação

Conceitos de IAM e o que endereça (4 As)

Soluções de segurança da IBM

Administração

Gerenciando Identidades



Feed e Workflow

Marge Greene
Director, Human Resources

HR System

HR Data Passed to Admin

Admin Maps Job to Roles

Admin

Access & Accounts Created

Audit

Access Control

IBM-RACF

Oracle

SAP

WINAD

MS Exchange

Sun Solaris

Portal

IBM AIX

WORK FLOW PROCESS

Procurement

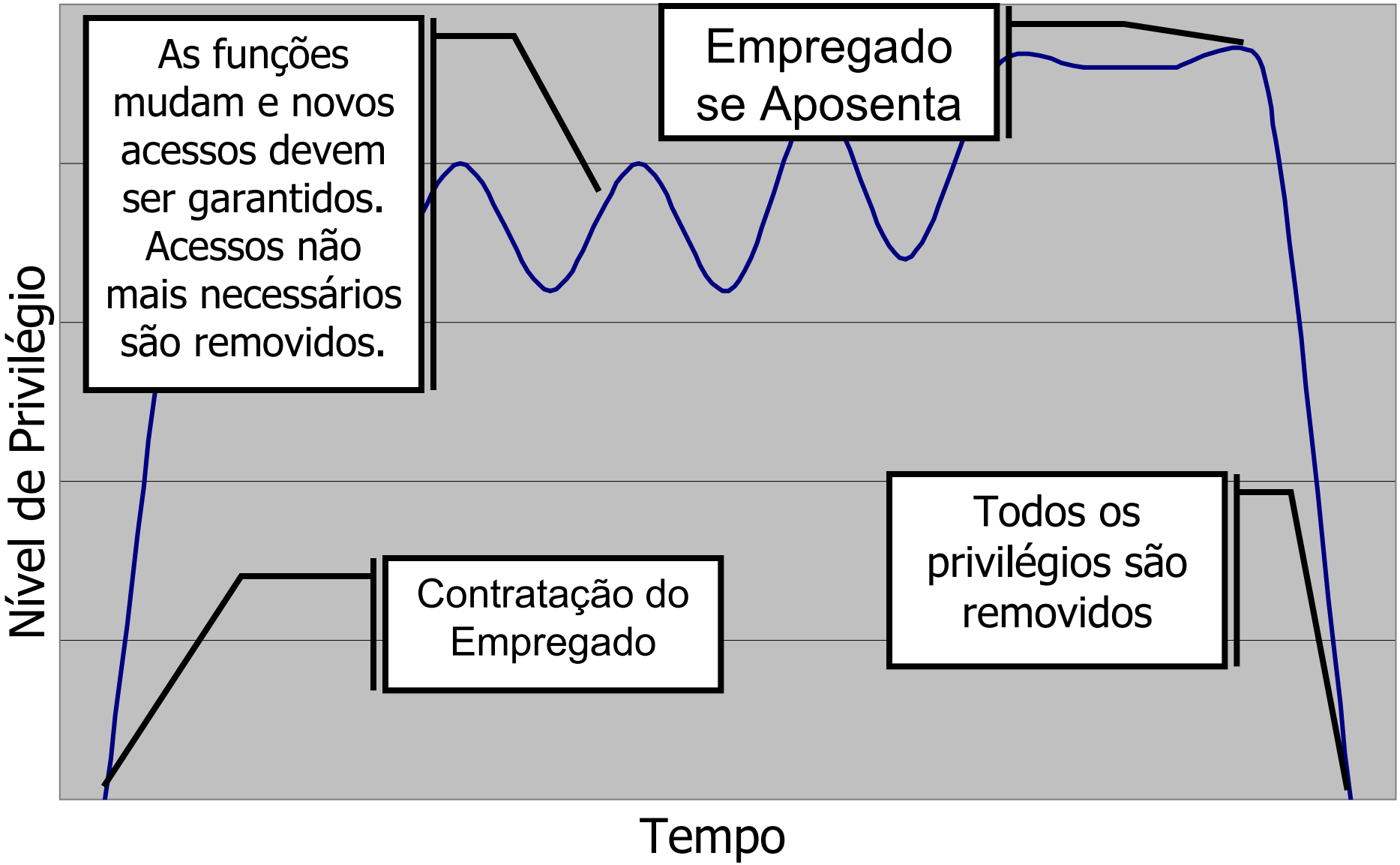
Facilities

Department Manager Gives - OK

New Hire

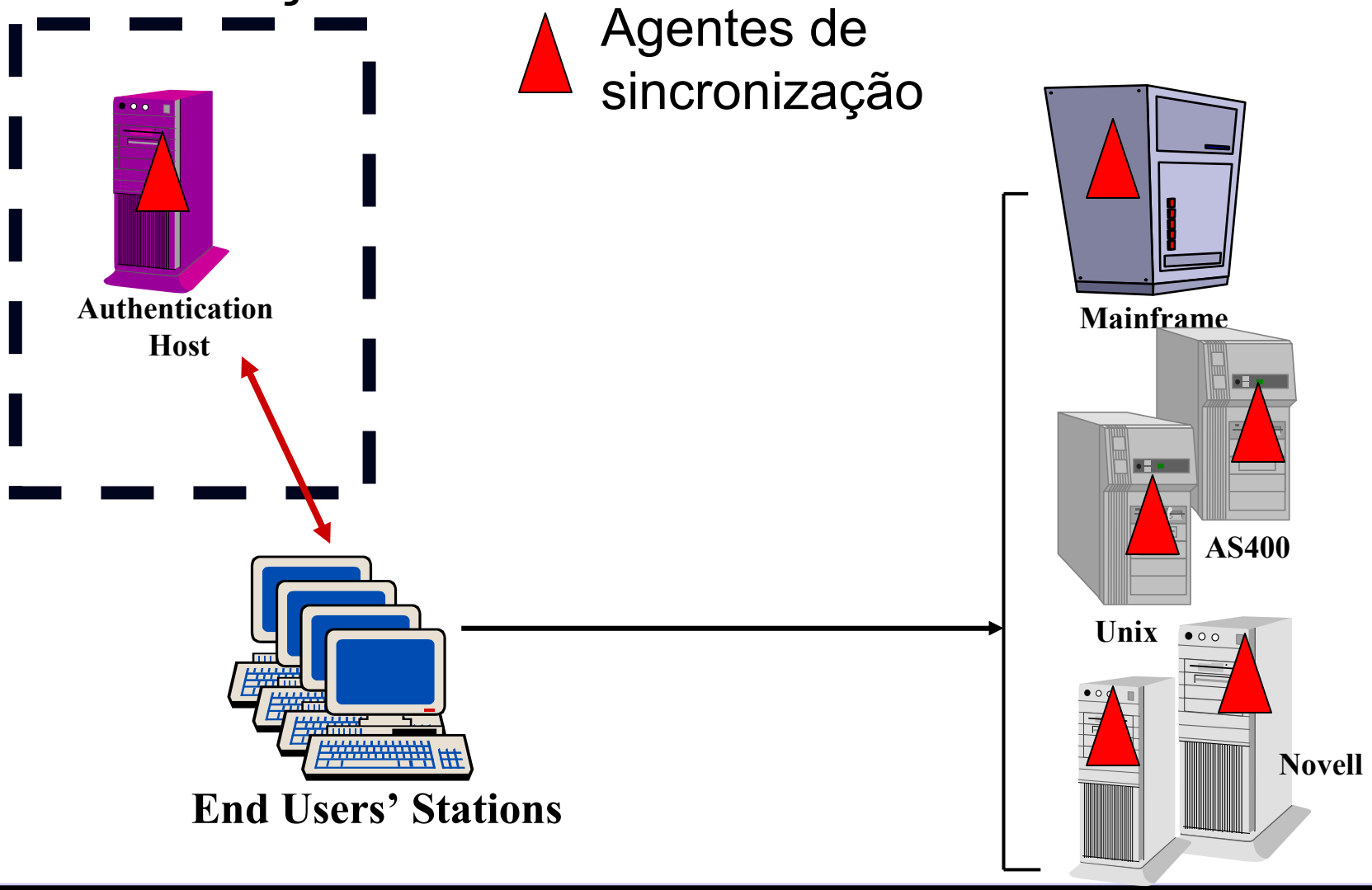
Robert Stone
EVP, Sales
New Division

Ciclo de Vida com Gestão de Identidades

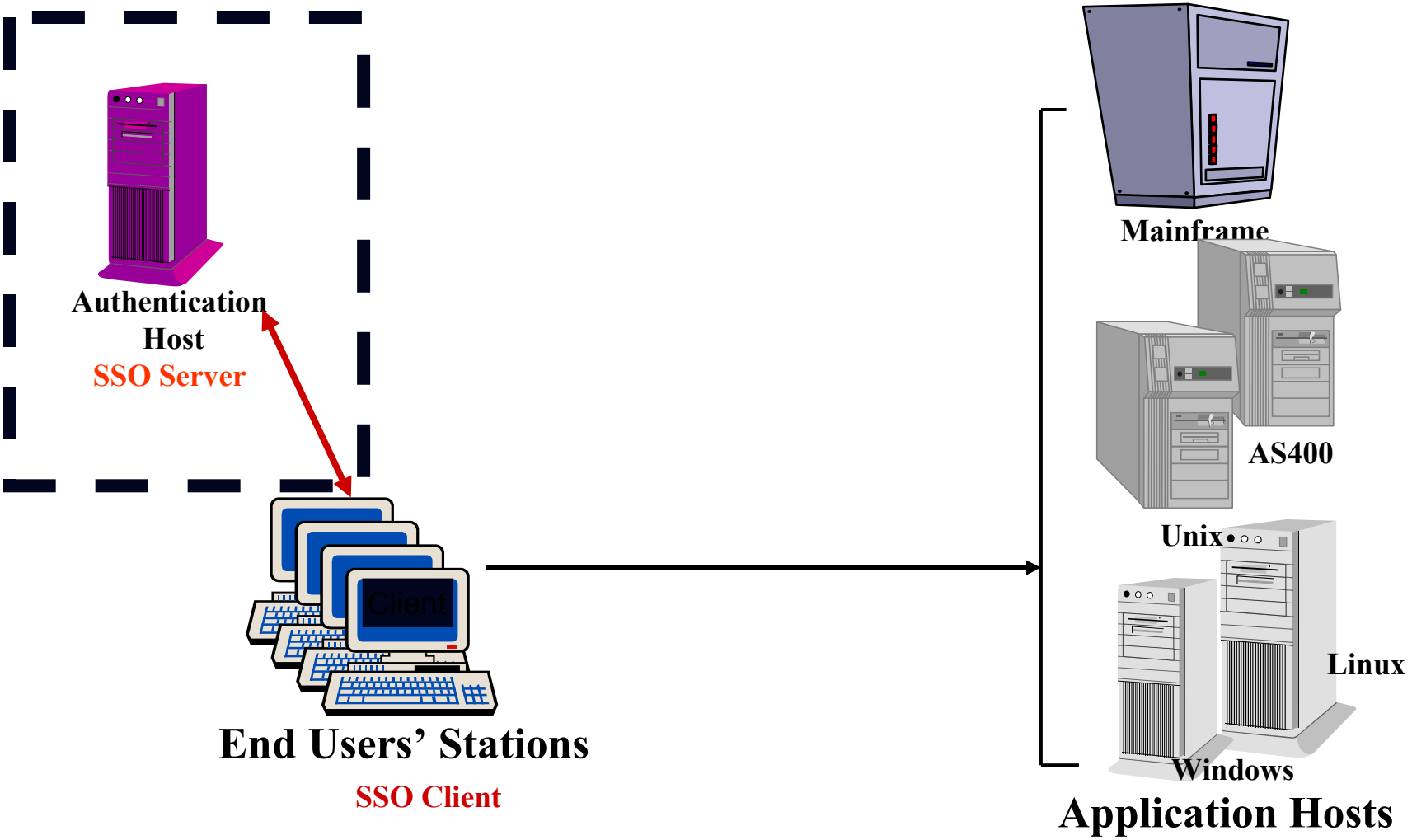


Autenticação

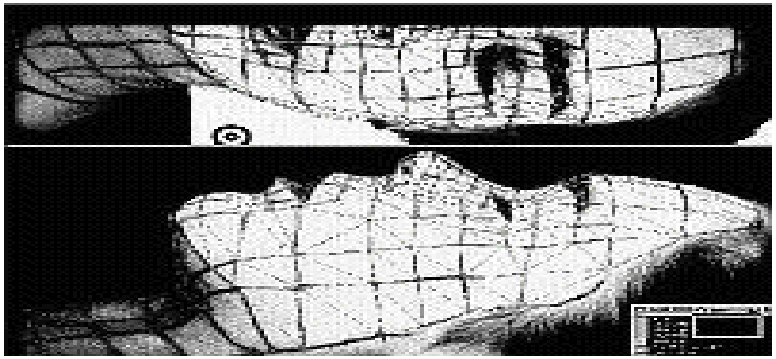
Sincronização de senhas



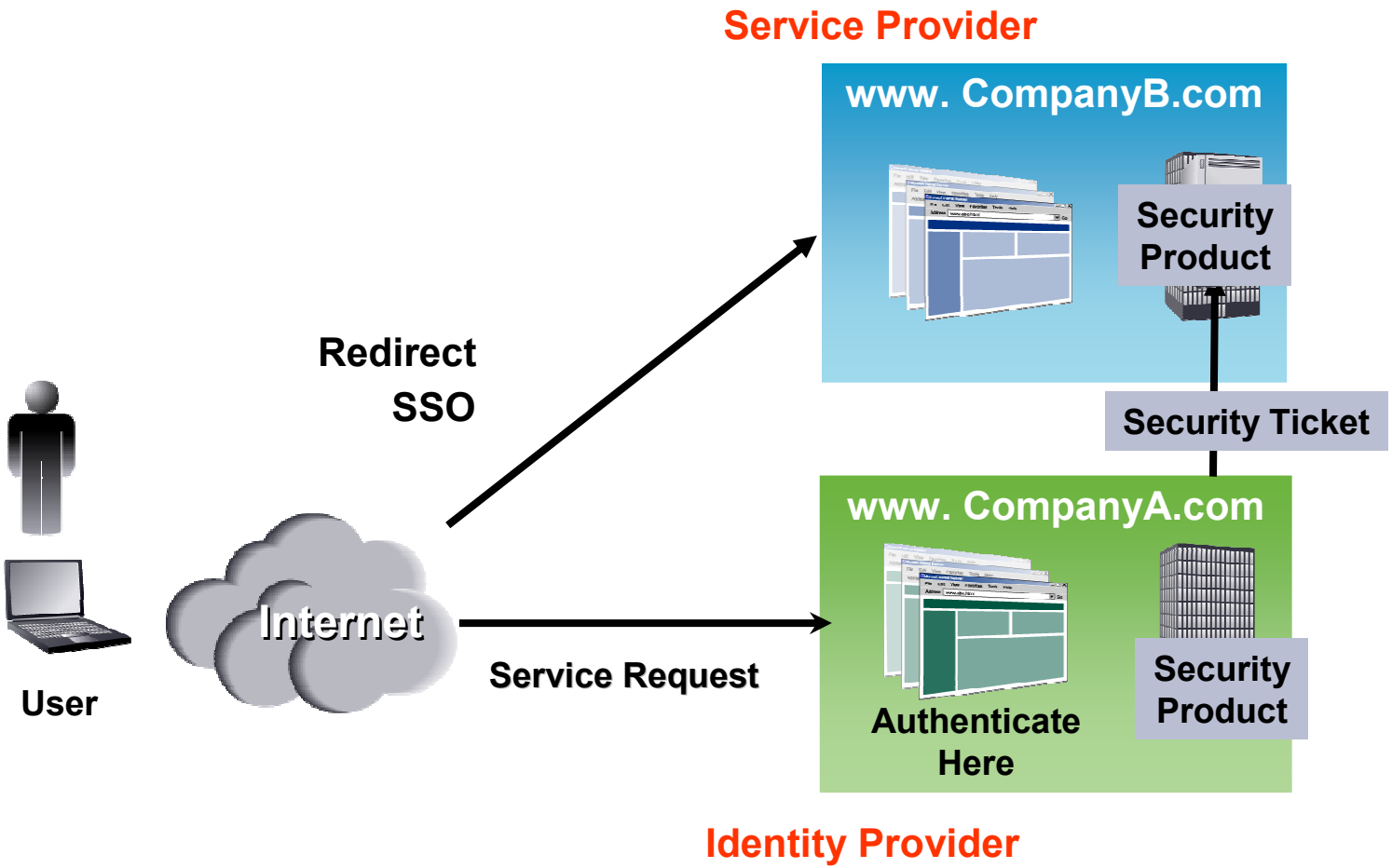
Single Sign On



Autenticação forte



Federação de Identidades



Autorização

Autorização

- Processo de determinar se uma identidade tem o direito ou a autoridade de executar um serviço ou acessar uma informação, em um domínio seguro.
  - Resposta: SIM ou NÃO

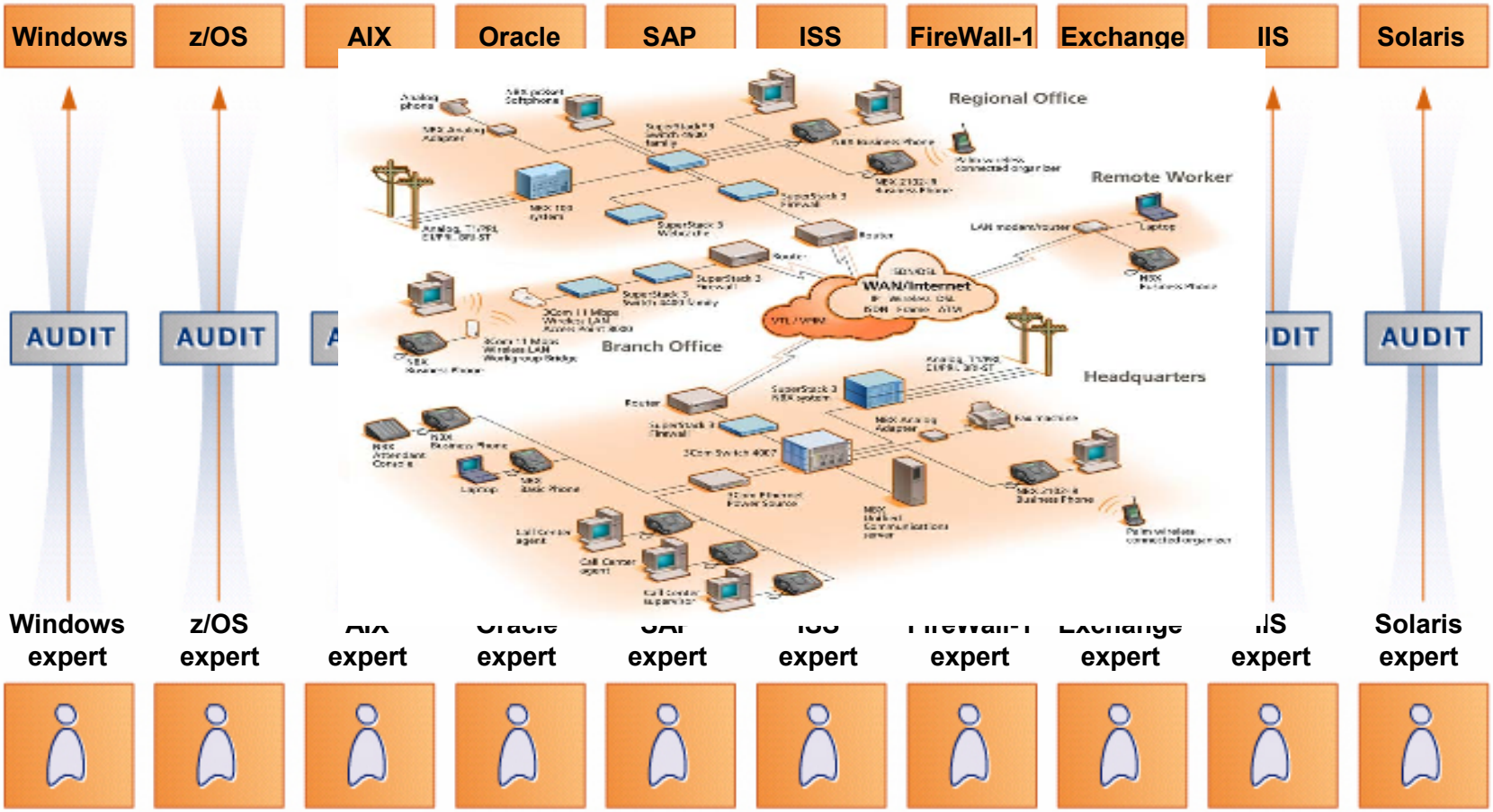
Camada Única de Autorização

Customers | **Employees** | **Partners**

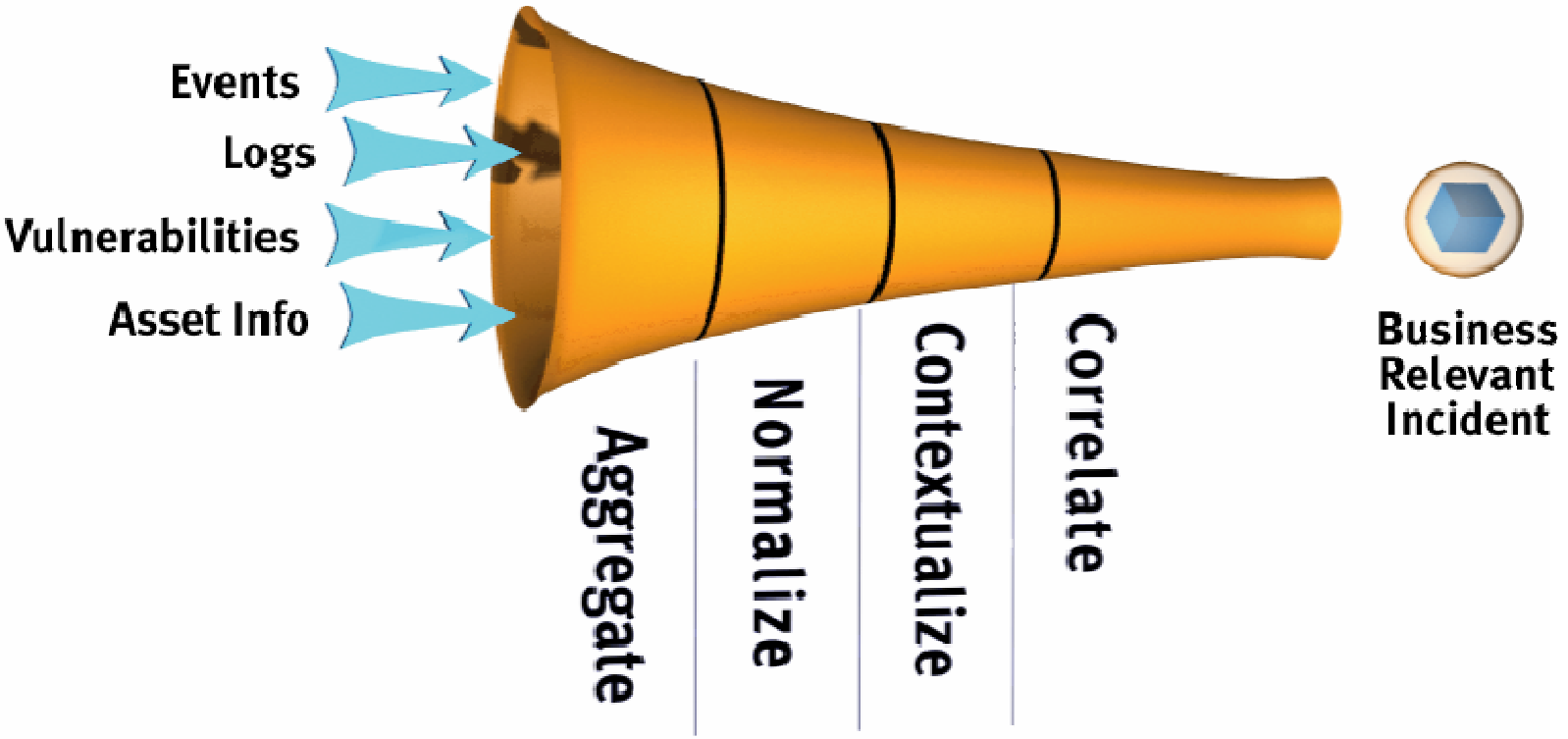
	Customer Self-Service	E-Commerce	CRM	ERP	HR	Partner Extranet	SCM
Security Layer	**Framework de controle de acesso**						
Application Layer	IBM	bea	SIEBEL	SAP	PEOPLESoft	Microsoft	ORACLE
User Store	SunONE LDAP	SQL 2000	LDAP	Oracle OID	Oracle RDBMS	Active Directory	Oracle
Operating System	Sun microsystems	Microsoft		IBM	hp invent	Microsoft	hp invent

Auditoria

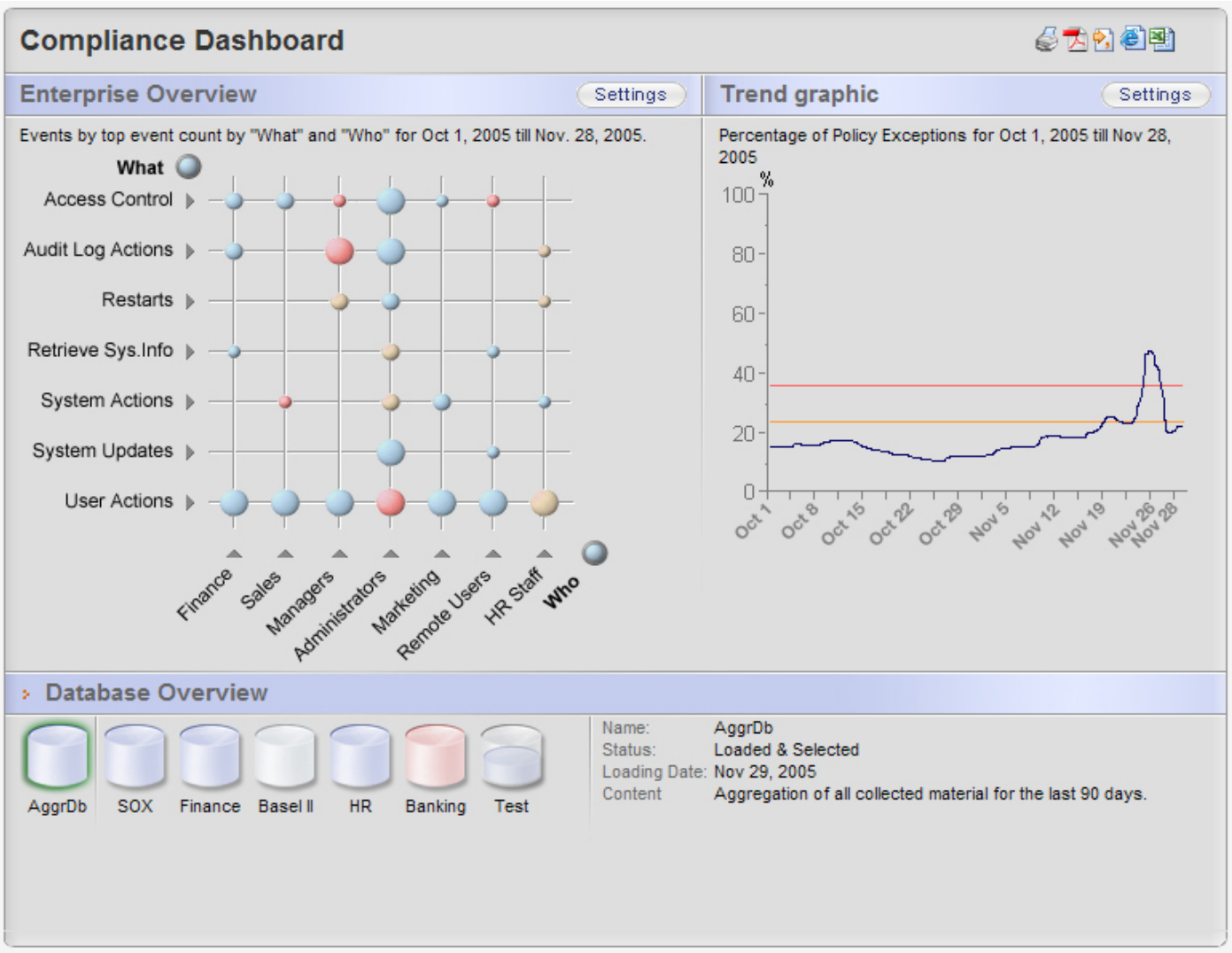
O desafio (infraestrutura heterogênea e complexa)



Normalização dos eventos



Compliance Dashboard



Agenda

Estratégia de segurança da IBM - objetivos

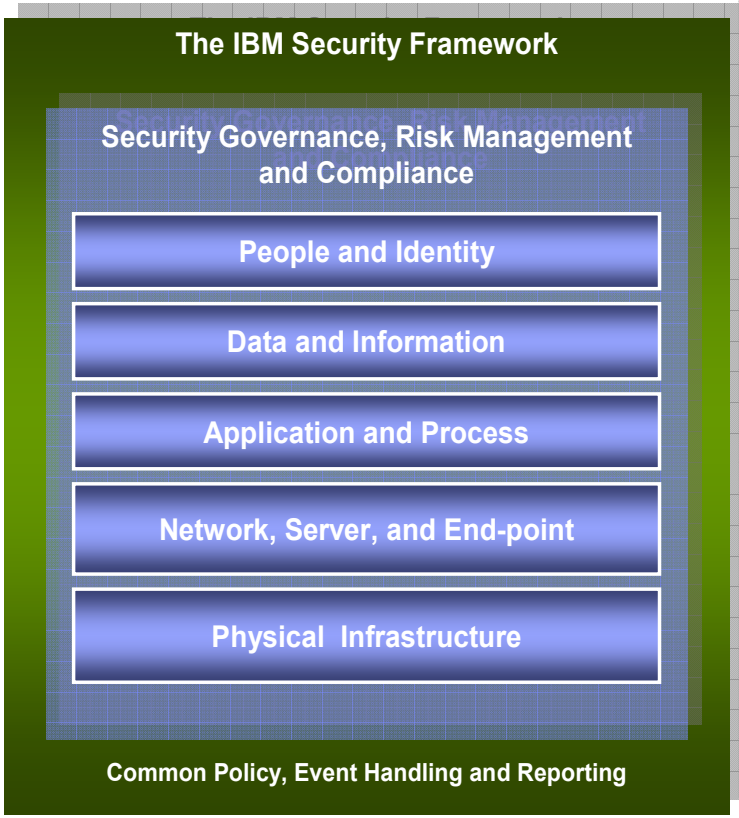
Desafios, motivação

Conceitos de IAM e o que endereça (4 As)

Soluções de segurança da IBM

Framework de Segurança da IBM

Proteção on-demand para ficar à frente das ameças externas e internas



IBM Security Solutions

CONFORMIDADE DE SEGURANÇA

- Aplicação de política demonstrável alinhada a regulamentos, padrões, leis, contratos (PCI, FISMA, etc..)

IDENTIDADE E ACESSO

- Permite colaboração integrada com segurança com usuários internos e externos com acesso controlado e seguro à informação, aplicativos e ativos

SEGURANÇA DE DADOS

- Protege e garante seus dados e informação de ativos

SEGURANÇA DE APLICATIVOS

- Gerenciar, monitorar e auditar continuamente (de forma contínua) a segurança de aplicativos

SEGURANÇA DE INFRAESTRUTURA

- Gerenciamento compreensivo de ameaças e vulnerabilidade através de redes, servidores e estações

Gerenciamento de Identidade e Acesso

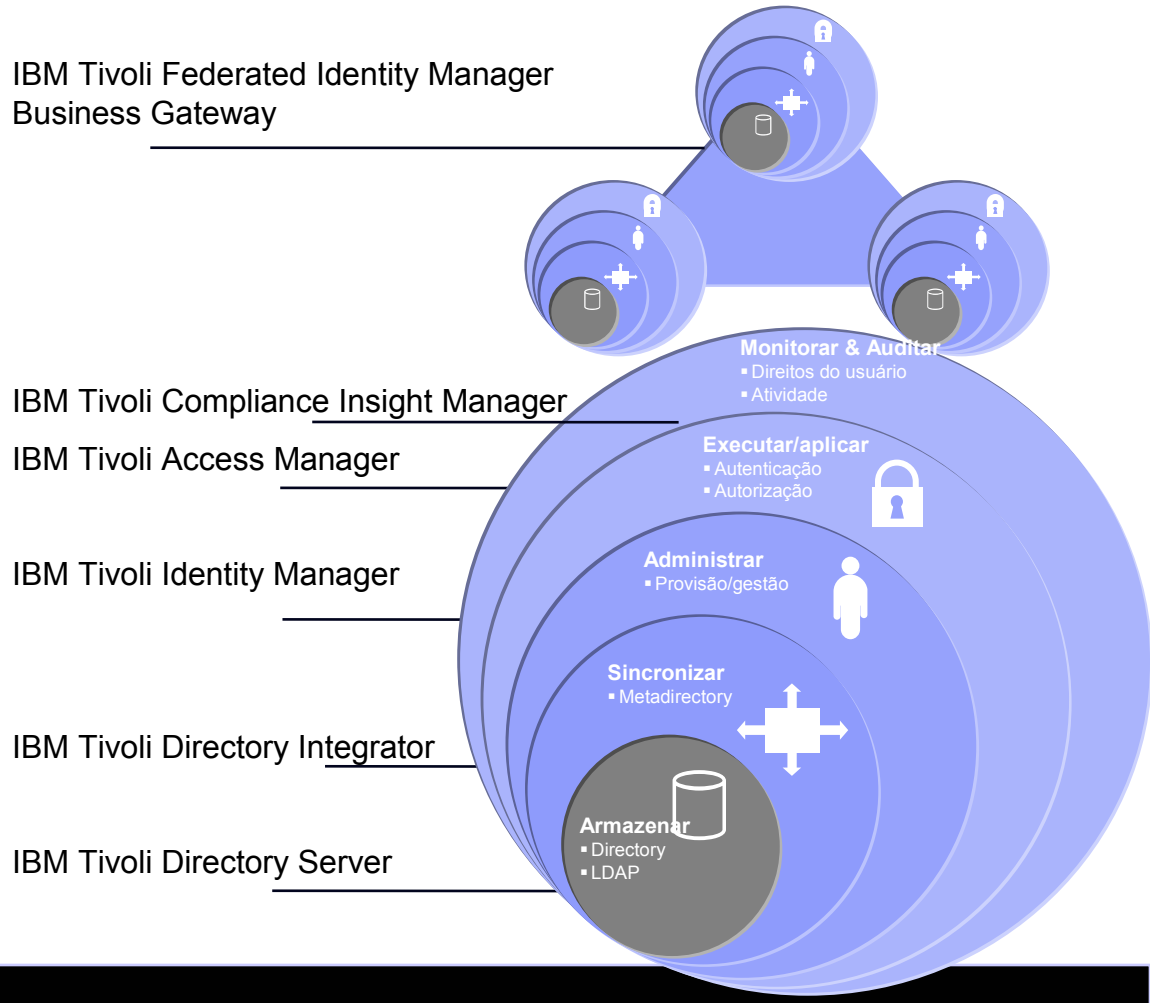
Gerencia usuários, identidades,direitos de acesso, controla e monitora atividade do usuário em todos os sistemas de IT

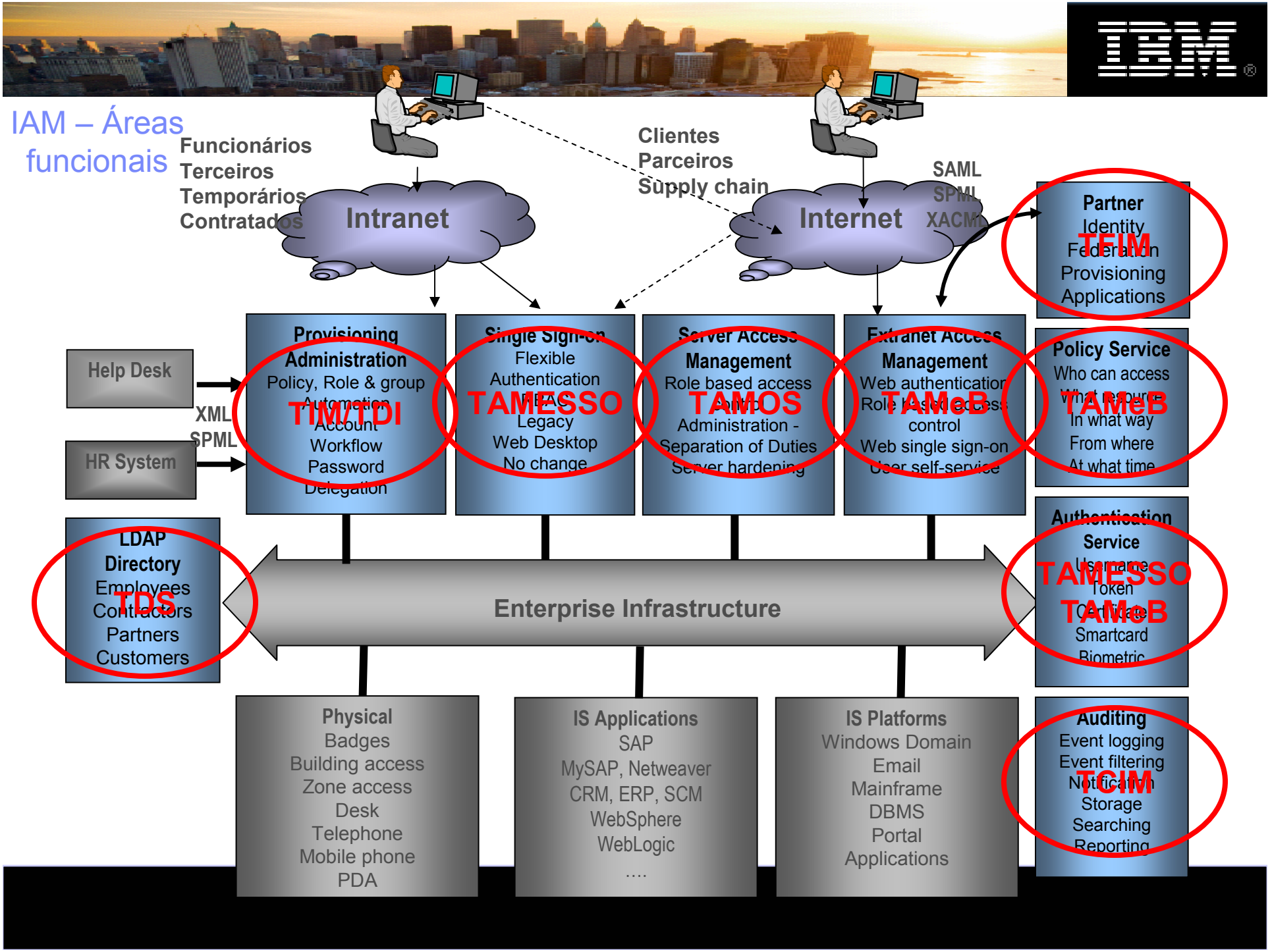
Objetivos

- Permite *single sign on* (acesso único, autenticação única)
- Gerencia o ciclo de vida da identidade: provision, deprovision.
- Monitora atividade de conta: contas inativas, atividade irregular.
- Revisão / Recertifica acesso periodicamente
- Automatiza processos manualmente implementados para controle de acesso aos recursos de IT
- Centraliza política de acesso e controles internos relacionados
- Verifica adequadamente a autenticidade de todos os usuários baseada em riscos potenciais

Soluções IBM

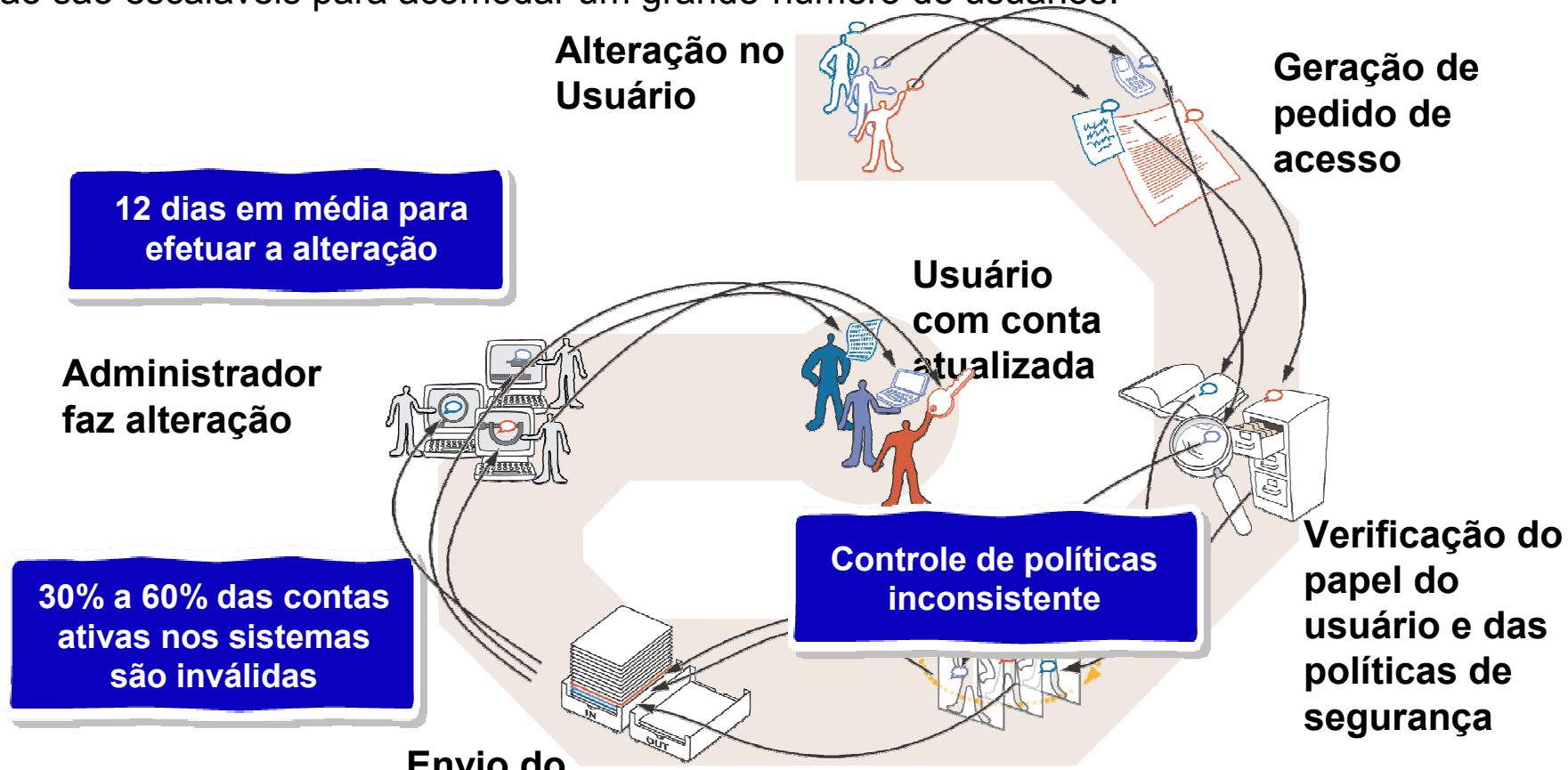
- Tivoli Identity Manager
- Tivoli Access Manager for Web
- Tivoli Access Manager for ESSO
- Tivoli Federated Identity Manager



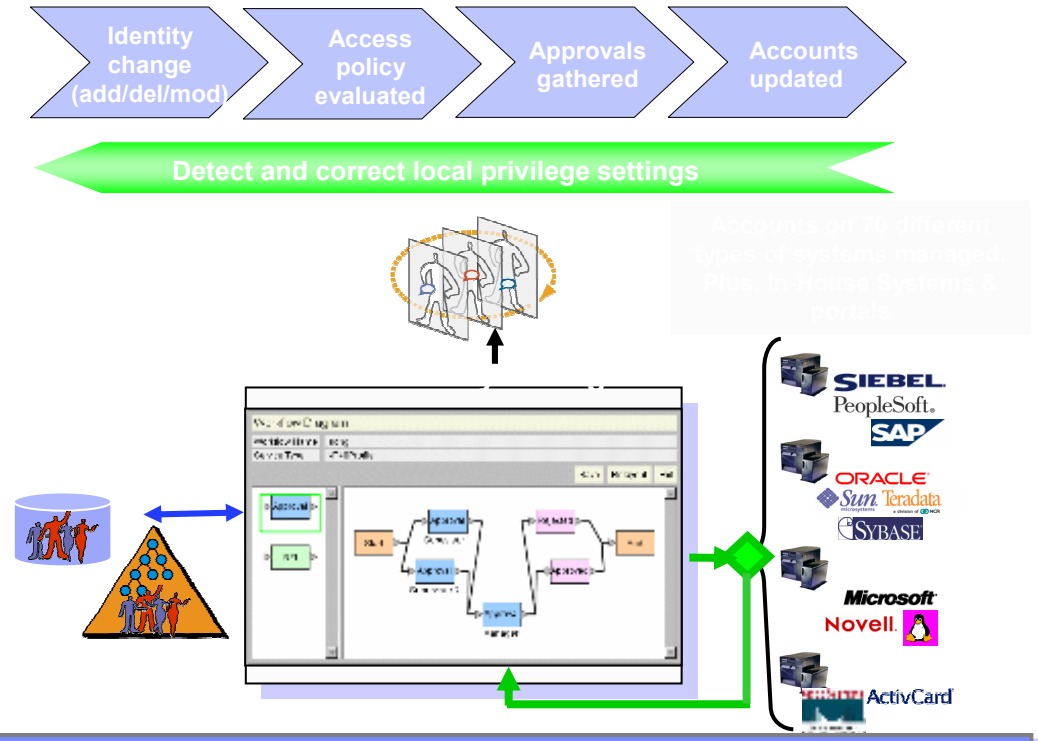

IAM – Áreas funcionais
Funcionários
Terceiros
Temporários
Contratados
Clientes
Parceiros
Supply chain
SAML
SPML
XACML
Intranet
Internet
Partner
Identity
Federation
Provisioning
Applications
TFIM
Help Desk
HR System
XML
SPML
Provisioning
Administration
Policy, Role & group
Automation
Account
Workflow
Password
Delegation
TIM/TDI
Single Sign-on
Flexible
Authentication
RBAC
Legacy
Web Desktop
No change
TAMESSO
Server Access
Management
Role based access
Admin
Administration -
Separation of Duties
Server hardening
TAMOS
Extranet Access
Management
Web authentication
Role based access
control
Web single sign-on
User self-service
TAMeB
Policy Service
Who can access
What resource
In what way
From where
At what time
TAMeB
LDAP
Directory
Employees
Contractors
Partners
Customers
TDS
Enterprise Infrastructure
Authentication
Service
Username
Token
Certificate
Smartcard
Biometric
TAMESSO
TAMeB
Physical
Badges
Building access
Zone access
Desk
Telephone
Mobile phone
PDA
IS Applications
SAP
MySAP, Netweaver
CRM, ERP, SCM
WebSphere
WebLogic
....
IS Platforms
Windows Domain
Email
Mainframe
DBMS
Portal
Applications
Auditing
Event logging
Event filtering
Notification
Storage
Searching
Reporting
TCIM

Provisionamento de Usuários: O Problema

Os processos manuais, demorados e inconsistentes usados pelas empresas atualmente não são escaláveis para acomodar um grande número de usuários.



Tivoli Identity Manager automatiza, audita e corrige direitos de acessos de forma corporativa.



- Know the ***people*** behind the accounts and ***why*** they have the access they do
- Fix non-compliant accounts
- Automate user privileges lifecycle across entire IT infrastructure
- Match your workflow processes

Cost

Redução de custos

- Auto-serviço
- Reset de senhas
- Provisionamento automático de usuários

Complexity

Simplificação

- Política consistente
- Integração rápida de usuários e aplicações

Compliance

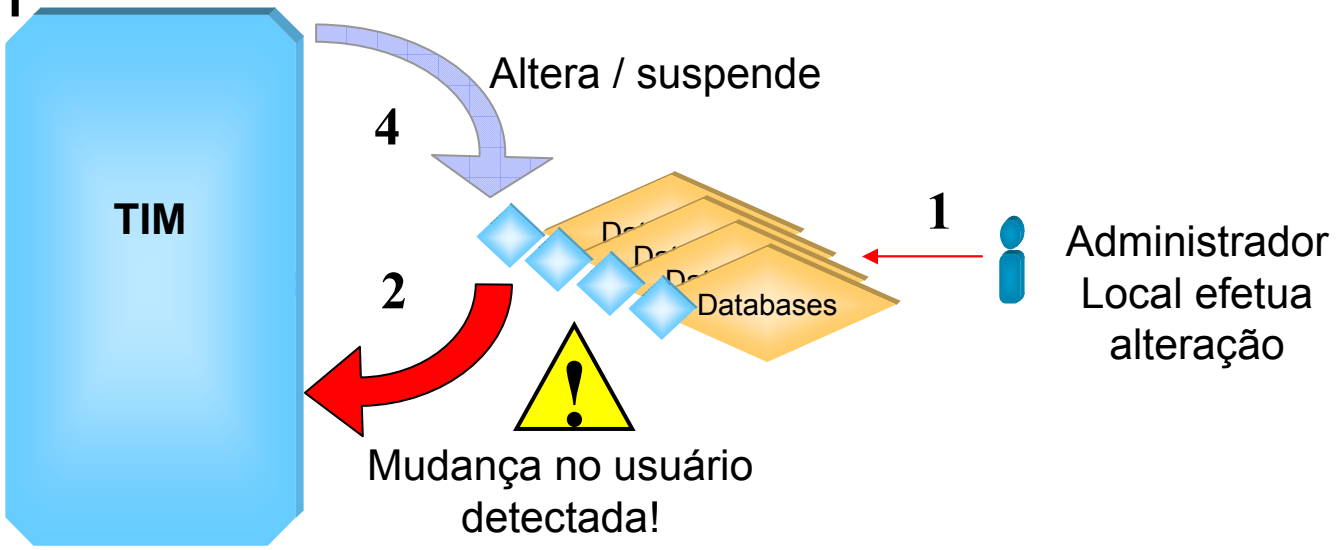
Conformidade

- Auditoria e relatórios

Consolidação de diretórios/repositórios: Reconciliation

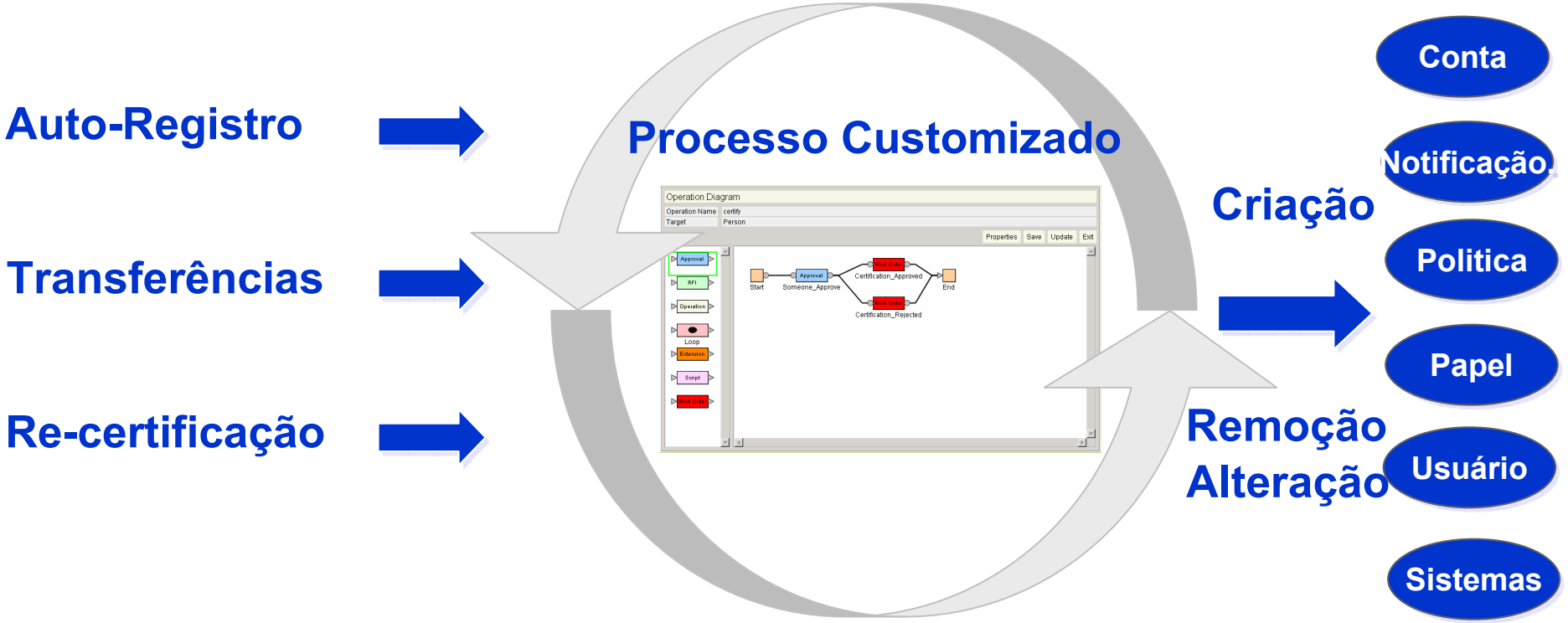
3

Avaliação da mudança em relação as políticas
1. Aceita
2. Suspende
3. Restaura



- Compara "O QUE É" com "O QUE DEVE SER"
- Operações não-autorizadas feitas por um operador local podem ser desfeitas
- Políticas são checadas durante um "reconciliation"
- Contas orfãs podem ser "adopted", "suspended", "restored" ou "deprovisioned"

Gerenciamento do Ciclo de Vida dos Usuários

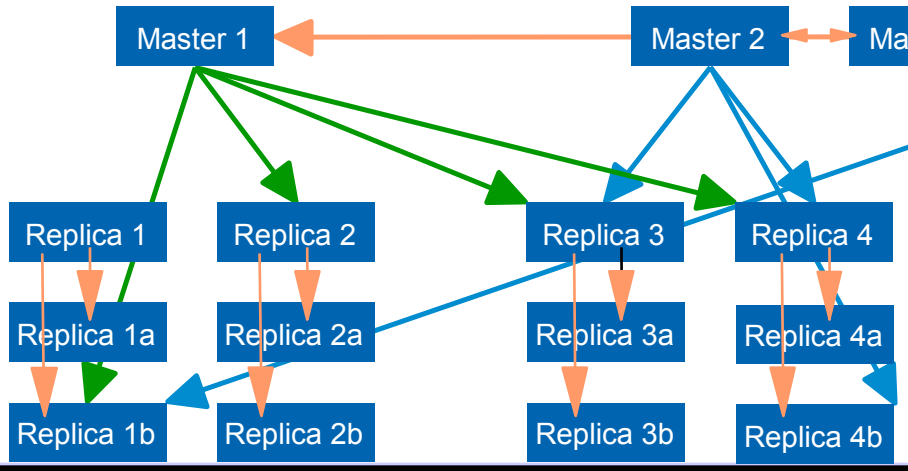


- Gerenciamento de todo o cliclo de vida das Identidades, desde a sua criação alteração e remoção.

- Processo de Re-Certificação: assegura a existência somente de contas válidas.

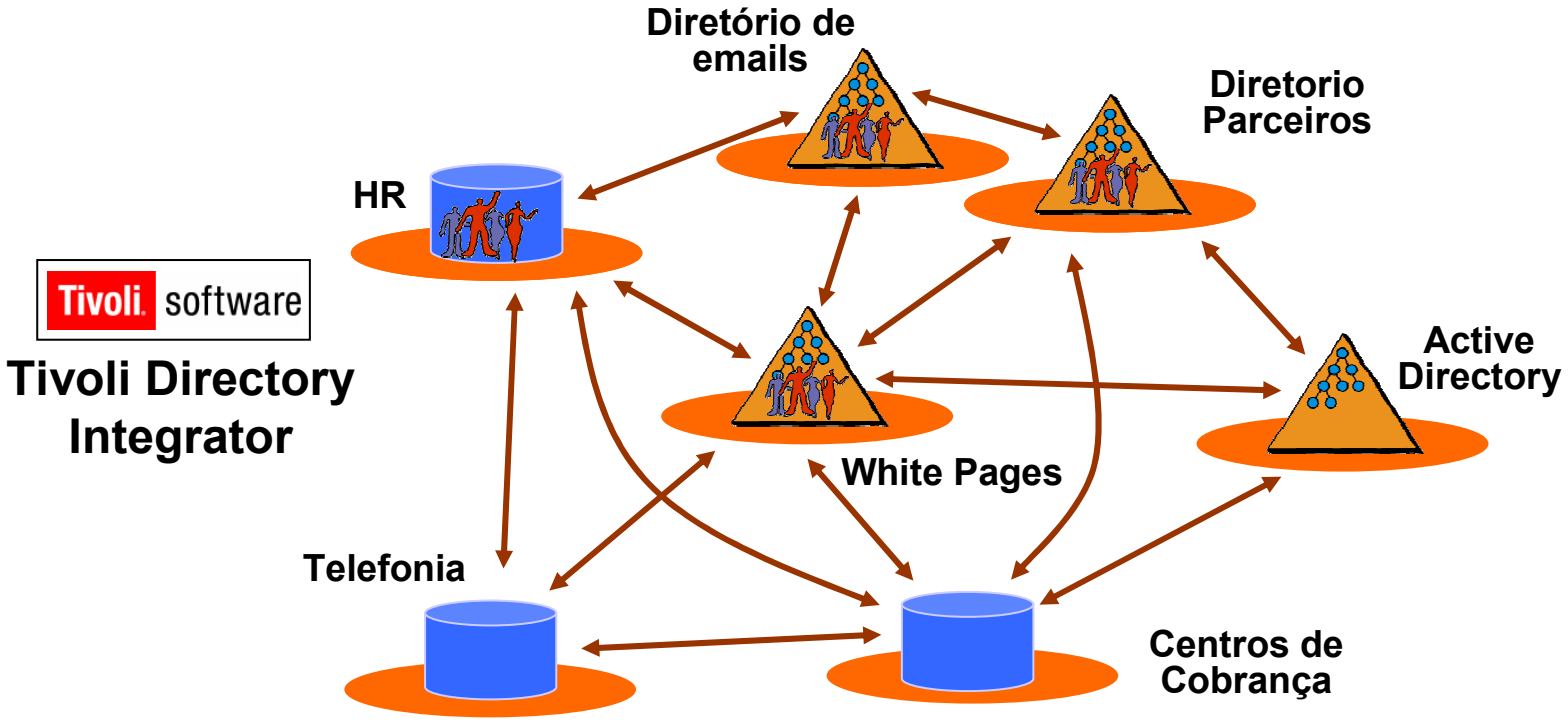
IBM Tivoli Directory Server

- Alta performance e escalabilidade
- Grande número de plataformas suportadas
  - –AIX, Solaris, Linux (RedHat and SuSE), HP-UX, Windows, OS/400, z/OS
- Sólido suporte a interface LDAPv3
  - – Certificado pelo The Open Group e Common Criteria
- Schema dinâmico e extensível
- Grandes capacidades de replicação, garantindo alta-disponibilidade



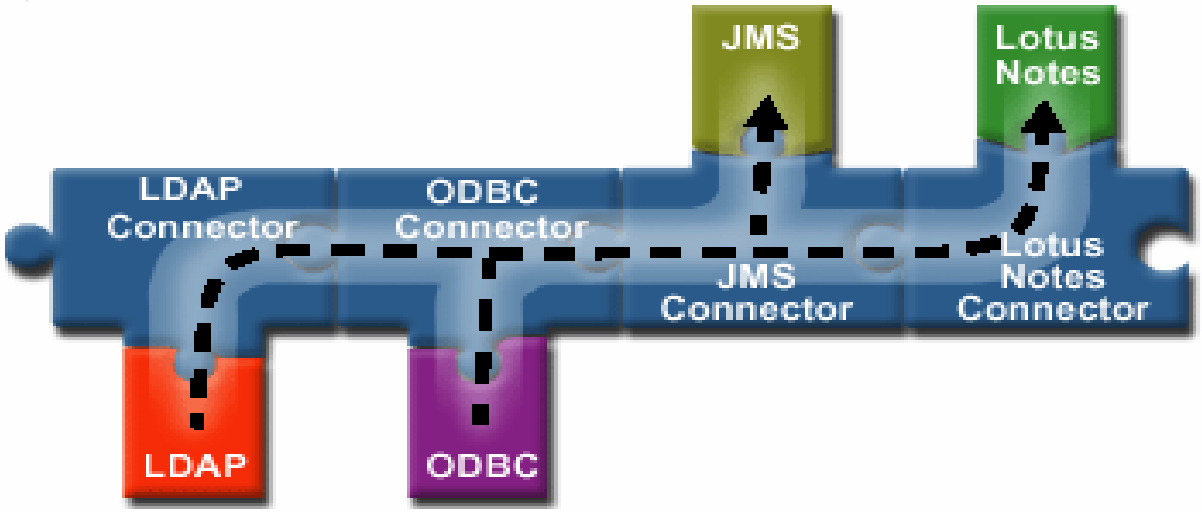
Um diretório deve comportar milhões de entradas e suportar milhões de operações por dia, com alta disponibilidade

Tivoli Directory Integrator



IBM Tivoli Directory Integrator

- Sincronismo ‘any-any’
- Move, copia e transforma dados entre sistemas
  - Metodologia AssemblyLine – linha de montagem
  - Mapeamento dos schemas e atributos dos sistemas conectados
  - Suporte a JavaScript e VBScript para desenvolver lógica de negócio e manuseio de exceções
- Parte integrante dos pacotes: Tivoli Identity Manager, Lotus Workplace Messaging and WebSphere Express for iSeries eServers



Tivoli Identity Manager Demo

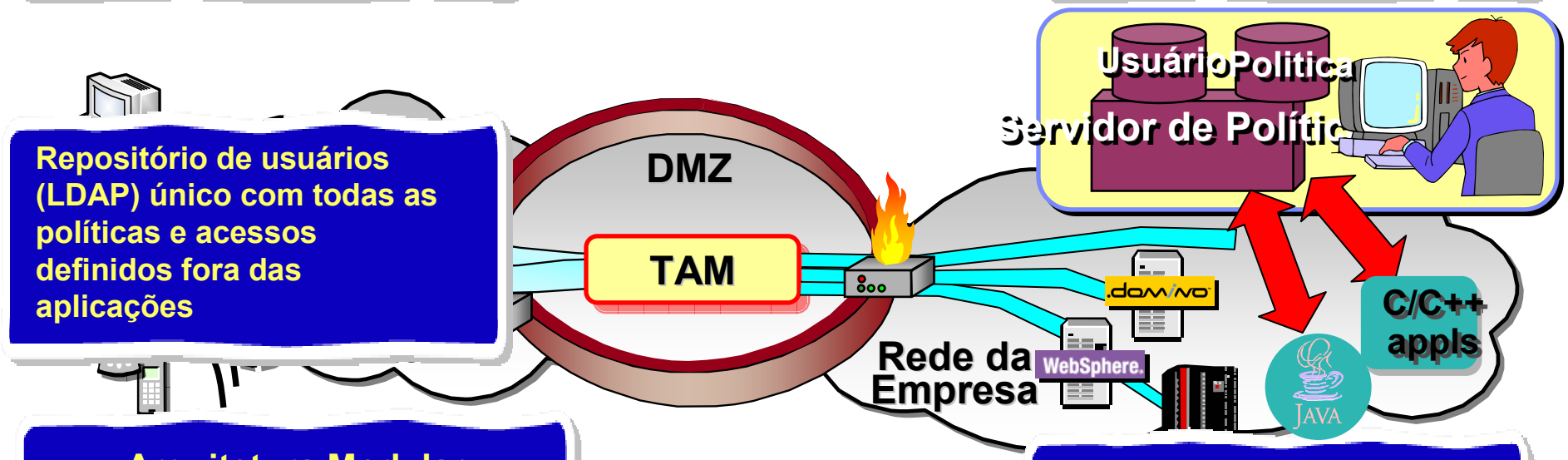
Self-Service Interface

Gerencia de Acesso TAMeb

APIS de Autenticação e Autorização baseados em padrões de mercado : Time to Market / foco no negocio

Alta disponibilidade e escalabilidade

Desenvolvimento foca em lógica de negócio e Não em Segurança
Aplicações Web existentes não necessitam ser alteradas

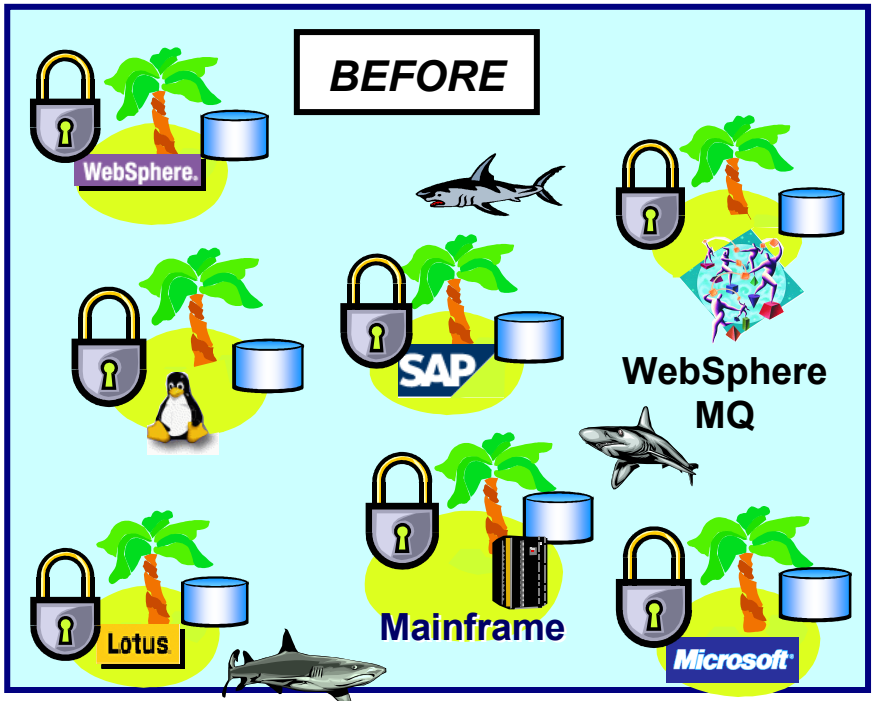


Repositório de usuários (LDAP) único com todas as políticas e acessos definidos fora das aplicações

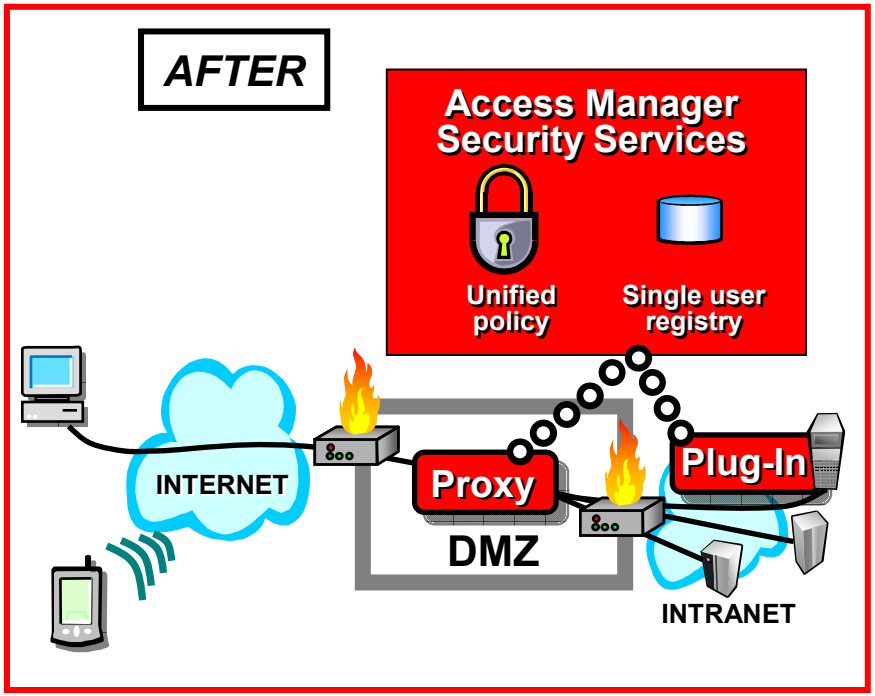
Arquitetura Modular suportando diversos mecanismos de autenticação Inclusive Certificados Digitais

Single Sign-on (Senha única) nas aplicações Web / Portal

Segurança integrada com TAMeb

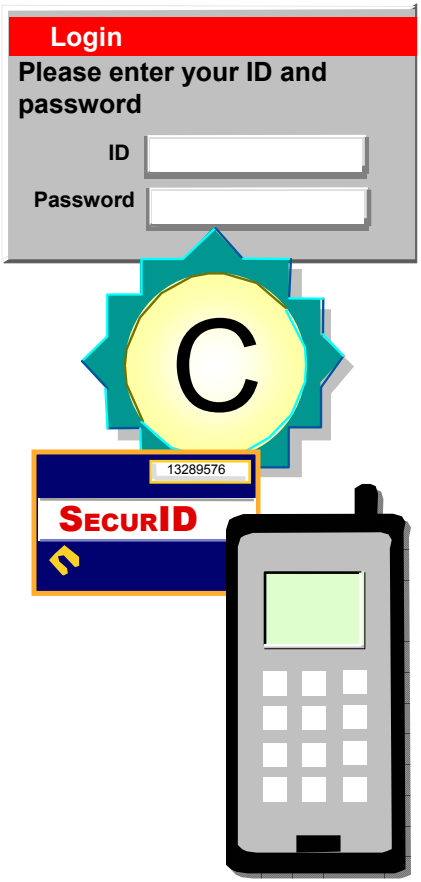


- Muitas senhas para lembrar
- Multiplos administradores e ferramentas
- Informações espelhadas de usuários e controle de acesso
- Desenvolvimento de código de segurança dentro das aplicações



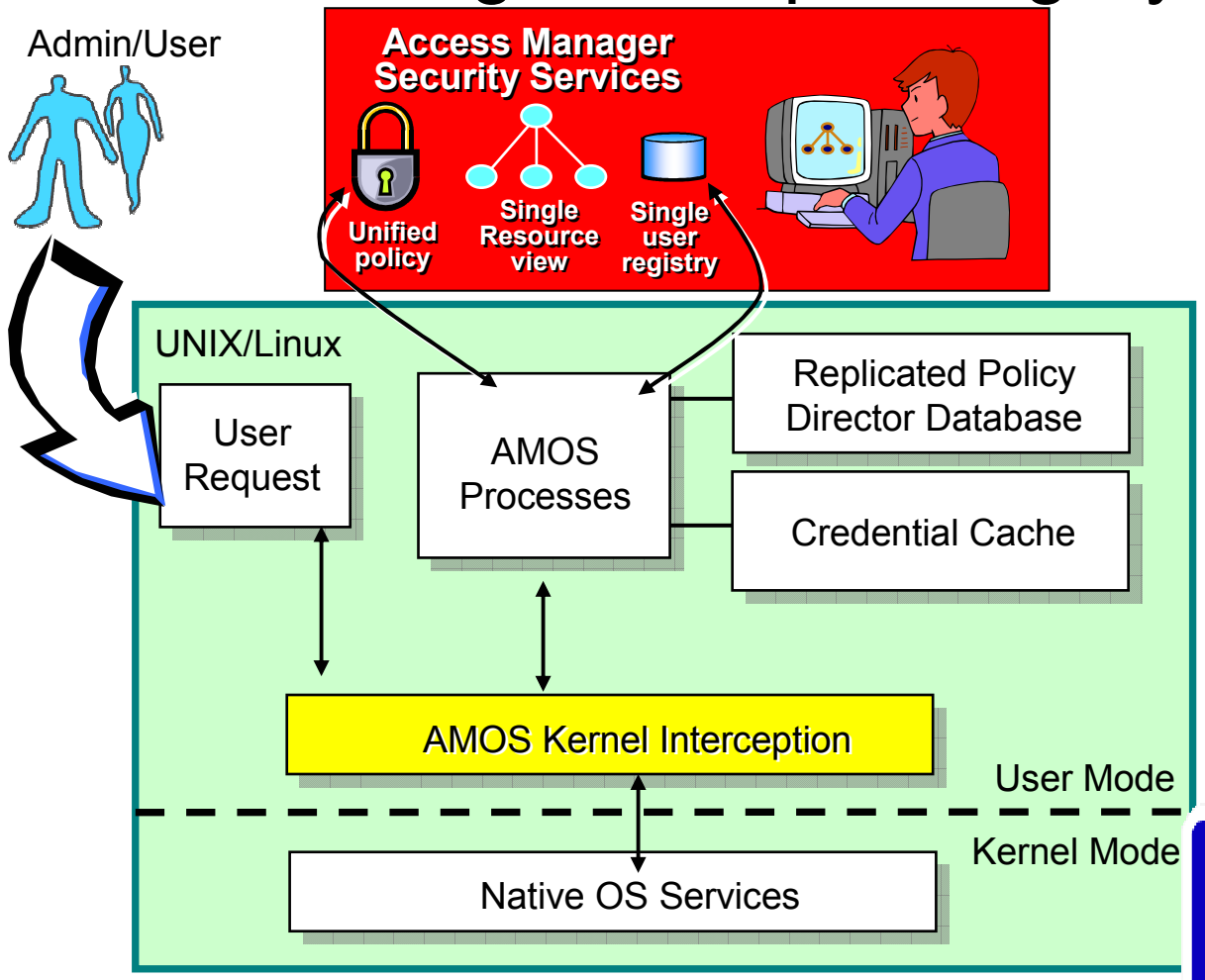
- Single Sign-On em ambiente Web
- Administração centralizada
- Informações de usuários e controle de acesso centralizadas - LDAP
- Transações seguras HTML & SOAP

Autenticação



- Provar a identidade do usuário
- Suporta vários mecanismos:
  - ✓Usuário / Senha
  - ✓Certificado Digital (X.509v3)
  - ✓SecurID Token
  - ✓WAP
  - ✓Recursos sensitivos
  - ✓Autenticação customizadas – CDAS/EAI

Access Manager for Operating Systems



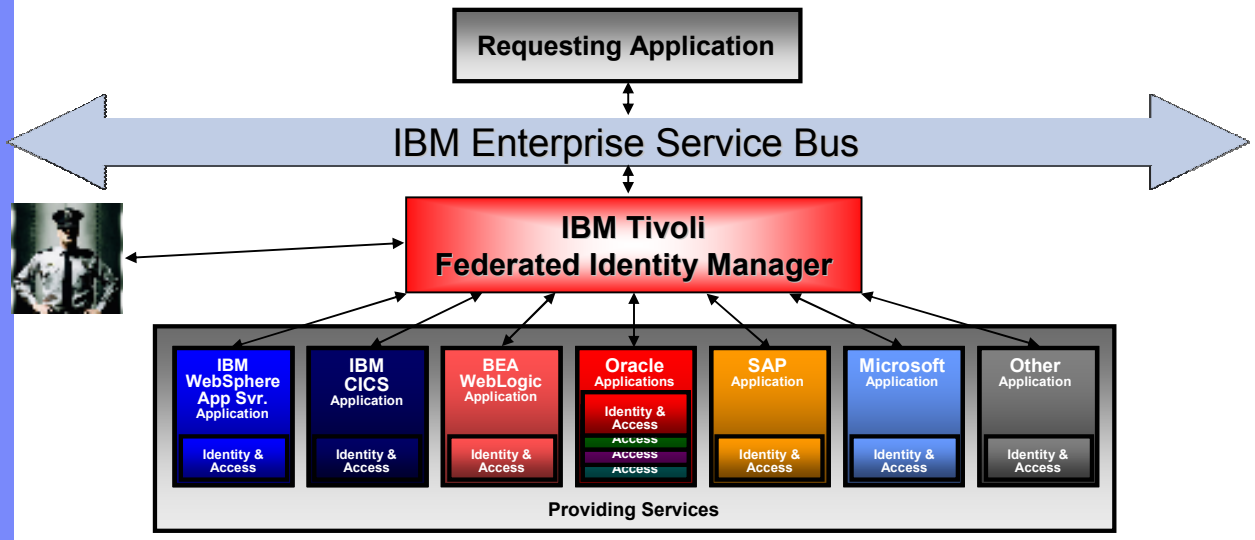
- **Protege:**
  - File systems
  - Remote network services
  - Local network services
  - Login services — quando e de que lugar
  - Mudanças no usuário e nos grupos
  - e mais..

Granularidade de controle dos acessos do usuário 'root' e dos demais usuários

Segurança de Aplicativo - SOA

Objetivos

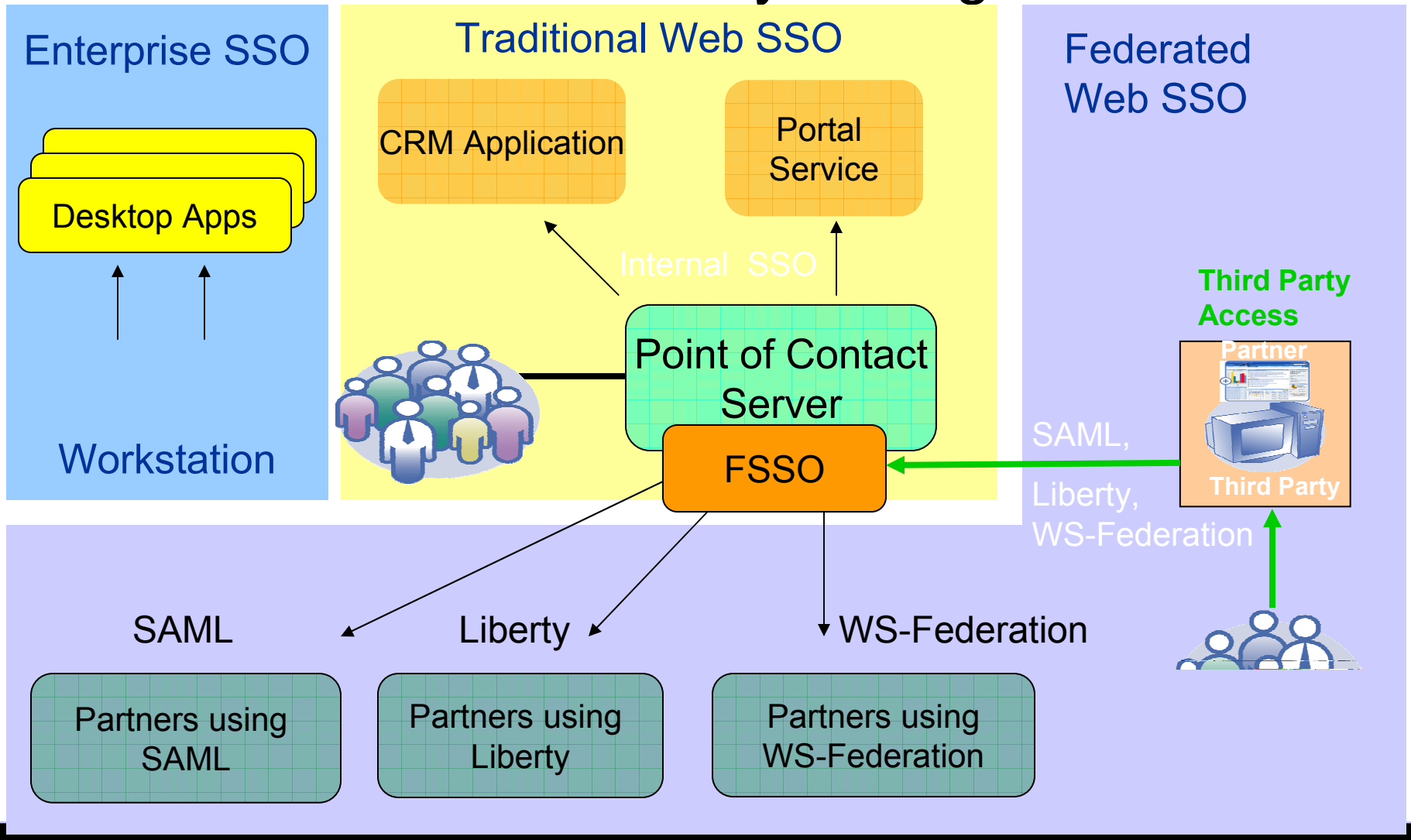
- Proporcionar acesso seguro e identidade federada através desses serviços em um ambiente SOA
- Externalizar serviços de segurança centrais a partir da aplicação
- Assegurar que os administradores de segurança façam as mudanças e NÃO os desenvolvedores.
- Assegurar que as mudanças de segurança sejam auditáveis



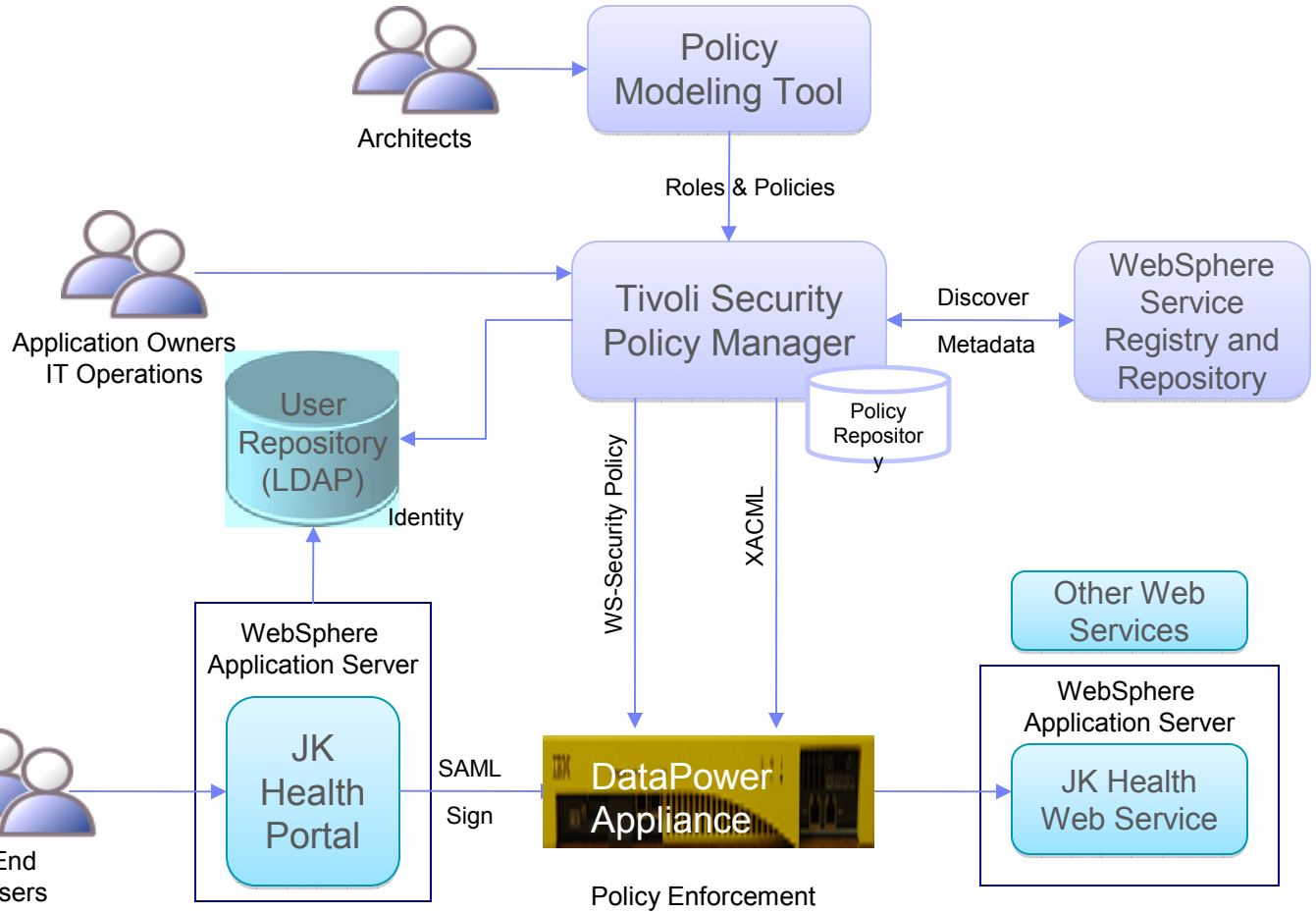
Soluções IBM

- Tivoli Federated Identity Manager
- Tivoli Security Policy Manager

IBM Tivoli Federated Identity Manager



Tivoli Security Policy Manager - TSPM

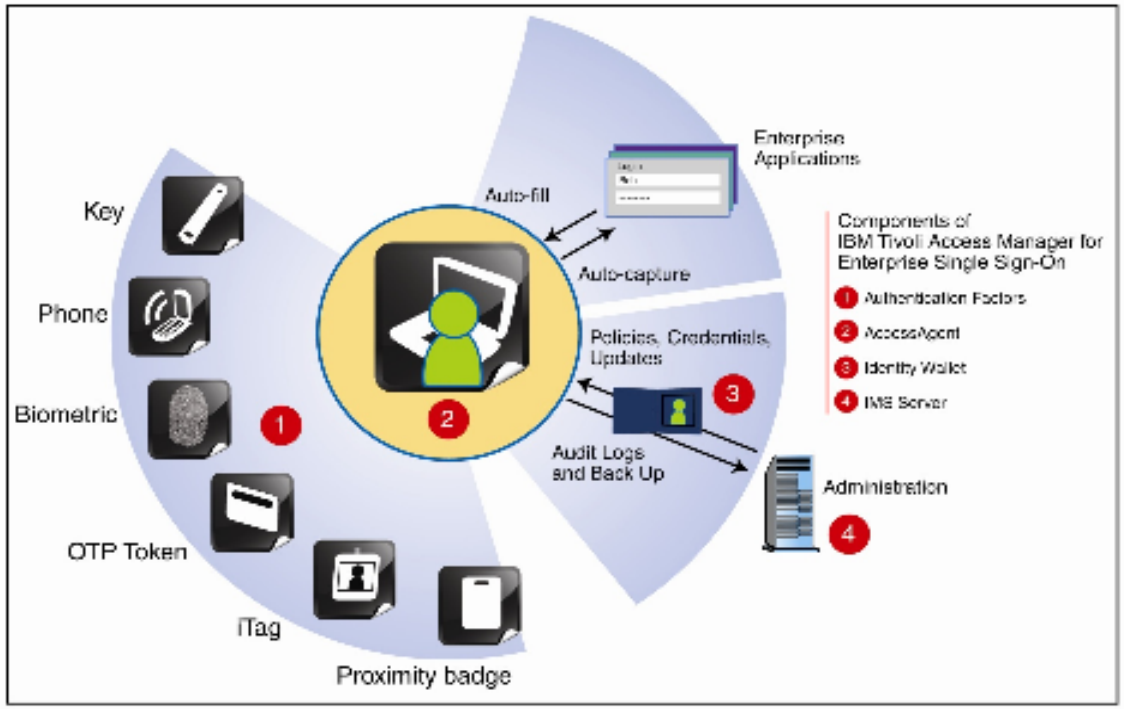


TAM-ESSO – Enterprise Single Sign-on

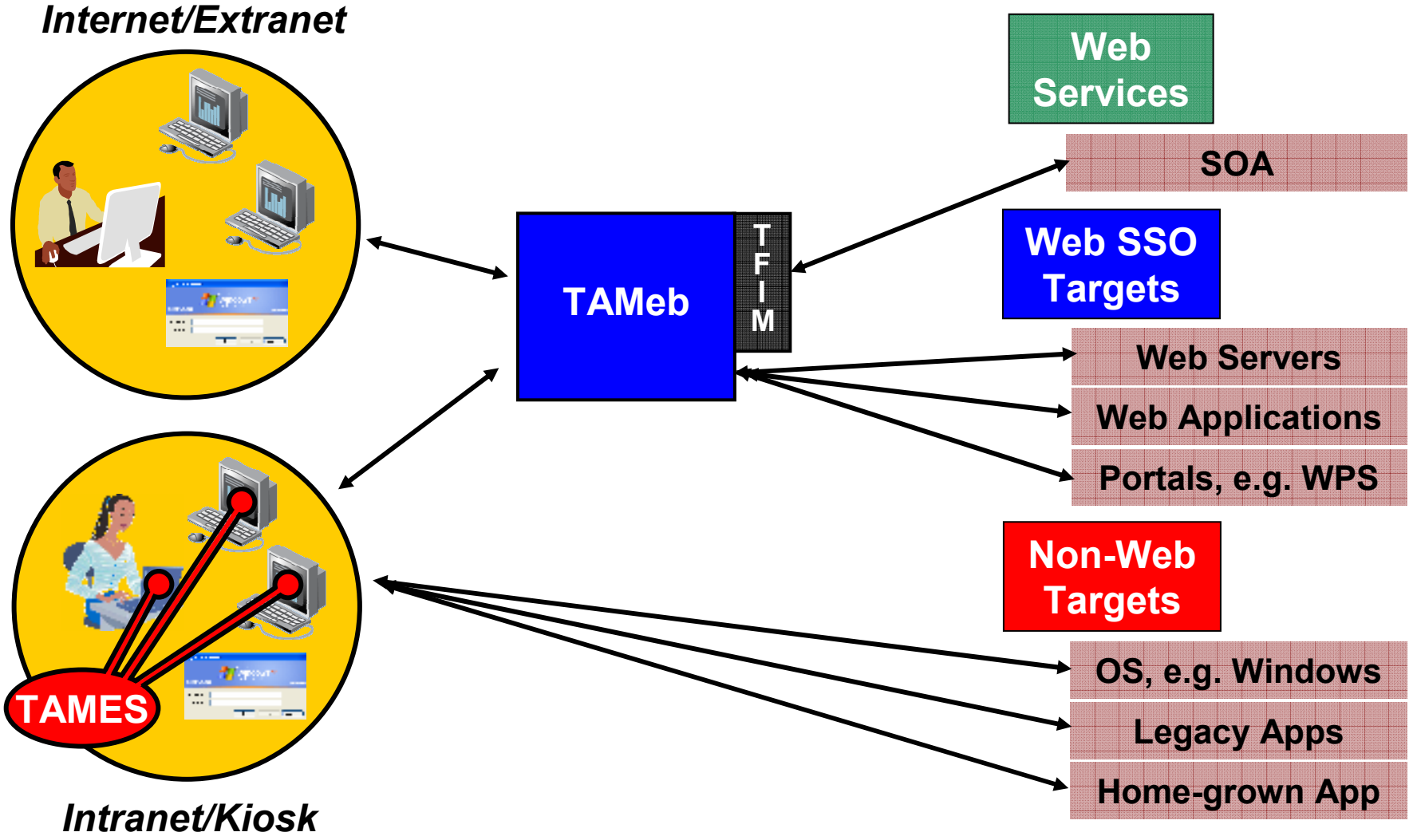
TAM E-SSO proporciona:

- **Single sign-on multi-ambiente**
- **Autenticação multi-Fator**
- **Security Workflow automation**
- **Fast user switching**
- **Trilha de auditoria de acesso**
- **Política de gerenciamento centralizado**

Sem mudança na infra-estrutura

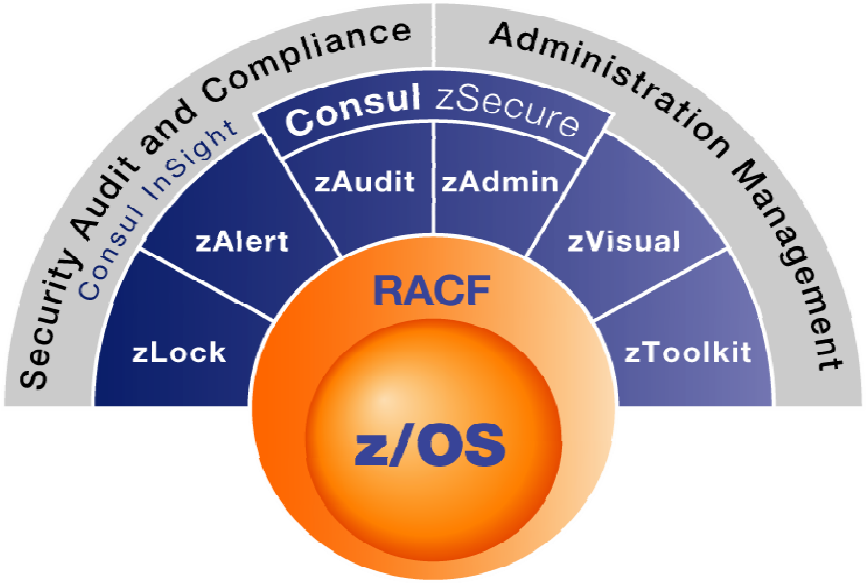


Solução Completa de Single Sign-On



Família ZSecure

A família de produtos Consul zSecure facilita a administração da segurança do Mainframe além de adicionar capacidades ao z/OS Resource Access Control Facility (RACF) de alerta, auditoria e monitoração.



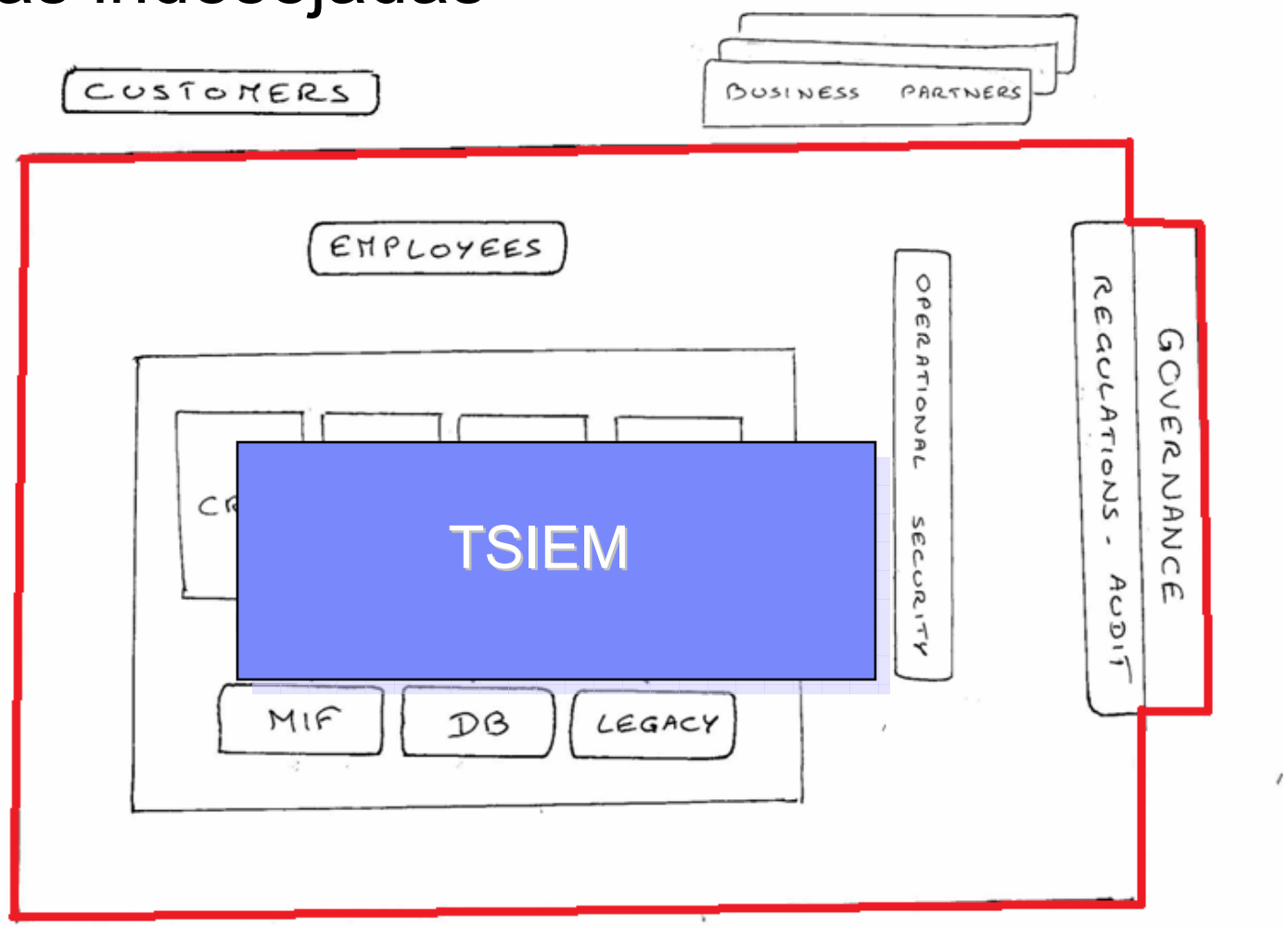
Funcionalidades

- Administração e Provisionamento:
  - **zAdmin:** facilita tarefas de administração de segurança e gerenciamento de usuários do RACF
  - **zVisual:** Janela Windows para acesso ao RACF
  - **zToolkit:** cria ambiente CICS para execução de comandos RACF
- Auditoria, monitoração e compliance:
  - **zLock:** previne a execução de comandos indesejados no RACF.
  - **zAlert:** alertas e detecção de intrusos e ações para para um ataque no Mainframe.
  - **zAudit:** analise e reportes de eventos para auditoria e analise.

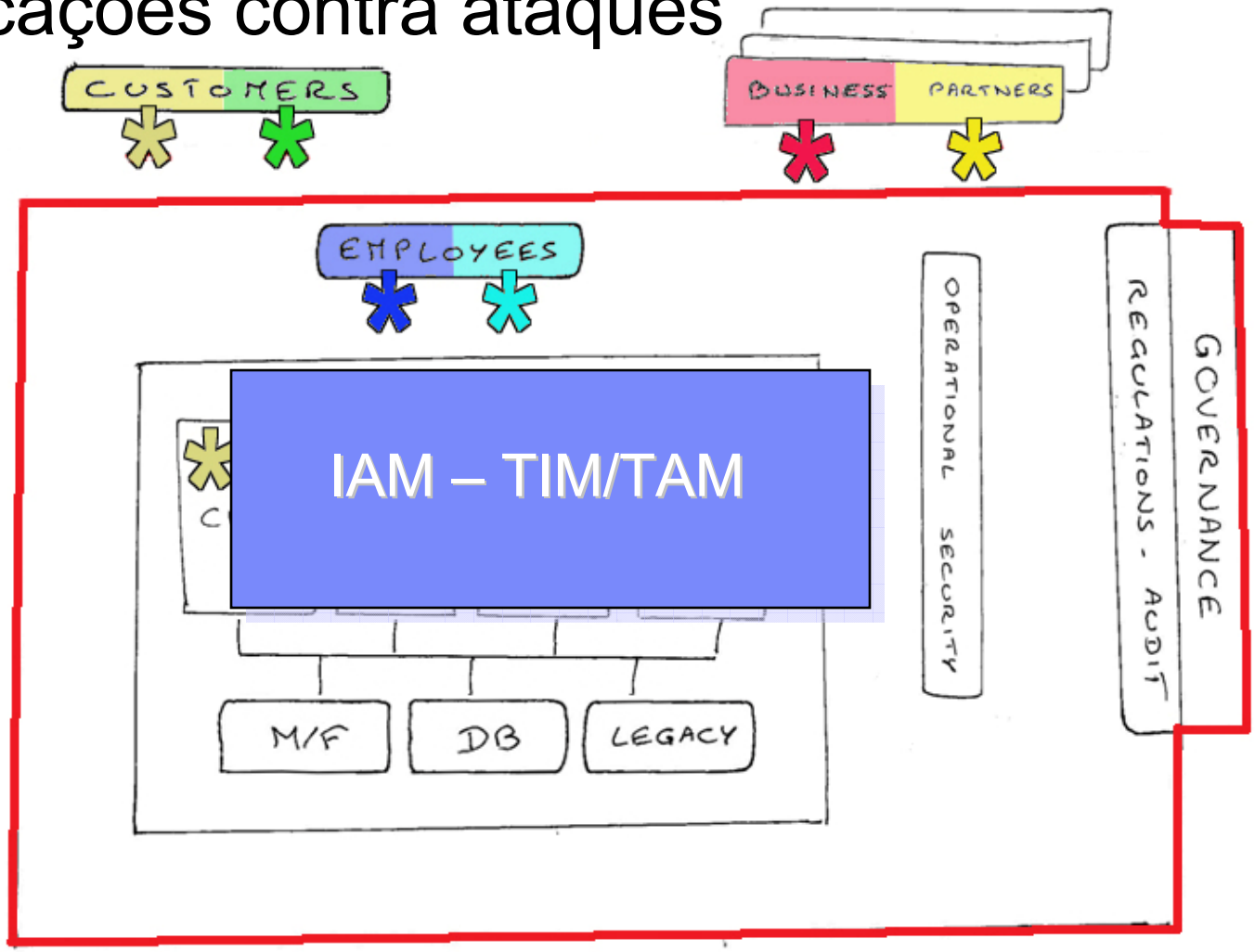
Benefícios

- Administração e Provisionamento:
  - Redução de tempo, esforço e custo de administração
  - Redução de tempo de treinamento para novos administradores
- Auditoria, monitoração e compliance:
  - Facilita auditorias, mostrando postura de segurança
  - Melhoria na segurança do ambiente e no manuseio de incidentes provendo redução de tempo e custos

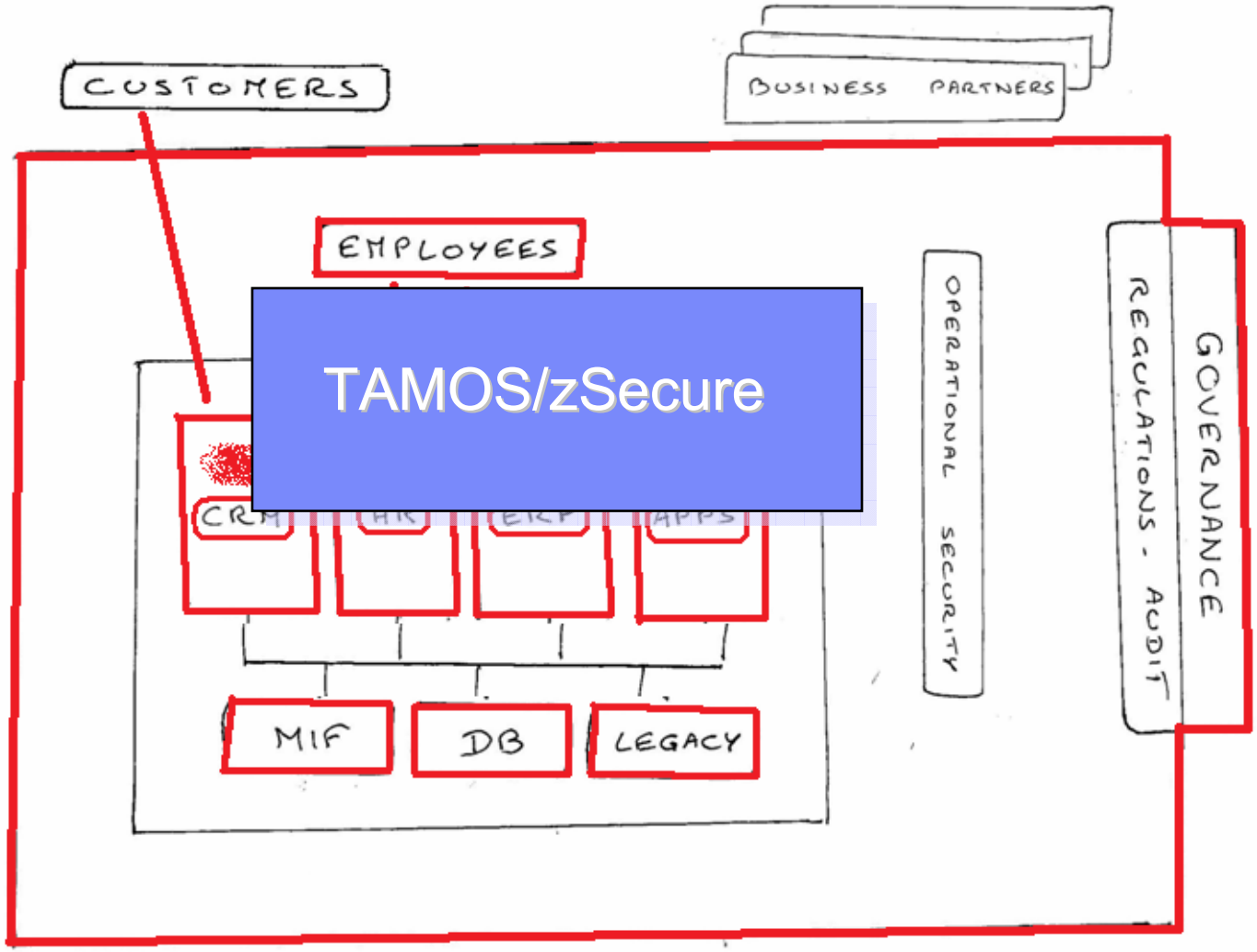
A organização precisa ser protegida contra pessoas indesejadas



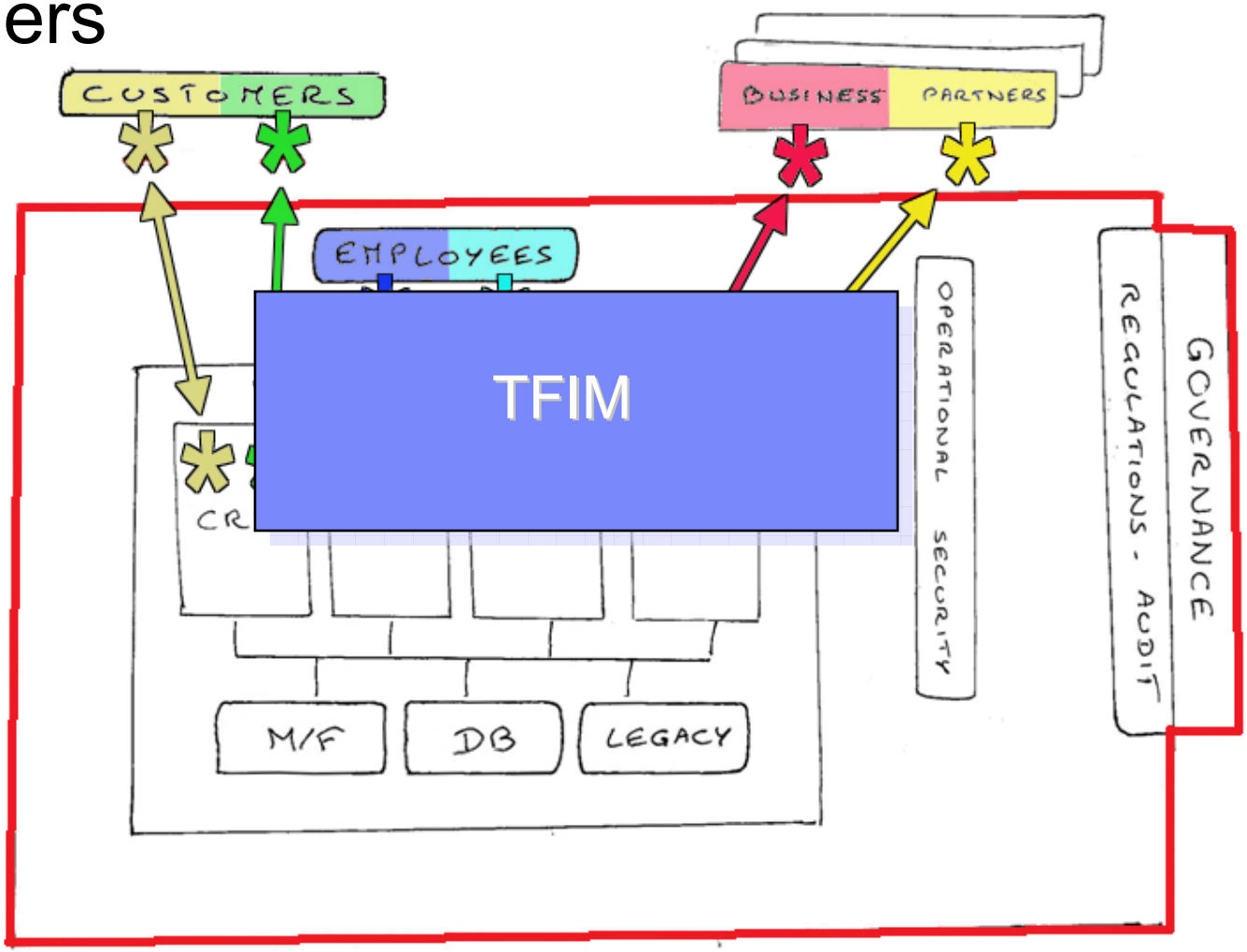
Gerenciar acessos e autorizações para proteger as aplicações contra ataques



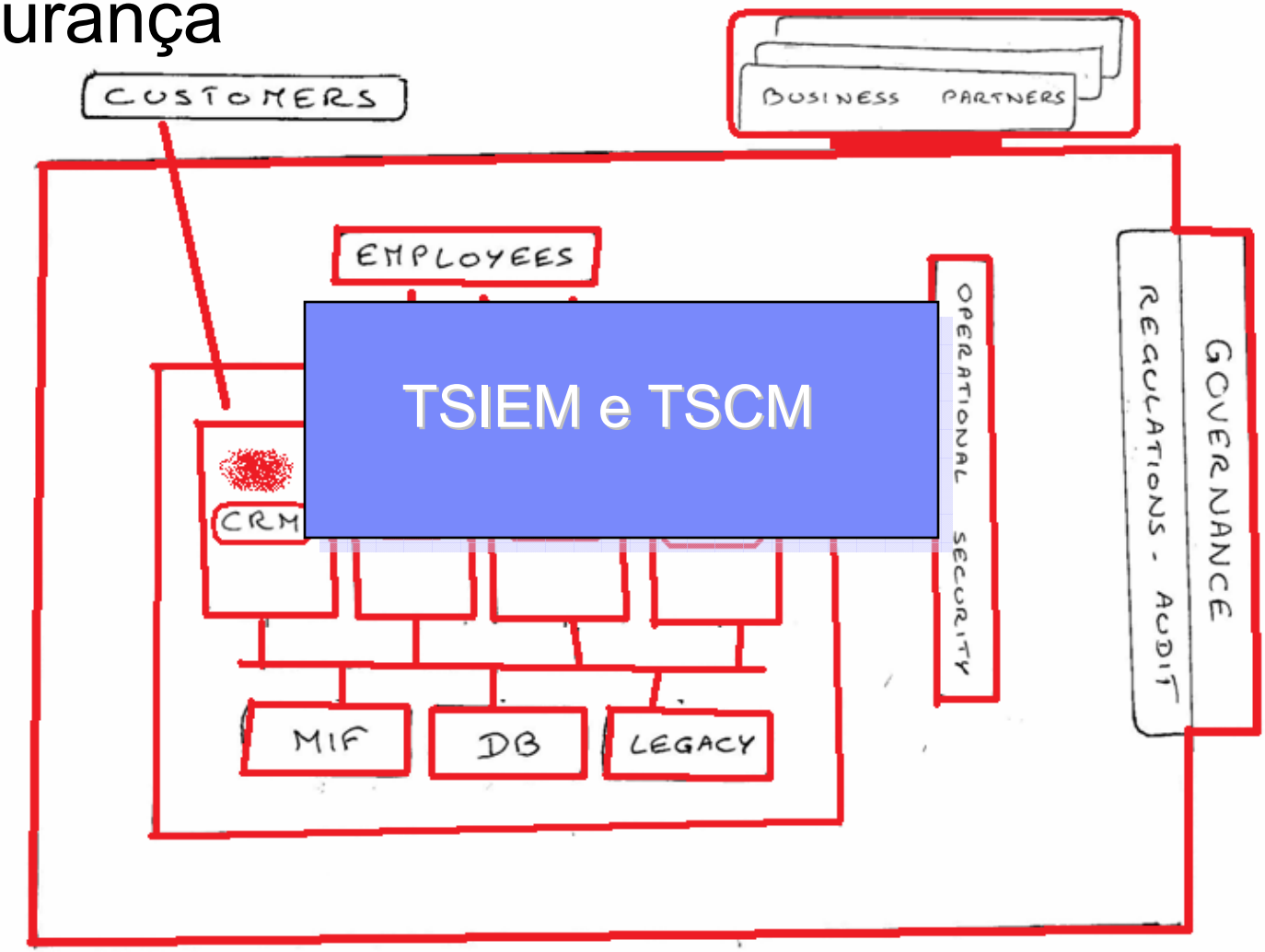
Como também os sistemas críticos



Proteger a federação de identidades com Business Partners



E isto precisará ser controlado pelo time de segurança



Reconhecimento de analistas de Mercado

	Título		Status 2006/7
Gartner	ISS Network Security, Firewalls and Managed Services		Leader
FROST & SULLIVAN	Identity Management (TIM , TAM, FIM, TDI, TDS)		Leader
FORRESTER	Wave: User Account Provisioning (TIM)		Leader
FORRESTER	Wave: Enterprise Security Information Management (Consul InSight)		Leader
Gartner	MQ: User Provisioning (TIM)		Leader
Gartner	MQ: Security Information & Event Management (TSOM, Consul InSight)		Challenger
Gartner	MQ: Web Access Management (TAM)		Leader
IDC Analyze the Future	Managed Security Services (Marketshare)		Leader
FROST & SULLIVAN	Marketshare: Identity and Access Management		Ranked #1

Porque IBM?

Abrangência e Solução com profundidade	Único fornecedor que proporciona abrangência da segurança e capacidades de conformidade para endereçar infraestrutura, aplicativos, informação, pessoal e identidades
Integração Extensiva	Integra com todos os tipos de dados de negócios (estruturado, semi-estruturado, e desestruturado) para endereçar informação e necessidade de segurança de dados e todos os principais tipos de aplicativos (web, legado, e ESB para SOA) para assegurar os processos de negócios
Padrões Abertos	Plataforma aberta de segurança e liderança em segurança em Web Services, gestão de políticas e identidade federada
Liderança do Produto	Liderança atestada por analistas em mercados para usuário e segurança de infraestrutura e software de conformidade e serviços
Melhor na classe System z security	Liderança em segurança de mainframe com RACF, z/OS security, identidade e acesso e conformidade permitindo clientes a alavancar o System z como o hub de segurança corporativa
Elemento central do IBM Service Management	Integração de segurança out-of-the-box com os processos chave de ITIL : Incidente, Problema, Troca, Release, SLA, Configuração, Disponibilidade
Gerenciamento e oferta da abrangência de serviço	IBM oferece abrangência total de solução de gestão de serviços e controle de ativos ponta a ponta que operam em uma infraestrutura comum de serviços web

Obrigado !!!

धन्यवाद
Hindi

多謝
Traditional Chinese

ขอบคุณ
Thai

Спасибо
Russian

Gracias
Spanish

Thank You
English

شكرا
Arabic

Obrigado
Brazilian Portuguese

多谢
Simplified Chinese

Danke
German

Grazie
Italian

Merci
French

நன்றி
Tamil

ありがとうございました
Japanese

감사합니다
Korean