Cloud Security

Jean-François Pujol

Cisco Systems

Quick reminder :
Cloud Deployment Model

NIST Deployment Models

Public Cloud	Cloud infrastructure made available to the general public.
Private Cloud	Cloud infrastructure operated solely for an organization.
Hybrid Cloud	Cloud infrastructure composed of two or more clouds that interoperate or federate through technology
Community Cloud	Cloud infrastructure shared by several organizations and supporting a specific community

… and one other

Virtual Private Cloud	Cloud services that simulate the private cloud experience in public cloud infrastructure

Cisco Systems

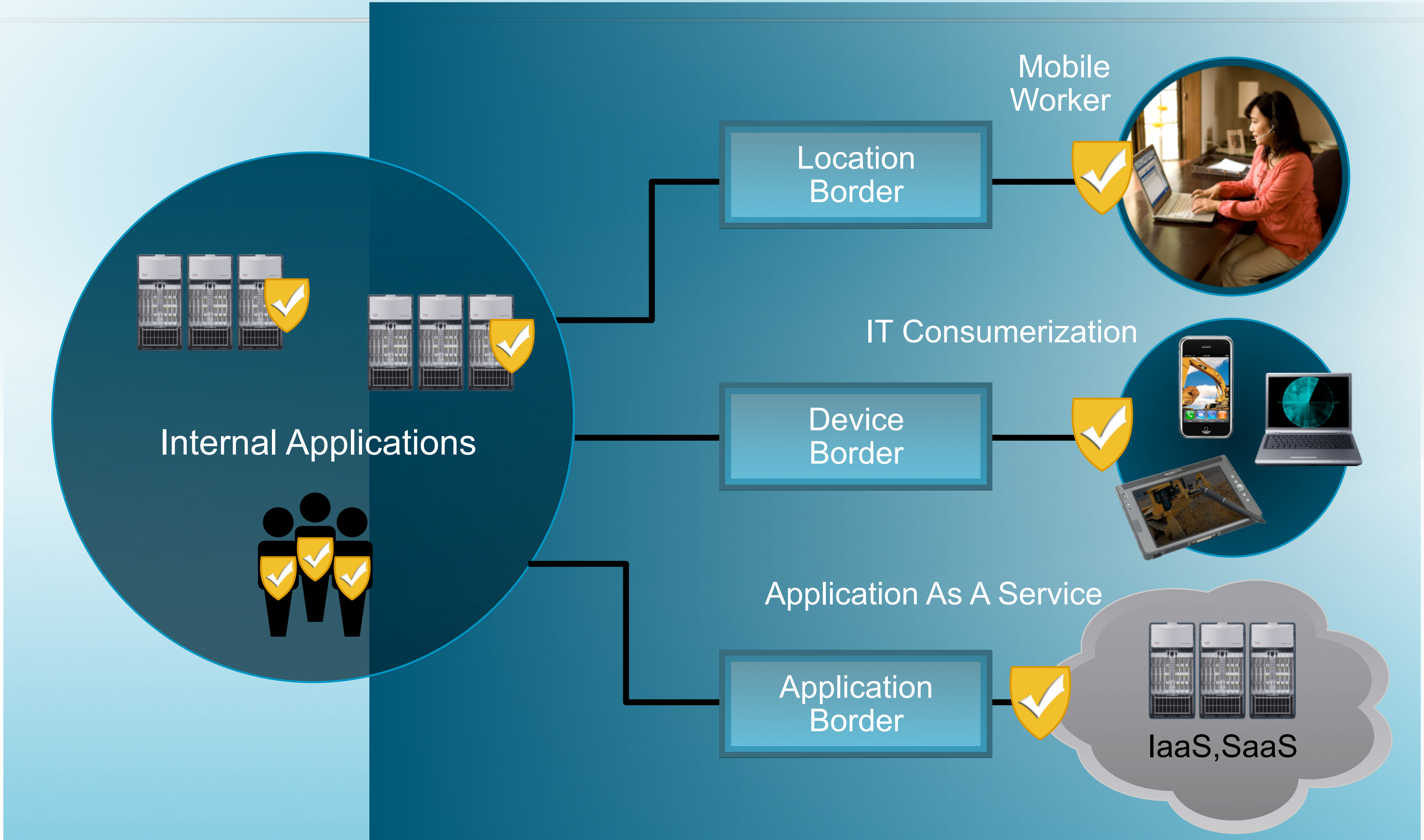
Public vs. Private Cloud Security

While the technology basement remains the same, we may consider two different approaches to the problem :

- Public Cloud :
  - Delegation versus Trust
- Private Cloud :
  - Abstraction / Virtualization versus Complexity

Considerations about the Public Cloud Security

The New World : Shifting Borders



Internal Applications

Location Border

Mobile Worker

IT Consumerization

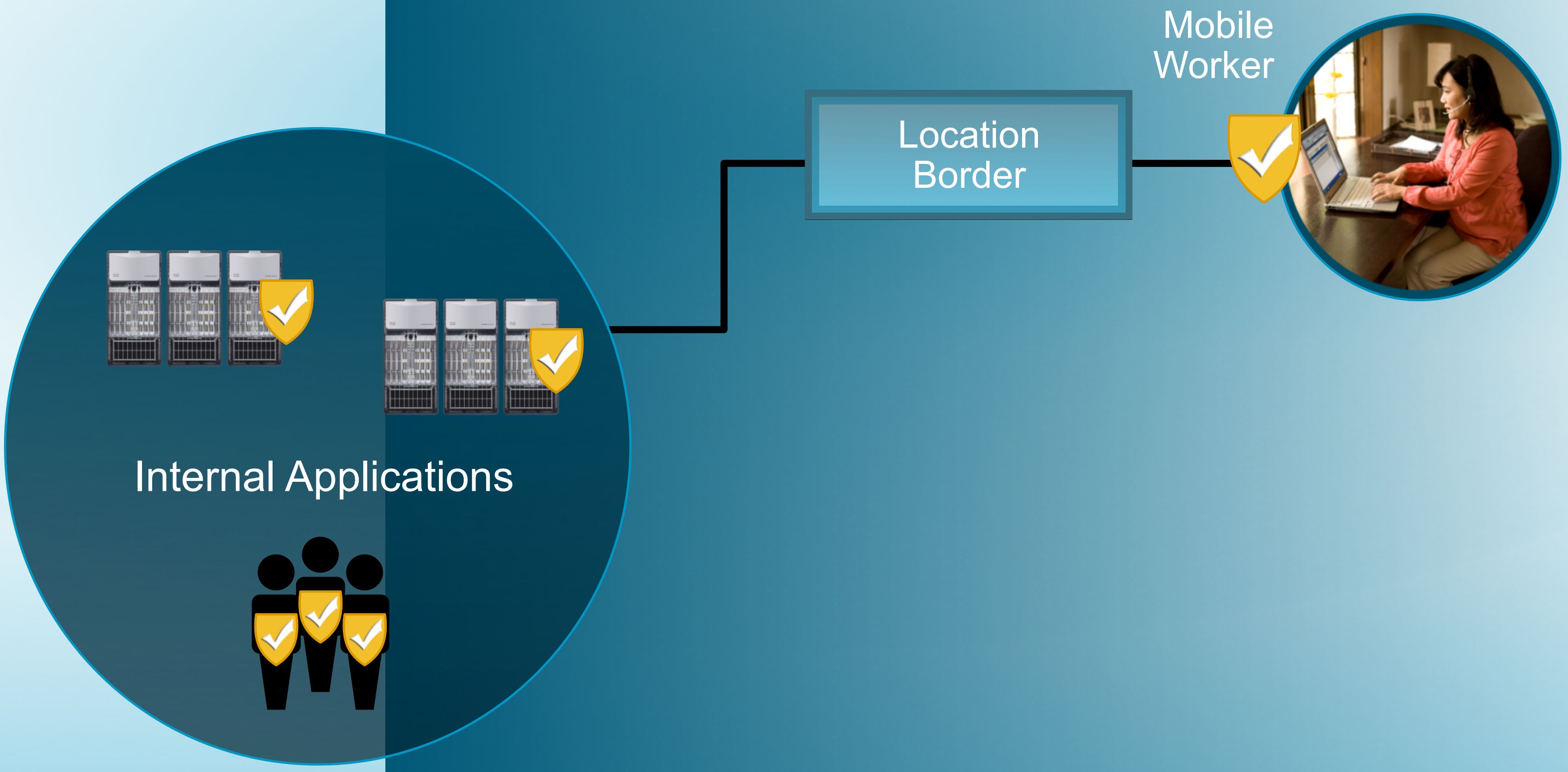
Device Border

Application As A Service

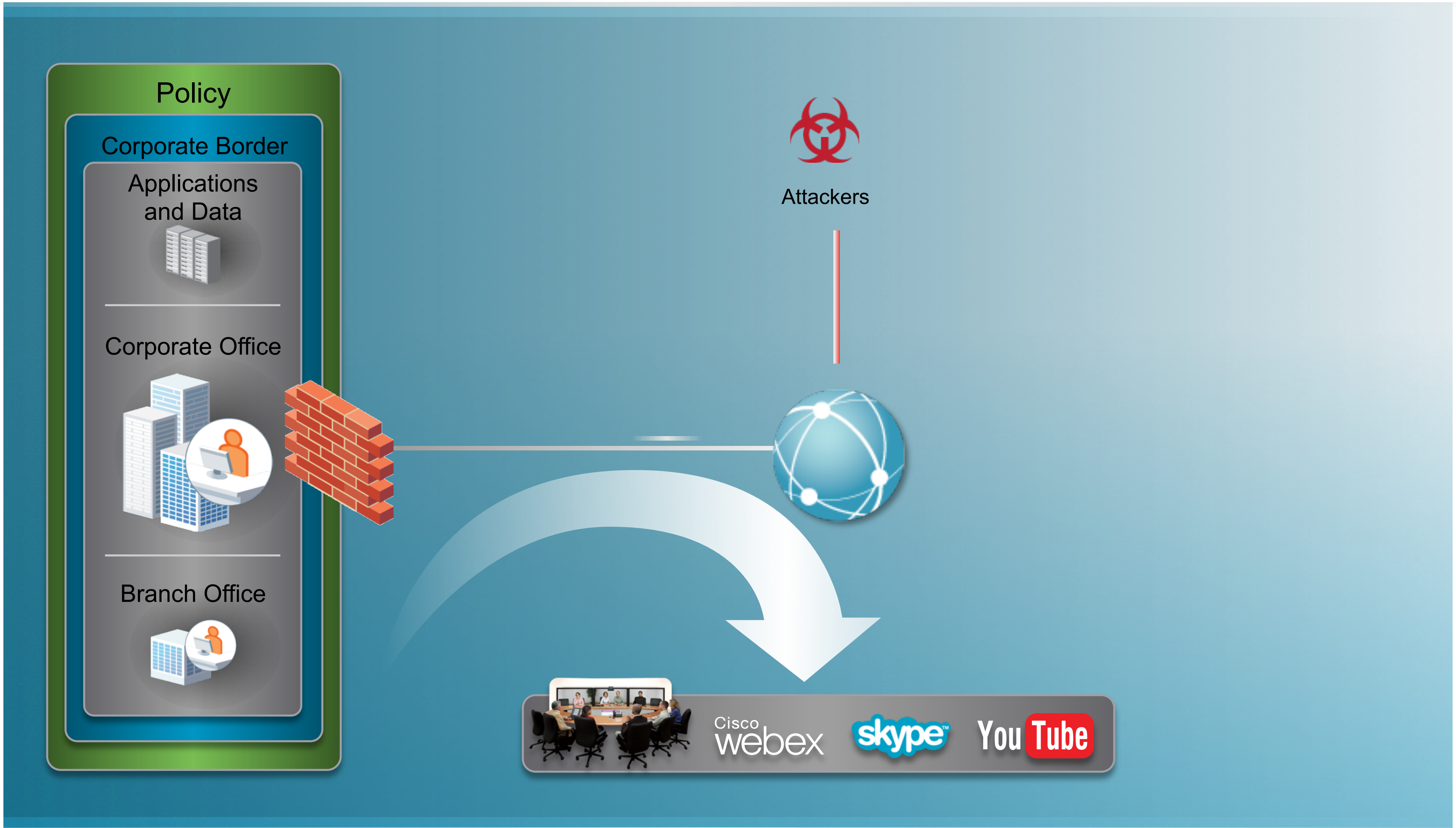
Application Border

IaaS,SaaS

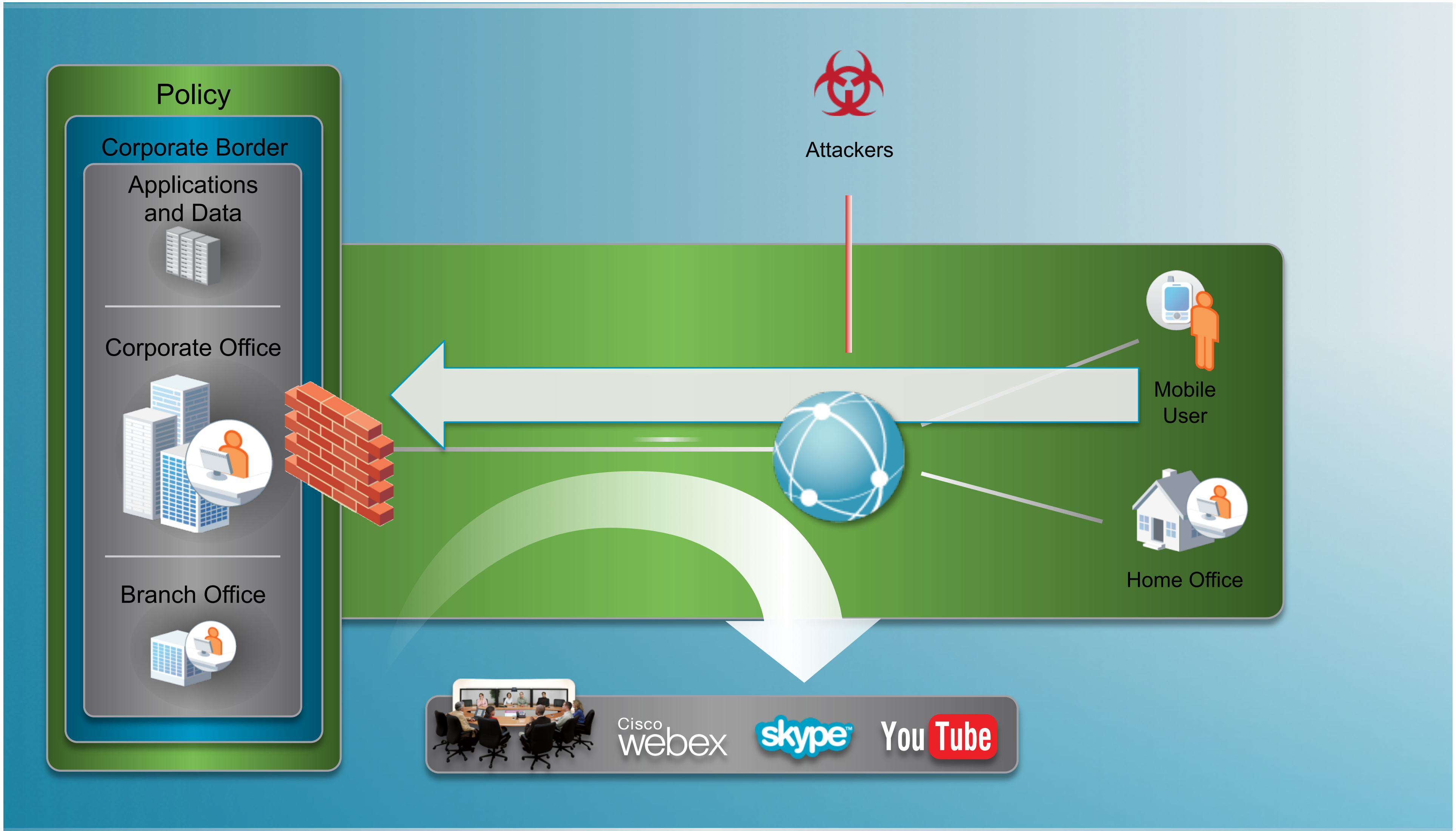
The (not so) New World : Location Border



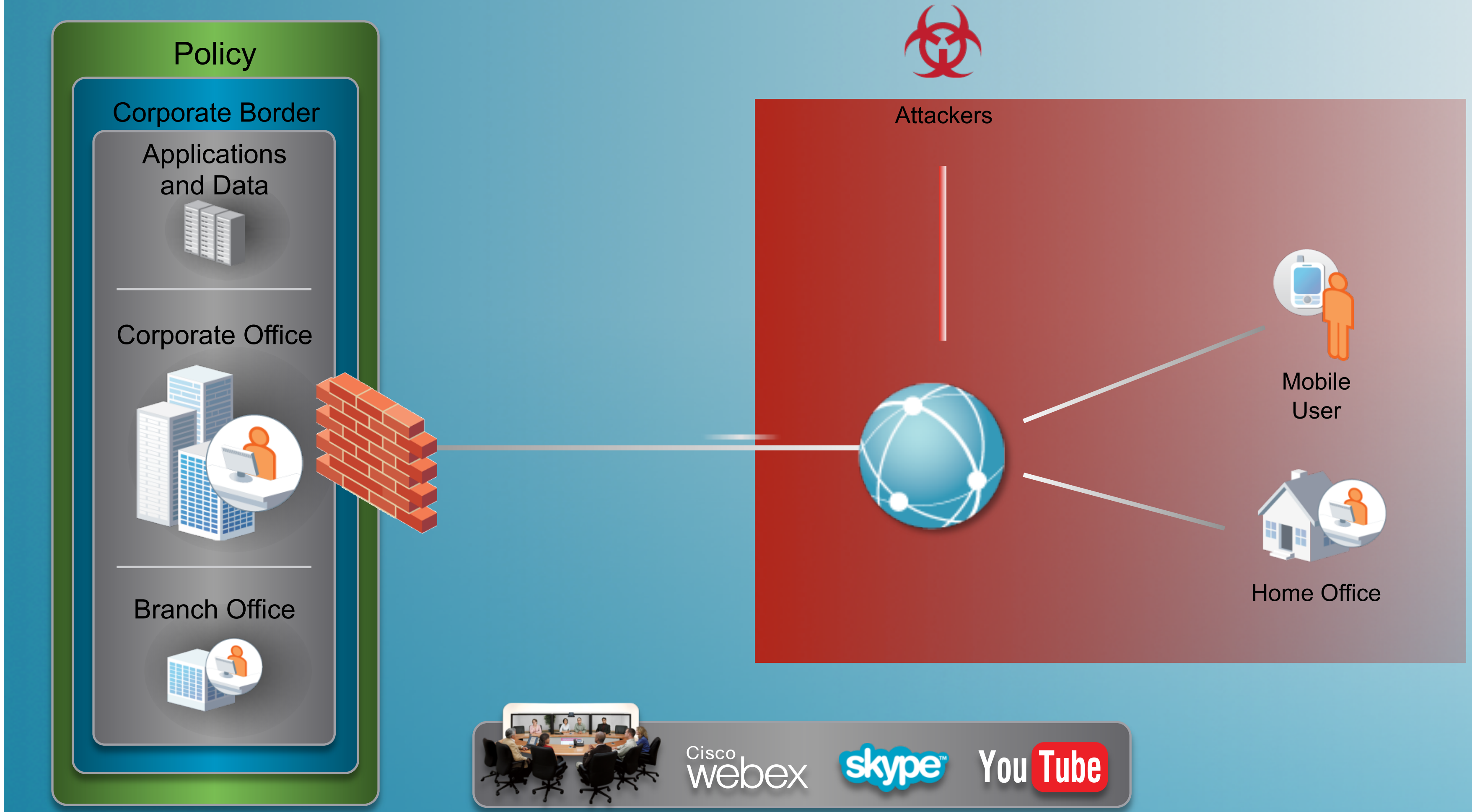
Traditional Corporate Border



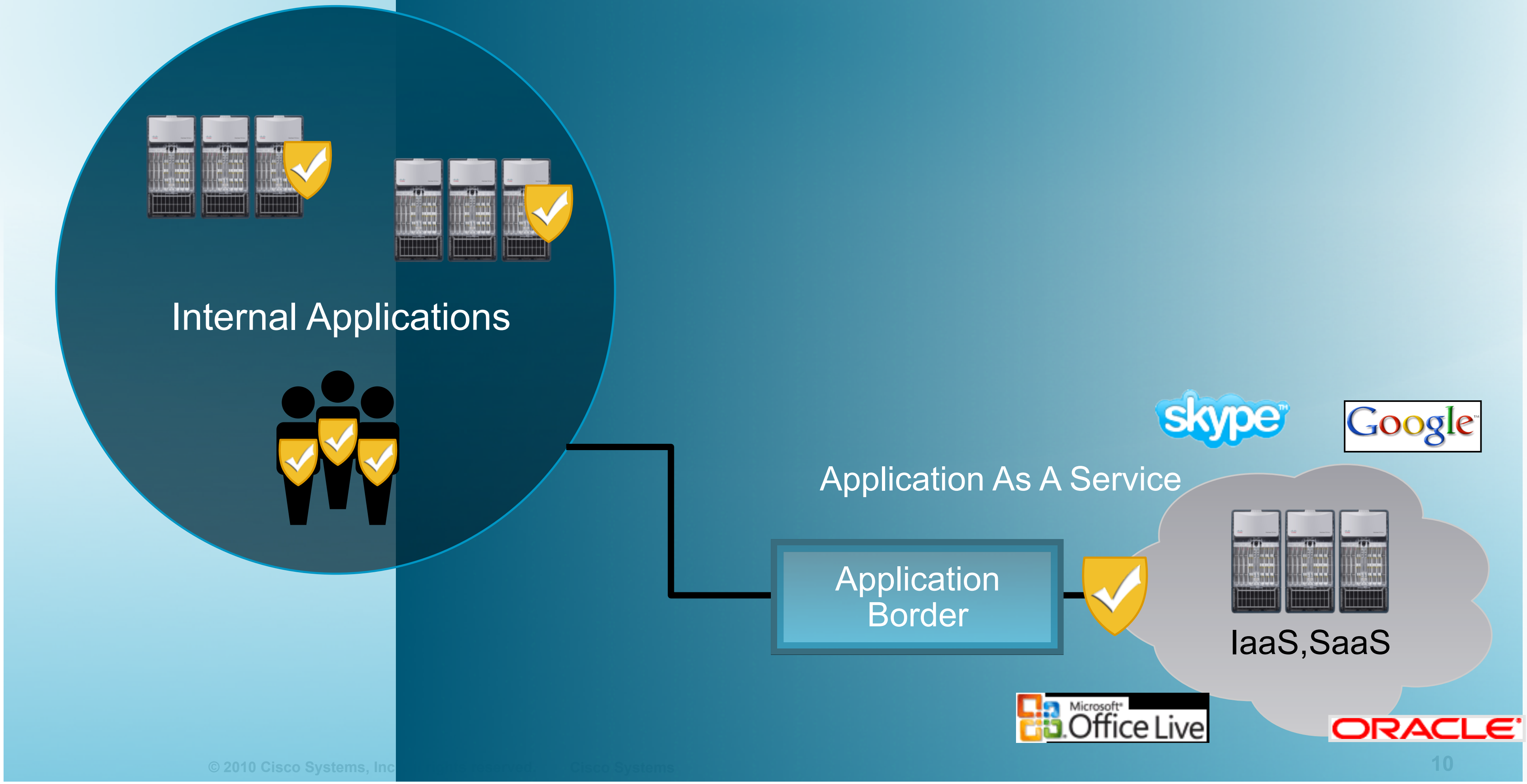
Now with Mobile Users and VPNs



With Mobile Users when not protected by VPNs…



The New World : Application Border



The Consumer's View of Cloud

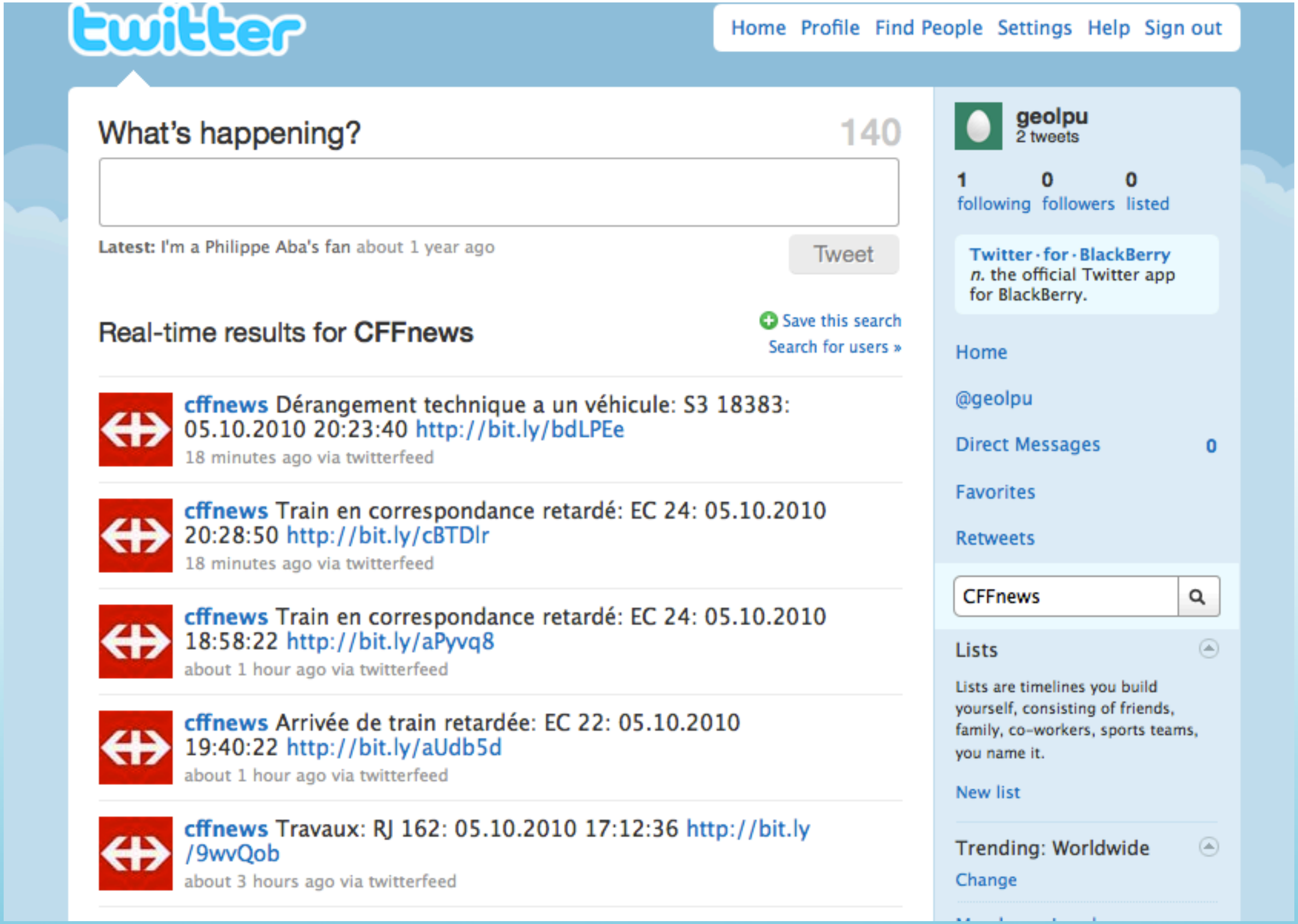
Gmail™
by Google
CARBONITE
Tuesday
9
mobile me
Blogger™
XBOX LIVE
mozy
BY DECHO
skype™
DANGER®
A Subsidiary of Microsoft®

...Everything is Cloud

These Cloudy Days …

- Internet is reliable
- Cloud services are well known in the consumer market, and the consumer market creates some pressure in the enterprise world.
- Is LinkedIn a consumer/personal or business service ?
- Enterprises are turning every single task into a process. It creates a strong traction for adopting services (OPEX vs CAPEX)

Organizations don’t have even the choice …



What’s happening? 140

Latest: I'm a Philippe Aba's fan about 1 year ago

Real-time results for CFFnews

cffnews Dérangement technique a un véhicule: S3 18383: 05.10.2010 20:23:40 http://bit.ly/bdLPEe
18 minutes ago via twitterfeed

cffnews Train en correspondance retardé: EC 24: 05.10.2010 20:28:50 http://bit.ly/cBTDlr
18 minutes ago via twitterfeed

cffnews Train en correspondance retardé: EC 24: 05.10.2010 18:58:22 http://bit.ly/aPyvq8
about 1 hour ago via twitterfeed

cffnews Arrivée de train retardée: EC 22: 05.10.2010 19:40:22 http://bit.ly/aUdb5d
about 1 hour ago via twitterfeed

cffnews Travaux: RJ 162: 05.10.2010 17:12:36 http://bit.ly/9wvQob
about 3 hours ago via twitterfeed

geolpu
2 tweets

1 following 0 followers 0 listed

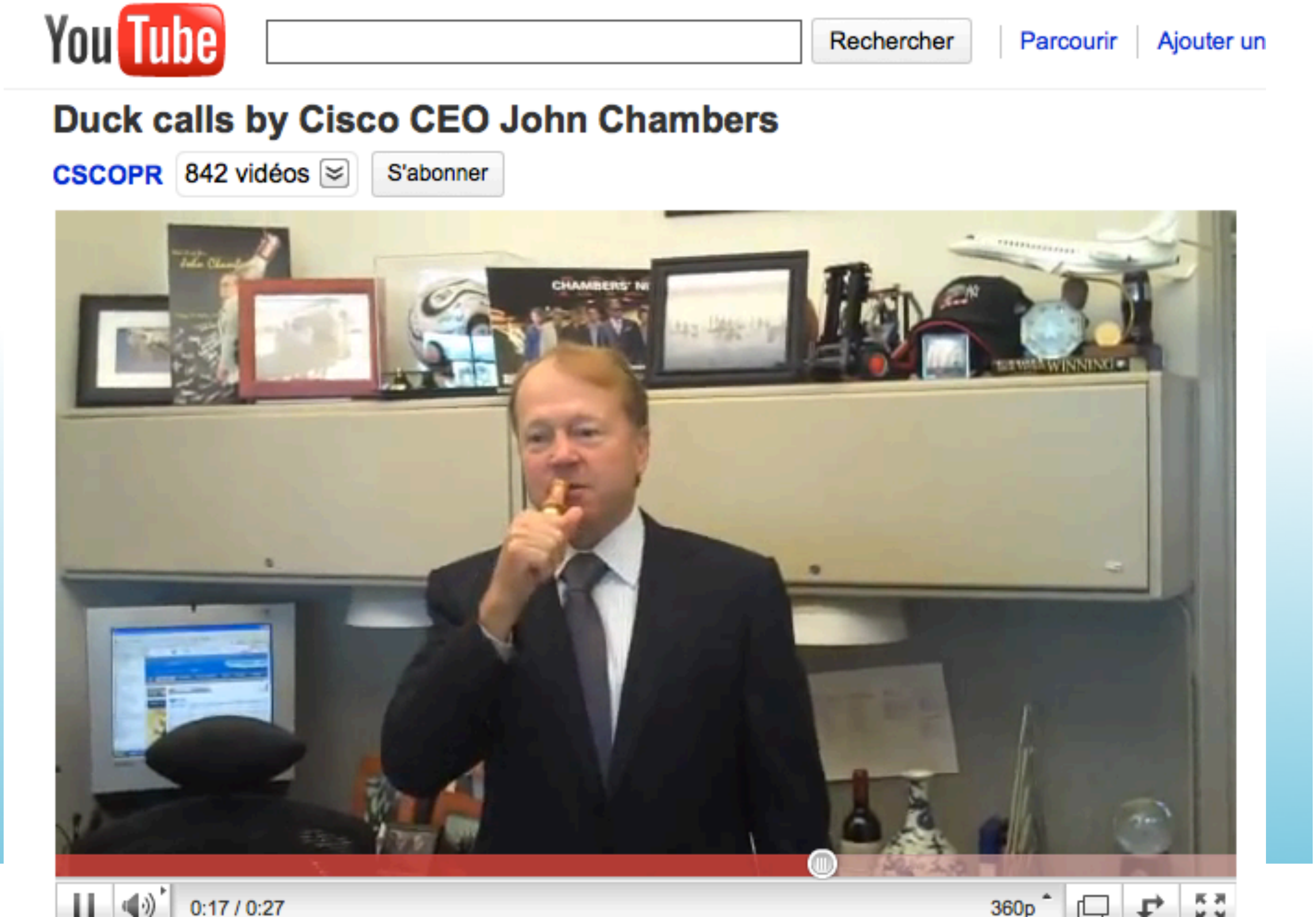
Twitter·for·BlackBerry
n. the official Twitter app for BlackBerry.

Lists

Lists are timelines you build yourself, consisting of friends, family, co-workers, sports teams, you name it.

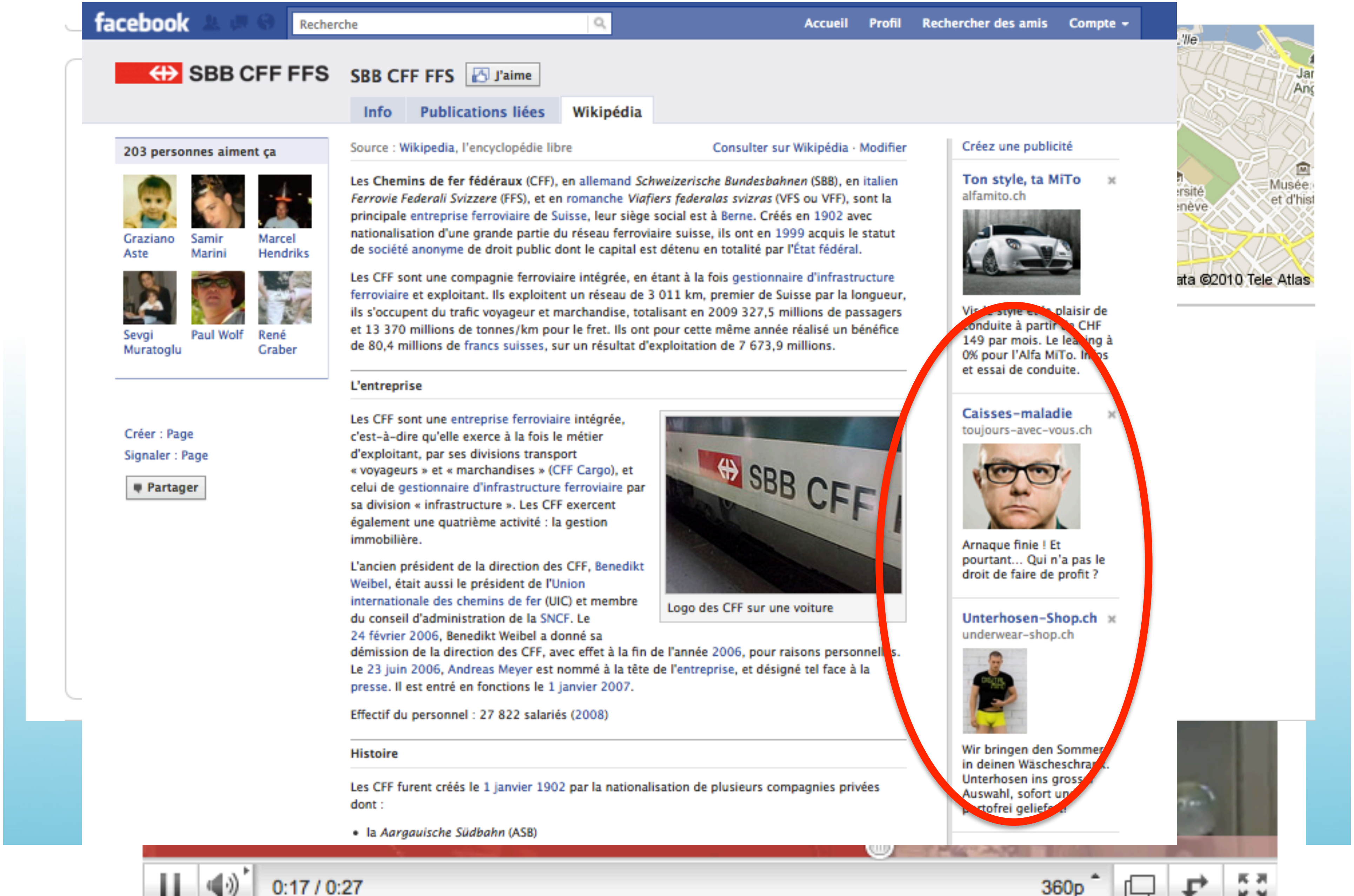
Trending: Worldwide

Organizations don't have even the choice …



Duck calls by Cisco CEO John Chambers

Organizations don't have even the choice …



Les **Chemins de fer fédéraux** (CFF), en allemand *Schweizerische Bundesbahnen* (SBB), en italien *Ferrovie Federali Svizzere* (FFS), et en romanche *Viafiers federalas svizras* (VFS ou VFF), sont la principale entreprise ferroviaire de Suisse, leur siège social est à Berne. Créés en 1902 avec nationalisation d'une grande partie du réseau ferroviaire suisse, ils ont en 1999 acquis le statut de société anonyme de droit public dont le capital est détenu en totalité par l'État fédéral.

Les CFF sont une compagnie ferroviaire intégrée, en étant à la fois gestionnaire d'infrastructure ferroviaire et exploitant. Ils exploitent un réseau de 3 011 km, premier de Suisse par la longueur, ils s'occupent du trafic voyageur et marchandise, totalisant en 2009 327,5 millions de passagers et 13 370 millions de tonnes/km pour le fret. Ils ont pour cette même année réalisé un bénéfice de 80,4 millions de francs suisses, sur un résultat d'exploitation de 7 673,9 millions.

L'entreprise

Les CFF sont une entreprise ferroviaire intégrée, c'est-à-dire qu'elle exerce à la fois le métier d'exploitant, par ses divisions transport « voyageurs » et « marchandises » (CFF Cargo), et celui de gestionnaire d'infrastructure ferroviaire par sa division « infrastructure ». Les CFF exercent également une quatrième activité : la gestion immobilière.

L'ancien président de la direction des CFF, Benedikt Weibel, était aussi le président de l'Union internationale des chemins de fer (UIC) et membre du conseil d'administration de la SNCF. Le 24 février 2006, Benedikt Weibel a donné sa démission de la direction des CFF, avec effet à la fin de l'année 2006, pour raisons personnelles. Le 23 juin 2006, Andreas Meyer est nommé à la tête de l'entreprise, et désigné tel face à la presse. Il est entré en fonctions le 1 janvier 2007.

Effectif du personnel : 27 822 salariés (2008)

Histoire

Les CFF furent créés le 1 janvier 1902 par la nationalisation de plusieurs compagnies privées dont :

- la *Aargauische Südbahn* (ASB)

Ton style, ta MiTo
alfamito.ch

Vis le style et le plaisir de conduite à partir de CHF 149 par mois. Le leasing à 0% pour l'Alfa MiTo. Infos et essai de conduite.

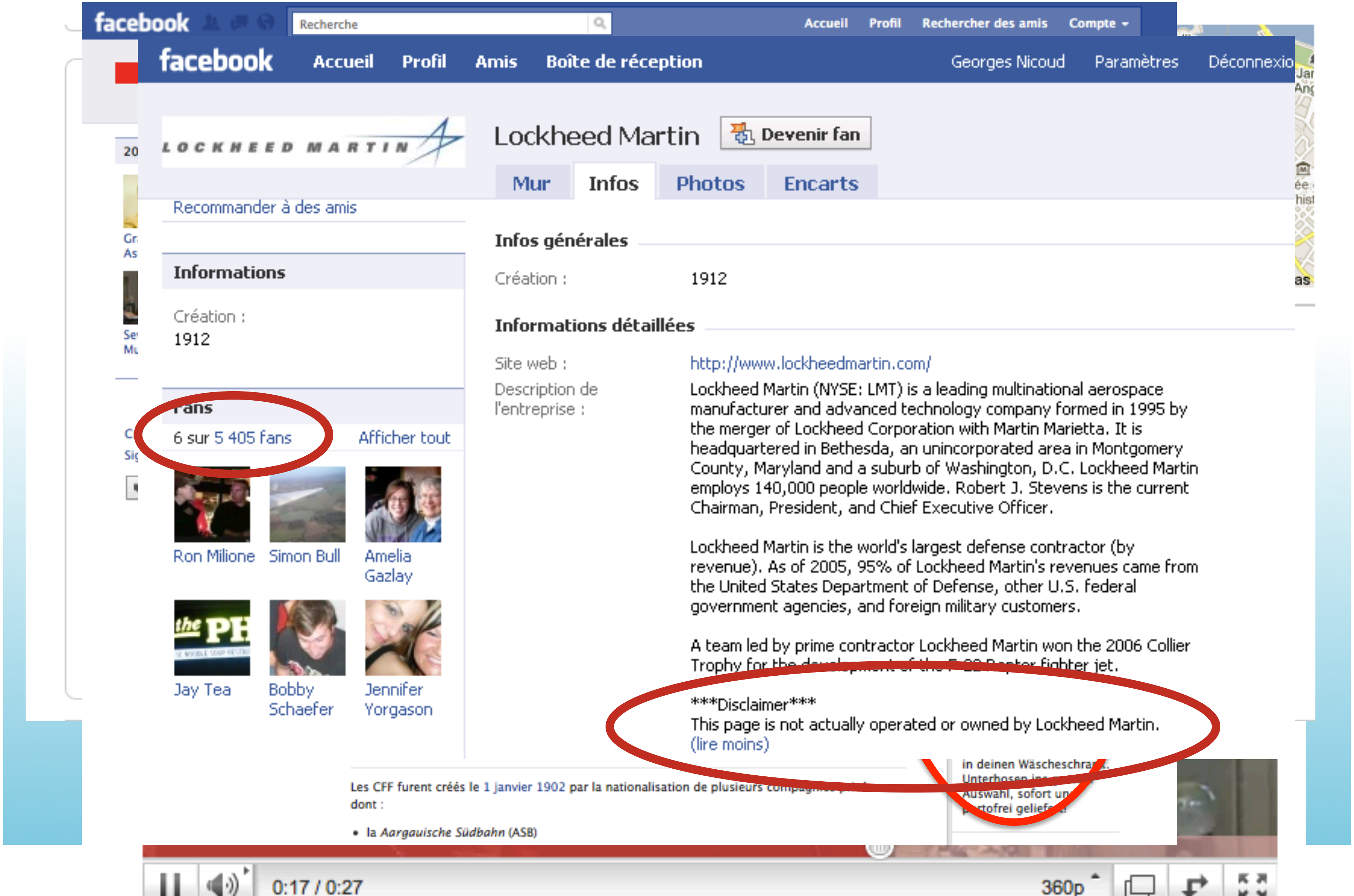
Caisses-maladie
toujours-avec-vous.ch

Arnaque finie ! Et pourtant... Qui n'a pas le droit de faire de profit ?

Unterhosen-Shop.ch
underwear-shop.ch

Wir bringen den Sommer in deinen Wäscheschrank. Unterhosen ins grosser Auswahl, sofort und portofrei geliefert!

Organizations don't have even the choice …



Lockheed Martin

Informations

Création :
1912

Fans

6 sur 5 405 fans

Ron Milione, Simon Bull, Amelia Gazlay, Jay Tea, Bobby Schaefer, Jennifer Yorgason

Infos générales

Création : 1912

Informations détaillées

Site web : http://www.lockheedmartin.com/

Description de l'entreprise :

Lockheed Martin (NYSE: LMT) is a leading multinational aerospace manufacturer and advanced technology company formed in 1995 by the merger of Lockheed Corporation with Martin Marietta. It is headquartered in Bethesda, an unincorporated area in Montgomery County, Maryland and a suburb of Washington, D.C. Lockheed Martin employs 140,000 people worldwide. Robert J. Stevens is the current Chairman, President, and Chief Executive Officer.

Lockheed Martin is the world's largest defense contractor (by revenue). As of 2005, 95% of Lockheed Martin's revenues came from the United States Department of Defense, other U.S. federal government agencies, and foreign military customers.

A team led by prime contractor Lockheed Martin won the 2006 Collier Trophy for the development of the F-22 Raptor fighter jet.

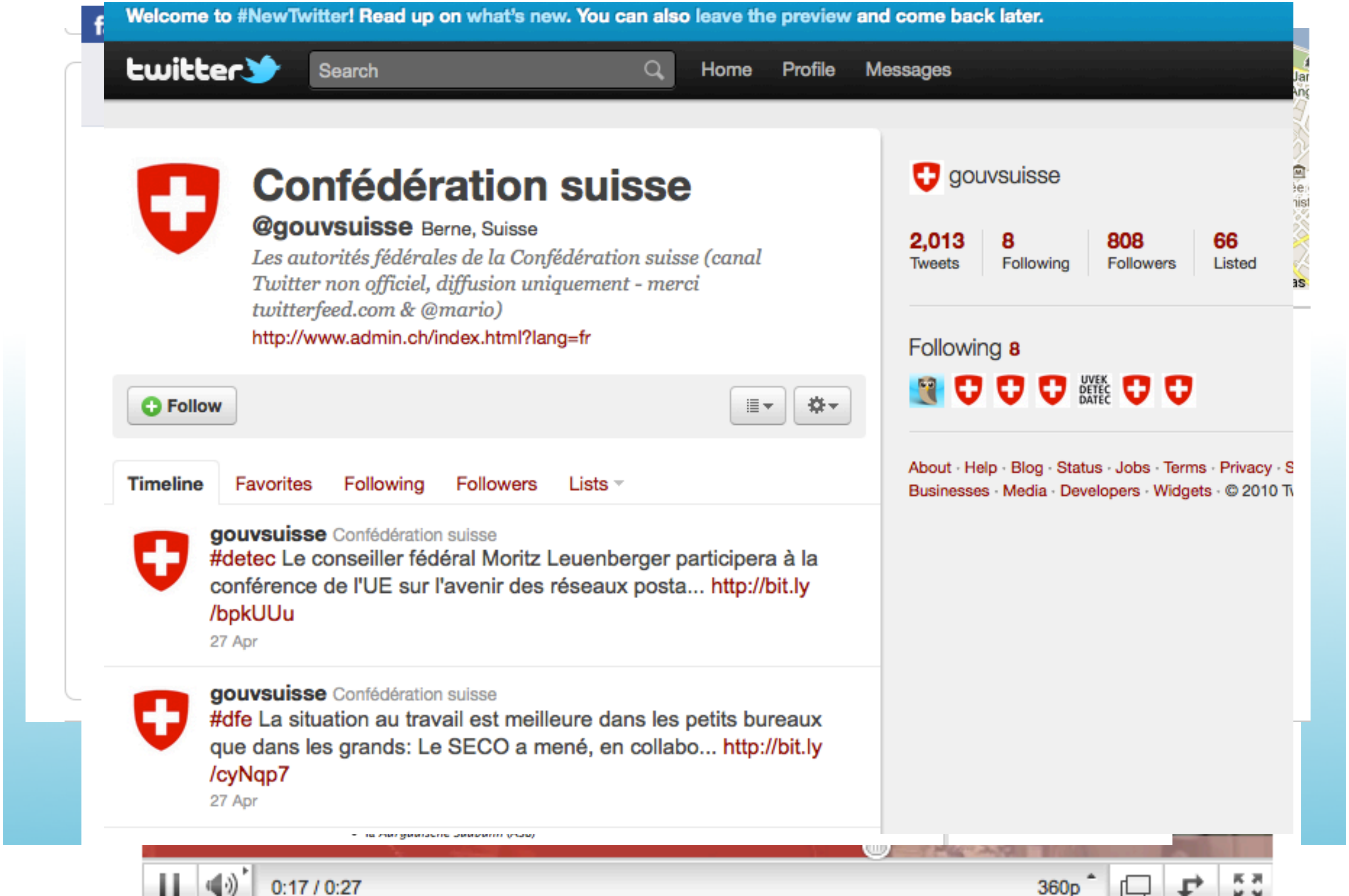
Disclaimer
This page is not actually operated or owned by Lockheed Martin.
(lire moins)

Les CFF furent créés le 1 janvier 1902 par la nationalisation de plusieurs compagnies ... dont :

- la *Aargauische Südbahn* (ASB)

in deinen Wäscheschrank. Unterhosen ... Auswahl, sofort un... portofrei geliefert!

Organizations don’t have even the choice …



Welcome to #NewTwitter! Read up on what's new. You can also leave the preview and come back later.

Confédération suisse

@gouvsuisse Berne, Suisse

Les autorités fédérales de la Confédération suisse (canal Twitter non officiel, diffusion uniquement - merci twitterfeed.com & @mario)

http://www.admin.ch/index.html?lang=fr

gouvsuisse Confédération suisse
#detec Le conseiller fédéral Moritz Leuenberger participera à la conférence de l'UE sur l'avenir des réseaux posta... http://bit.ly/bpkUUu
27 Apr

gouvsuisse Confédération suisse
#dfe La situation au travail est meilleure dans les petits bureaux que dans les grands: Le SECO a mené, en collabo... http://bit.ly/cyNqp7
27 Apr

gouvsuisse

2,013	8	808	66
Tweets	Following	Followers	Listed

Following 8

About · Help · Blog · Status · Jobs · Terms · Privacy · S
Businesses · Media · Developers · Widgets · © 2010 Tw

First security concern

- Enterprises are using unmanaged cloud services today
  - in a more or less control way
- On public and (almost) free consumer platforms :
  - No real control over the corporate image
  - Risks of information leakage
  - Risks of misleading
  - Risks of Social Engineering attacks

Global trend for outsourcing

- Every business process is analyzed :
  - Down to a single application
  - Down to any individual
- If you can define it, measure it, and it is not a core business activity, you want to outsource it

Can you afford to manage the risk ?
Imagine you have :

- A couple of consultants
- Employees under temporary contract
- A complete department is outsourced (Dev, Marketing, etc…)
- Datacenter exploitation is outsourced
- Networks, servers, premises, and people are outsourced
- Cloud based services

Key to Broader Adoption of Cloud: Trust

Security

Control

Service-Level Management

Compliance

Before the Economics of Cloud Computing Can be Considered, Organizations Require a Trusted Service Infrastructure

Enterprise Deployment Models

Distinguishing between Ownership and Control

Ownership

Internal Resources

All cloud resources owned by or dedicated to enterprise

External Resources

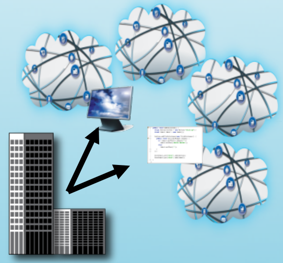
All cloud resources owned by providers; used by many customers

Control

Private Cloud

Cloud definition/ governance controlled by enterprise

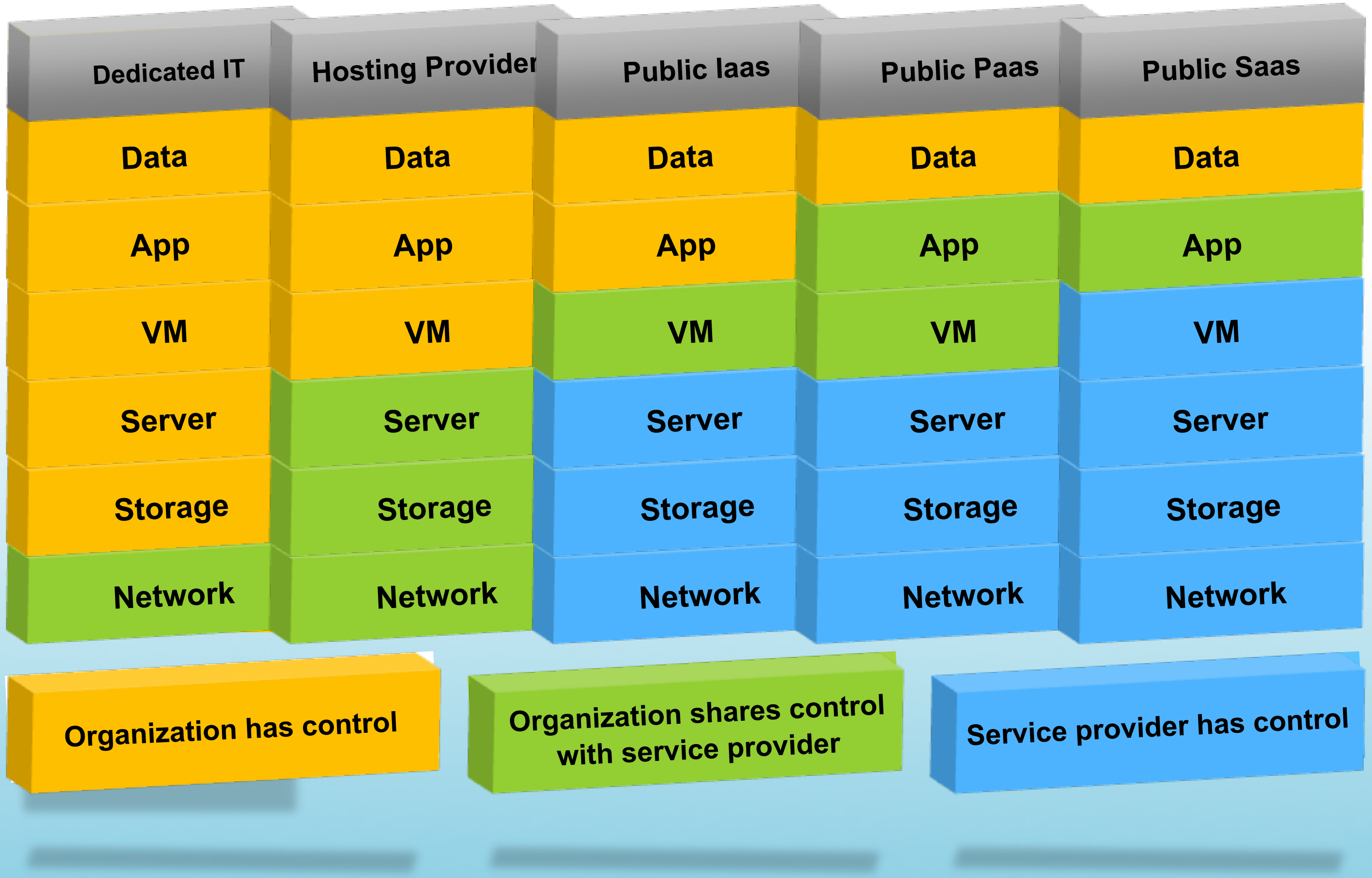
Public Cloud



Cloud definition/ governance controlled by provider

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Systems

Control and Trust evolve with cloud



Dedicated IT	Hosting Provider	Public Iaas	Public Paas	Public Saas
🟨 Data	🟨 Data	🟨 Data	🟨 Data	🟨 Data
🟨 App	🟨 App	🟨 App	🟩 App	🟩 App
🟨 VM	🟨 VM	🟩 VM	🟩 VM	🟦 VM
🟨 Server	🟩 Server	🟦 Server	🟦 Server	🟦 Server
🟨 Storage	🟩 Storage	🟦 Storage	🟦 Storage	🟦 Storage
🟩 Network	🟩 Network	🟦 Network	🟦 Network	🟦 Network

🟨 Organization has control

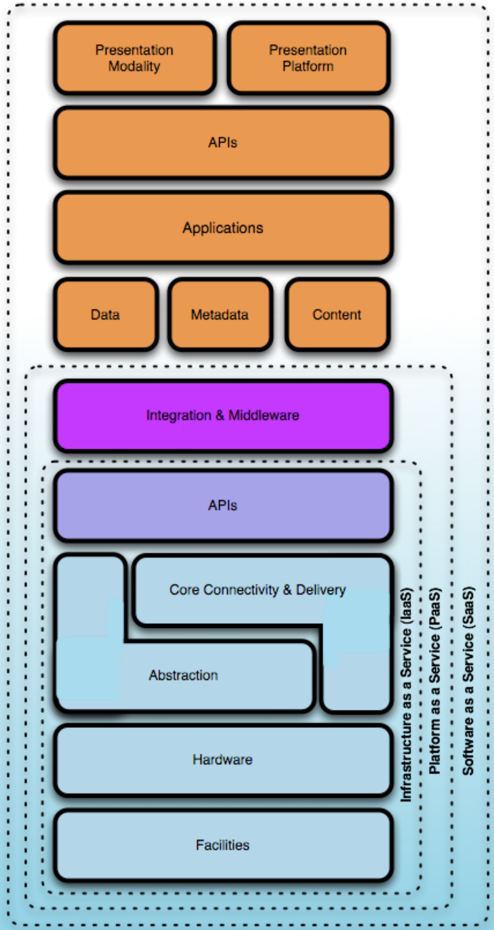
🟩 Organization shares control with service provider

🟦 Service provider has control

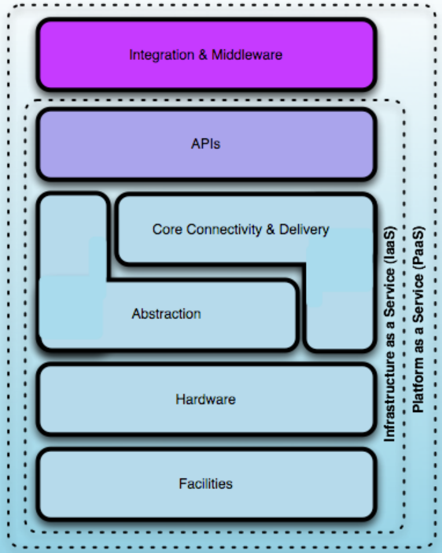
What This Means To Security

The lower down the stack the Cloud provider stops, the more security **you** are tactically responsible for implementing & managing yourself.

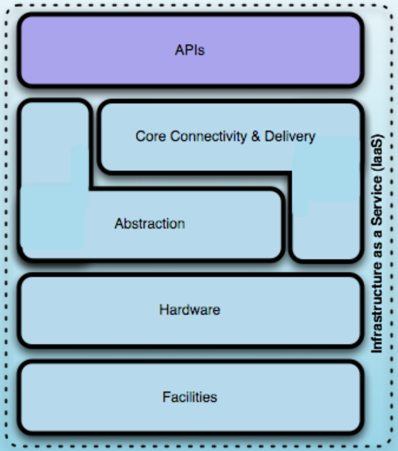
Salesforce - SaaS



Google AppEngine - PaaS


Integration & Middleware
APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)

Amazon EC2 - IaaS


APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)

Cloud Security Alliance - Guidance

The Cloud Security Alliance's 13 Critical Areas Of Focus for Cloud:

1. Architecture & Framework	
Governing the Cloud	***Operating the Cloud***
2. Governance & Risk Mgmt	8. Traditional BCM, DR
3. Legal & Electronic Discovery	9. Datacenter Operations
5. Compliance & Audit	10. Incident Response
6. Information Lifecycle Mgmt	11. Application Security
7. Portability & Interoperability	12. Encryption & Key Mgmt
	13. Identity & Access Mgmt

CSA cloud security alliance

www.cloudsecurityalliance.org

Cloud Security Alliance
Top Threats to Cloud Computing

The Cloud Security Alliance's Top Threats to Cloud Computing V1.0 :

1. Abuse and Nefarious Use of Cloud
2. Insecure Interfaces and APIs
3. Malicious Insiders
4. Shared Technology
5. Data Loss or
6. Account or Service Hijacking
7. Unknown Risk Profile

www.cloudsecurityalliance.org

Some important factors to consider for the service

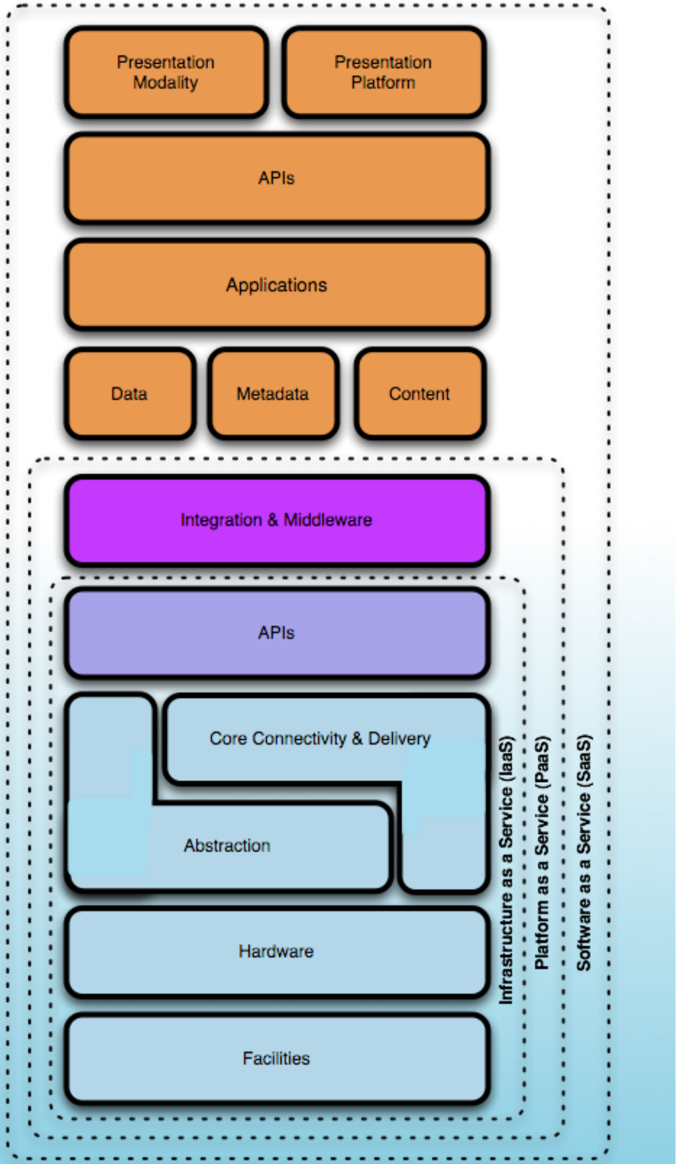
- Single Tenancy / Multi-tenancy
- Isolated Data / Co-mingled Data
- Dedicated Security / Socialist Security
- On-premise / Off-premise

CloudAudit & the A6 Deliverable

- Provide a common interface and namespace that allows cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance (A6) of their environments

- Allow authorized consumers of services to do likewise via an open, extensible and secure interface and methodology.

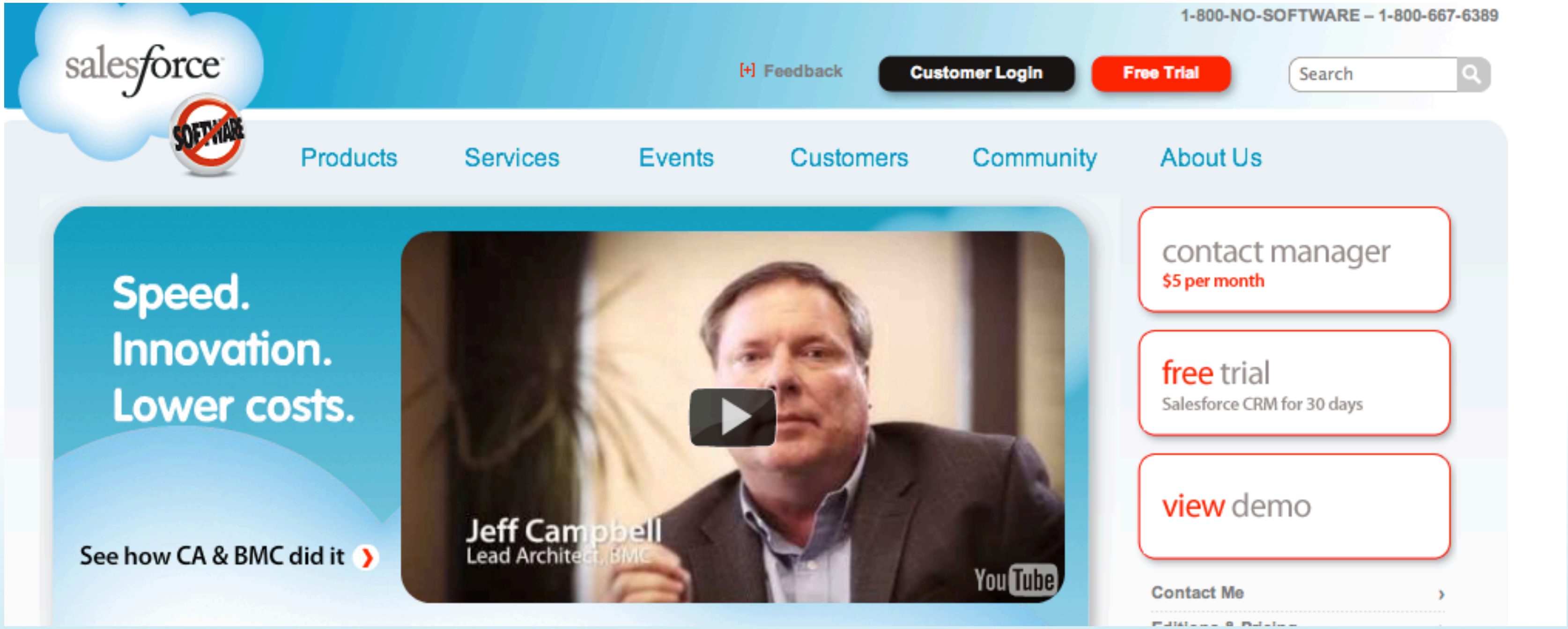
http://www.cloudaudit.org



That is the question …

- May your private organization be potentially more secure than a public cloud service ?
- (and/or cheaper …)

Saleforce.com



Speed. Innovation. Lower costs.

See how CA & BMC did it ›

Jeff Campbell
Lead Architect, BMC

contact manager
$5 per month

free trial
Salesforce CRM for 30 days

view demo

Contact Me ›

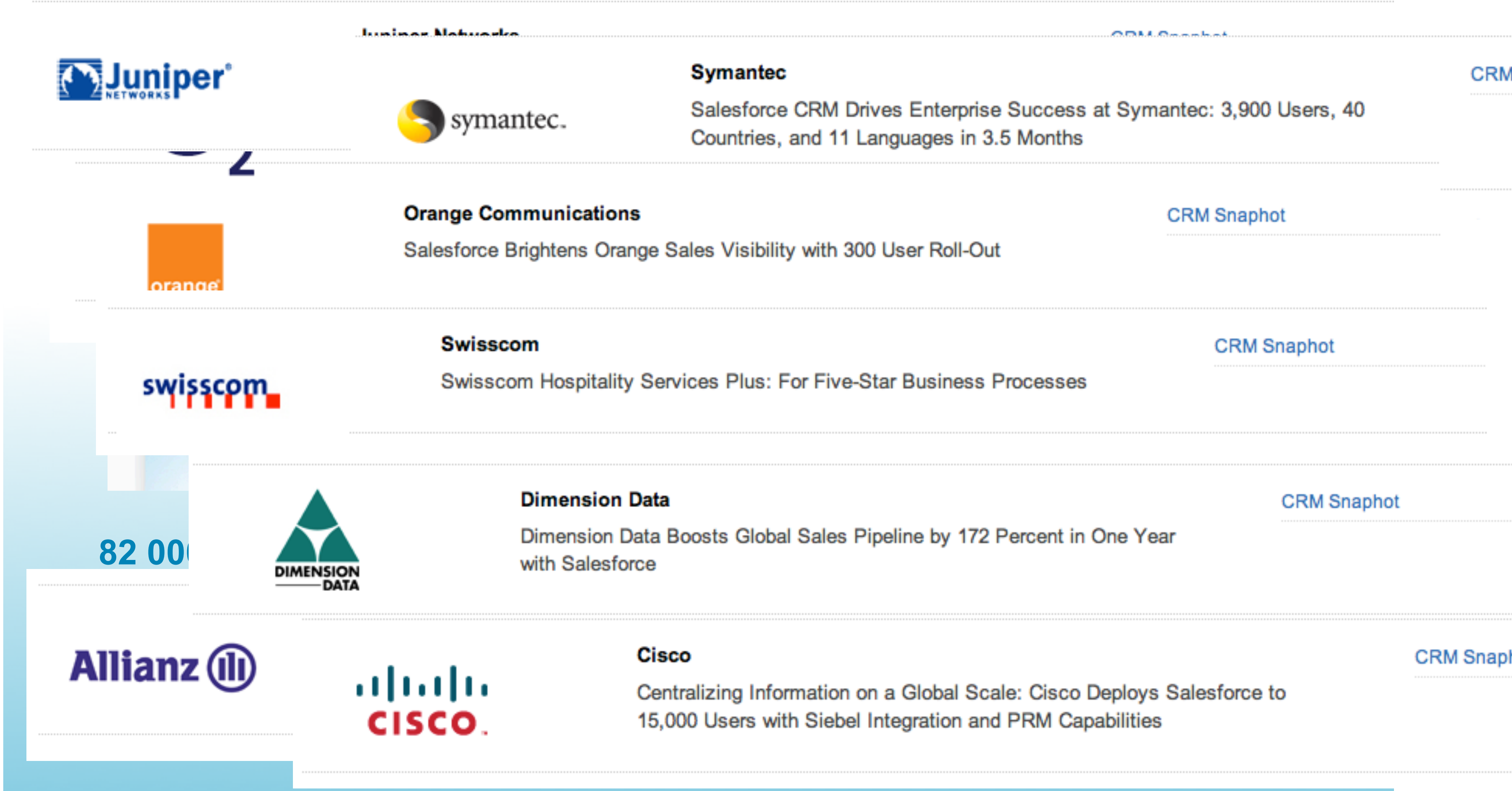
82 000 + customers …

Cisco

Centralizing Information on a Global Scale: Cisco Deploys Salesforce to 15,000 Users with Siebel Integration and PRM Capabilities

CRM Snaphot

Saleforce.com



Juniper Networks

CRM Snaphot

Symantec

Salesforce CRM Drives Enterprise Success at Symantec: 3,900 Users, 40 Countries, and 11 Languages in 3.5 Months

CRM

Orange Communications

Salesforce Brightens Orange Sales Visibility with 300 User Roll-Out

CRM Snaphot

Swisscom

Swisscom Hospitality Services Plus: For Five-Star Business Processes

CRM Snaphot

82 00

Dimension Data

Dimension Data Boosts Global Sales Pipeline by 172 Percent in One Year with Salesforce

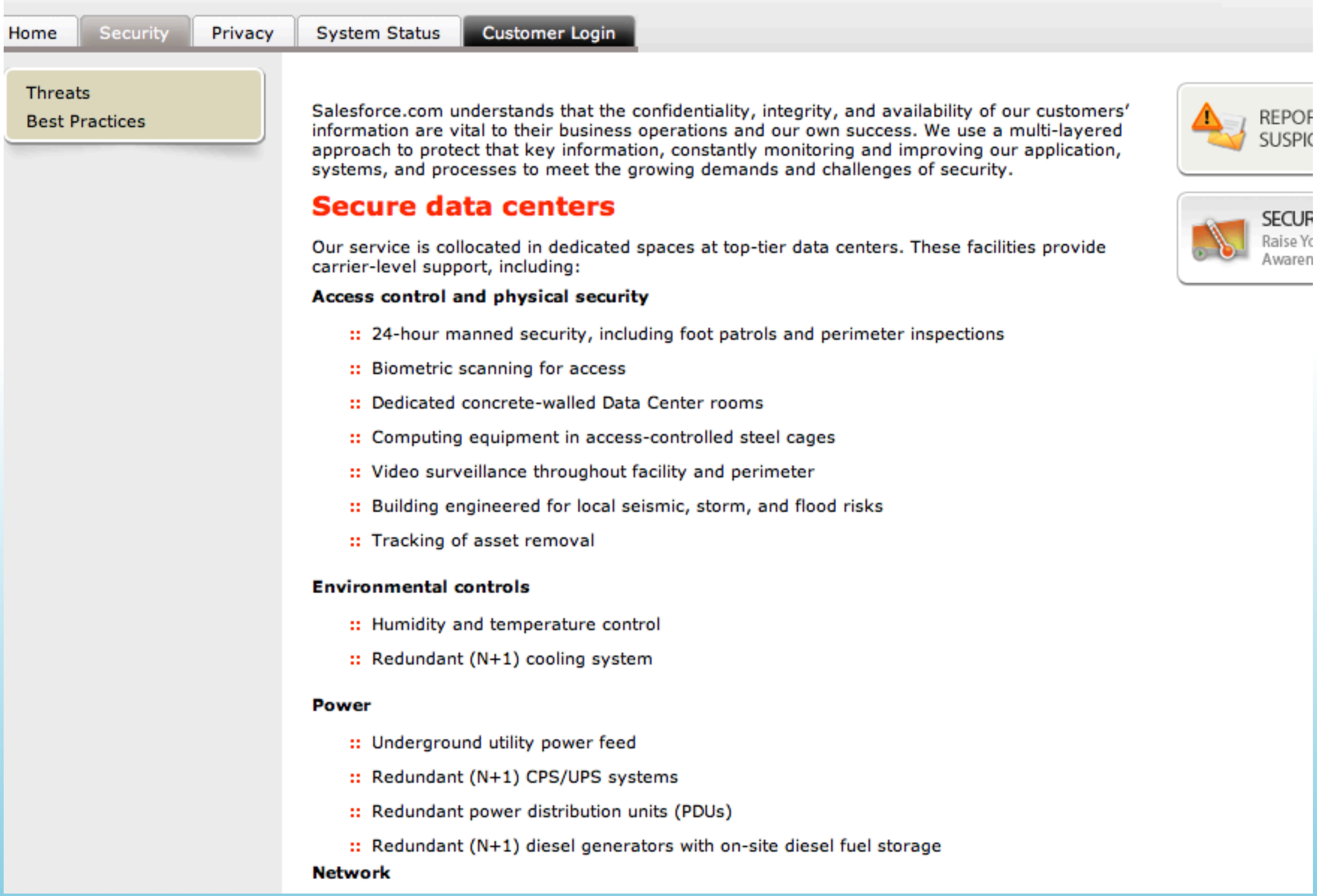
CRM Snaphot

Cisco

Centralizing Information on a Global Scale: Cisco Deploys Salesforce to 15,000 Users with Siebel Integration and PRM Capabilities

CRM Snapl

Could you Trust Force.com ?



Salesforce.com understands that the confidentiality, integrity, and availability of our customers' information are vital to their business operations and our own success. We use a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security.

Secure data centers

Our service is collocated in dedicated spaces at top-tier data centers. These facilities provide carrier-level support, including:

Access control and physical security

- 24-hour manned security, including foot patrols and perimeter inspections
- Biometric scanning for access
- Dedicated concrete-walled Data Center rooms
- Computing equipment in access-controlled steel cages
- Video surveillance throughout facility and perimeter
- Building engineered for local seismic, storm, and flood risks
- Tracking of asset removal

Environmental controls

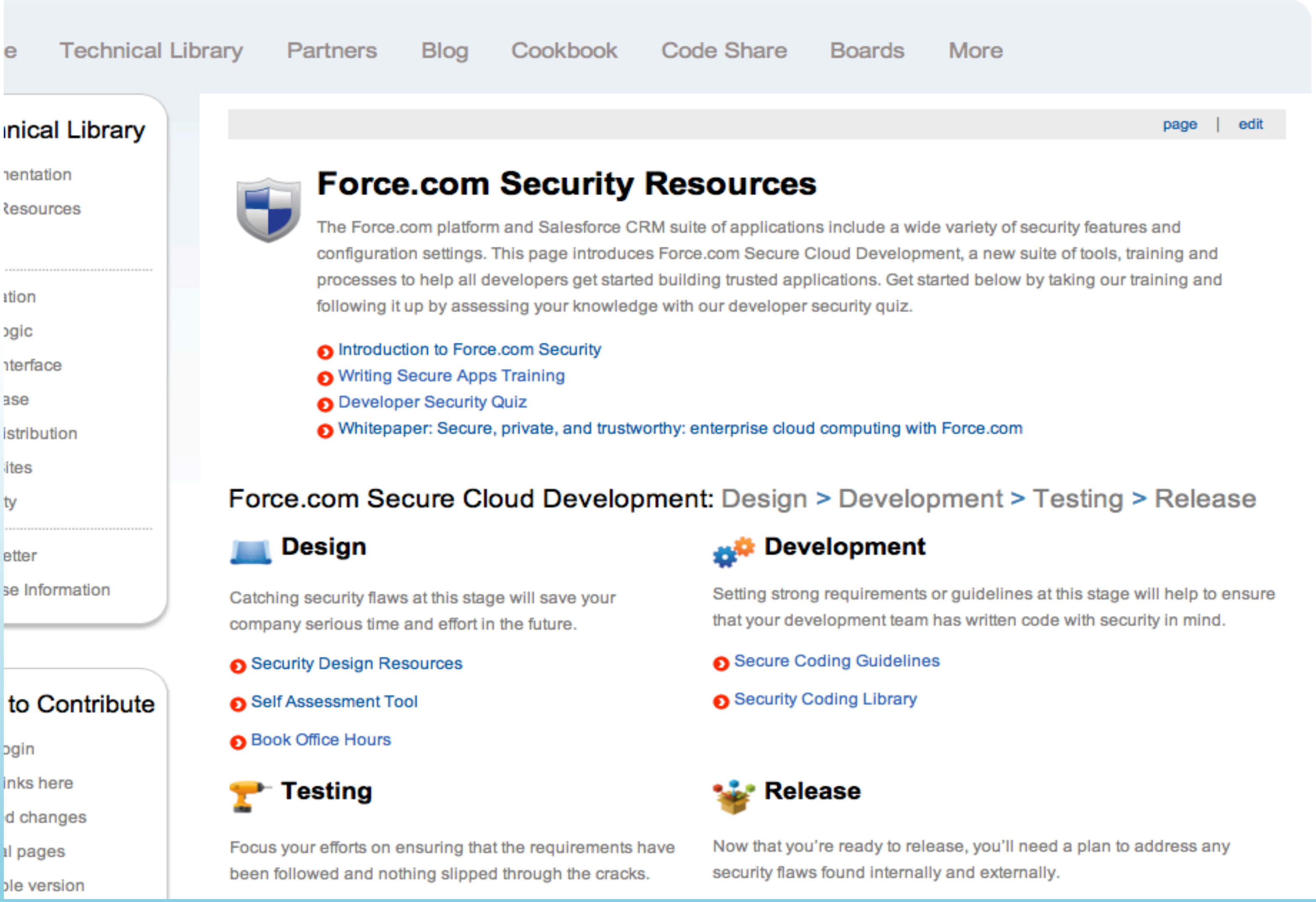
- Humidity and temperature control
- Redundant (N+1) cooling system

Power

- Underground utility power feed
- Redundant (N+1) CPS/UPS systems
- Redundant power distribution units (PDUs)
- Redundant (N+1) diesel generators with on-site diesel fuel storage

Network

Force.com Security Literature



Force.com Security Resources

The Force.com platform and Salesforce CRM suite of applications include a wide variety of security features and configuration settings. This page introduces Force.com Secure Cloud Development, a new suite of tools, training and processes to help all developers get started building trusted applications. Get started below by taking our training and following it up by assessing your knowledge with our developer security quiz.

- Introduction to Force.com Security
- Writing Secure Apps Training
- Developer Security Quiz
- Whitepaper: Secure, private, and trustworthy: enterprise cloud computing with Force.com

Force.com Secure Cloud Development: Design > Development > Testing > Release

Design

Catching security flaws at this stage will save your company serious time and effort in the future.

- Security Design Resources
- Self Assessment Tool
- Book Office Hours

Development

Setting strong requirements or guidelines at this stage will help to ensure that your development team has written code with security in mind.

- Secure Coding Guidelines
- Security Coding Library

Testing

Focus your efforts on ensuring that the requirements have been followed and nothing slipped through the cracks.

Release

Now that you're ready to release, you'll need a plan to address any security flaws found internally and externally.

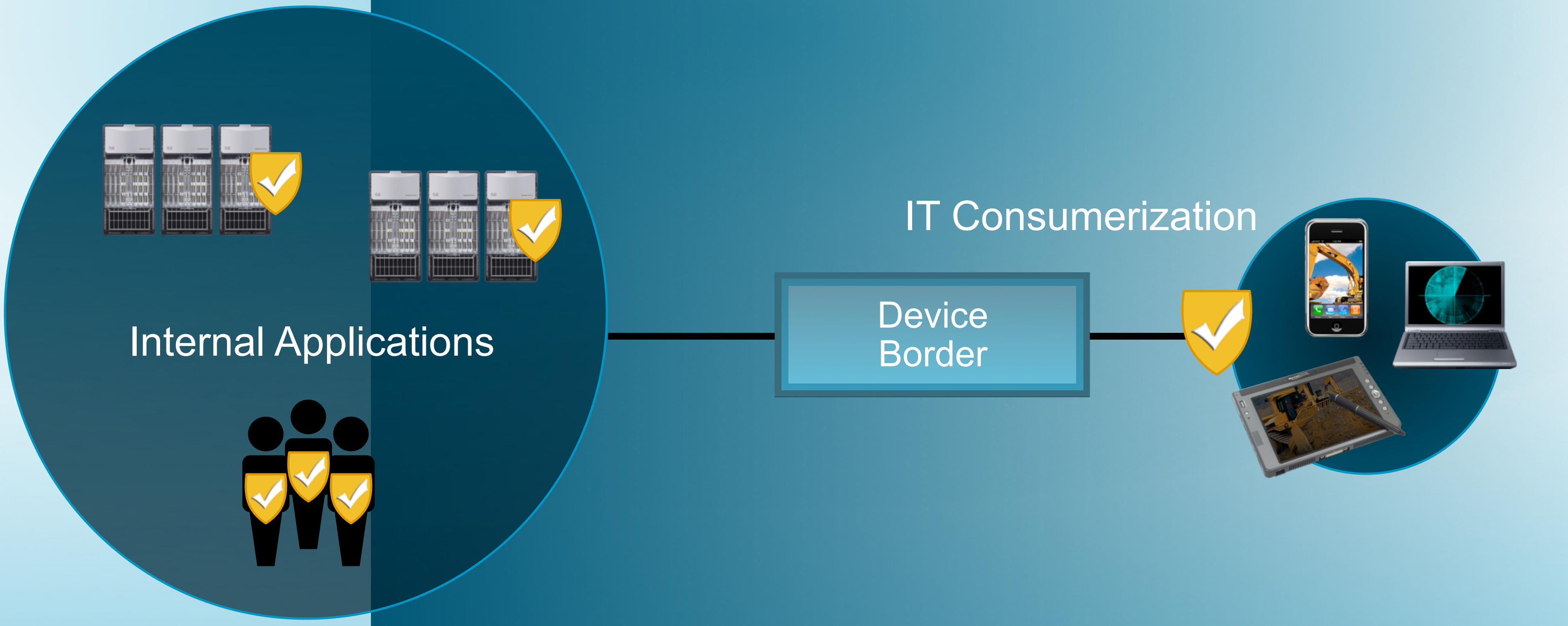
Security recommendations

- 1# educate your users
- 2# Identify your primary security contact
- 3# Secure Employee Systems
- 4# Implement IP restrictions
- 5# strengthen password policies
- 6# require secure sessions
- 7# Decrease session timeout value

Reference: http://wiki.developerforce.com/index.php/An_Overview_of_Force.com_SecuritySecurity

Webinar : https://salesforce.acrobat.com/securitywebinar

The New World : Device Borders



Internal Applications

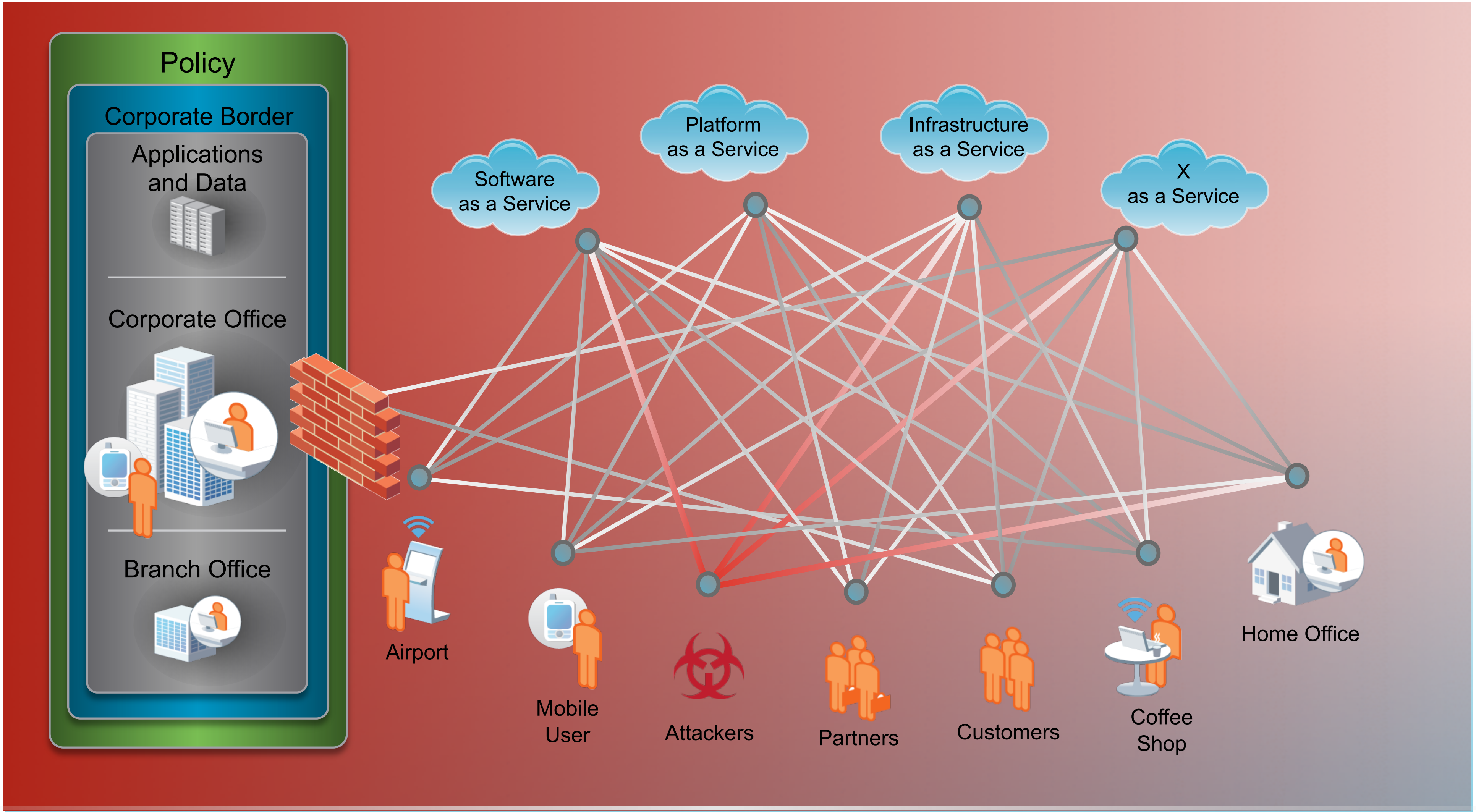
Device Border

IT Consumerization

Are they still corporate assets ?

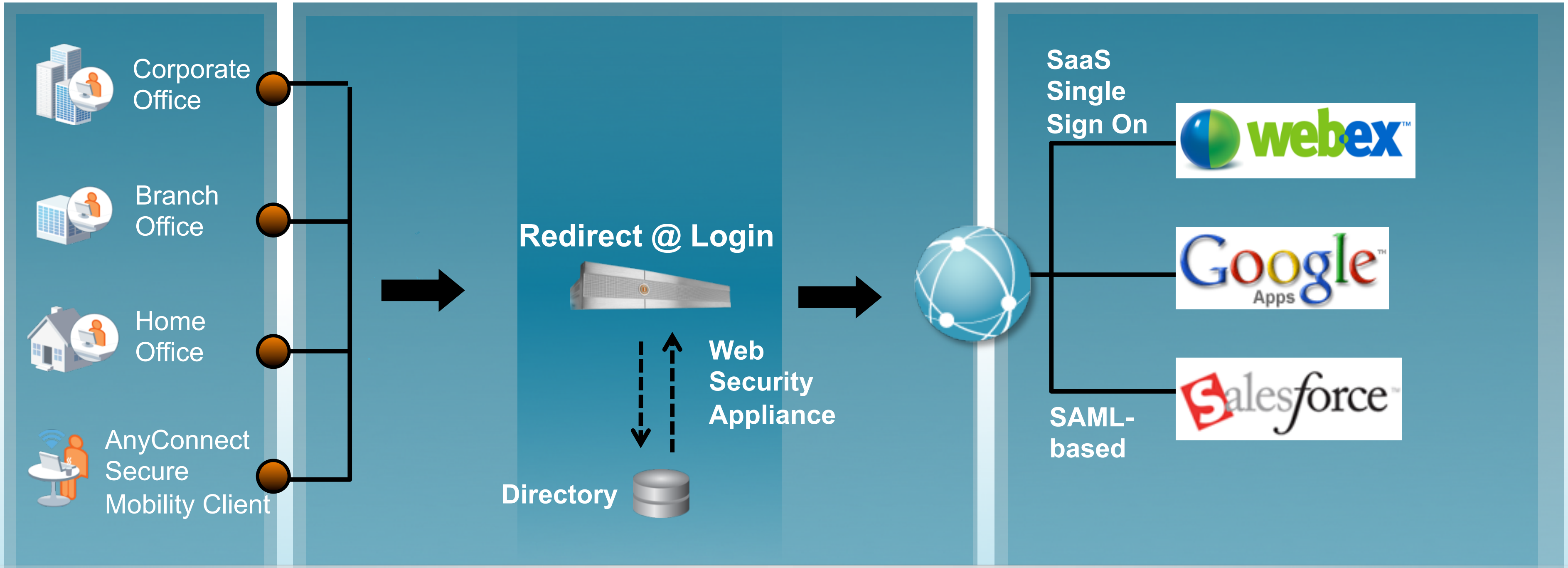
Desktop Virtualization is part of the Security Journey

Concern: Security in a Cloud World



SaaS Access Control

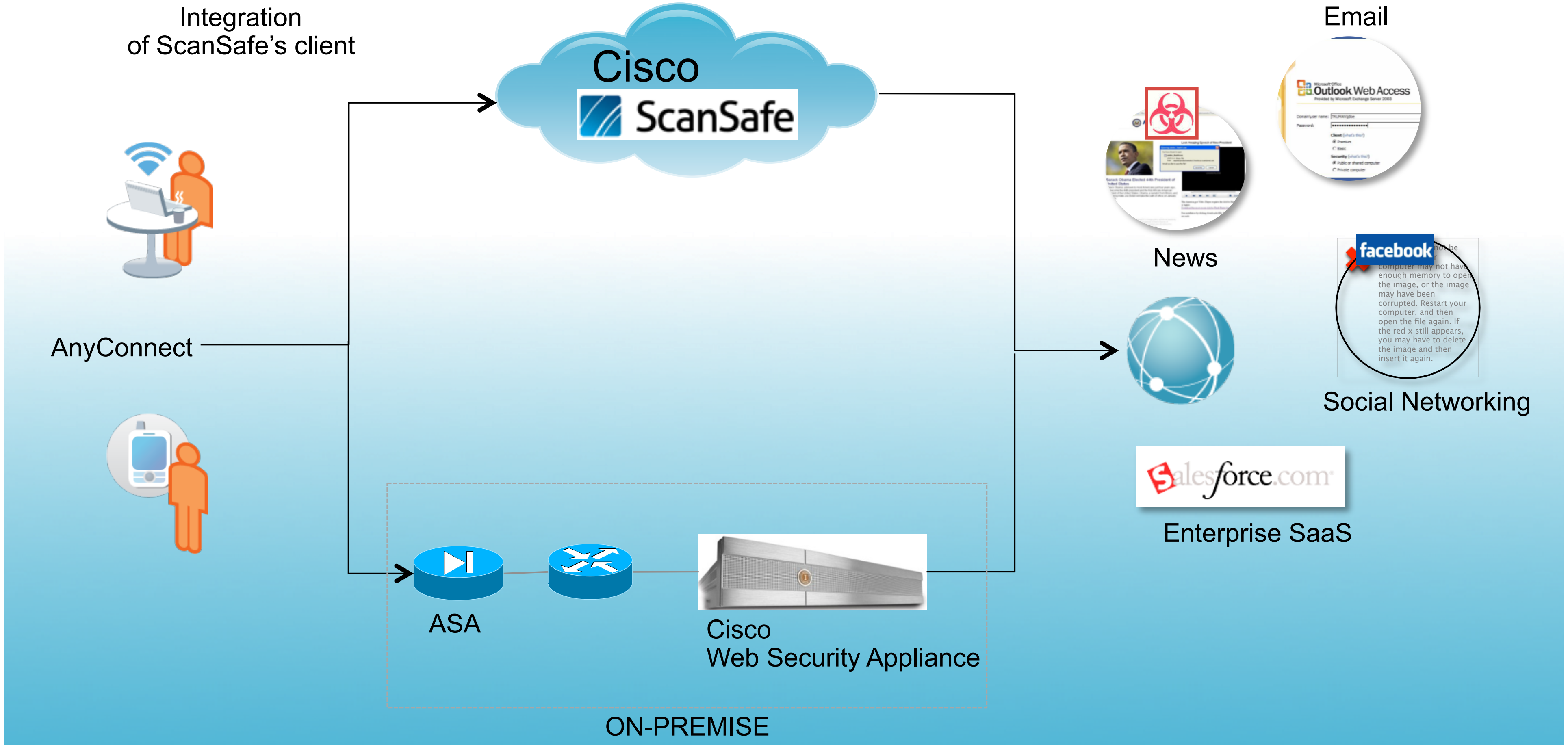
Regaining Visibility and Control Through Identity



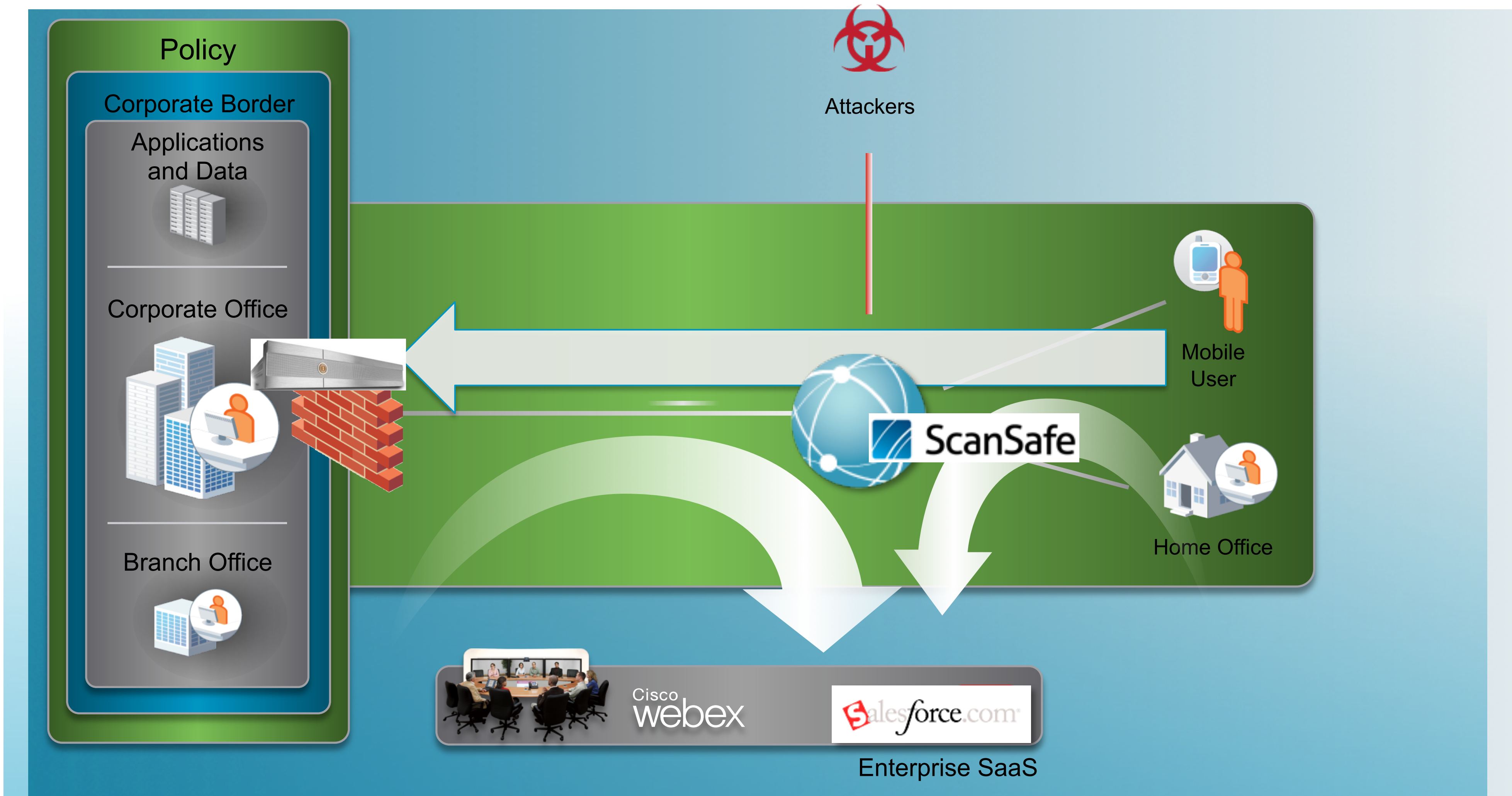
Visibility | Centralized Enforcement | Single Source Revocation

AnyConnect Secure Mobility Vision

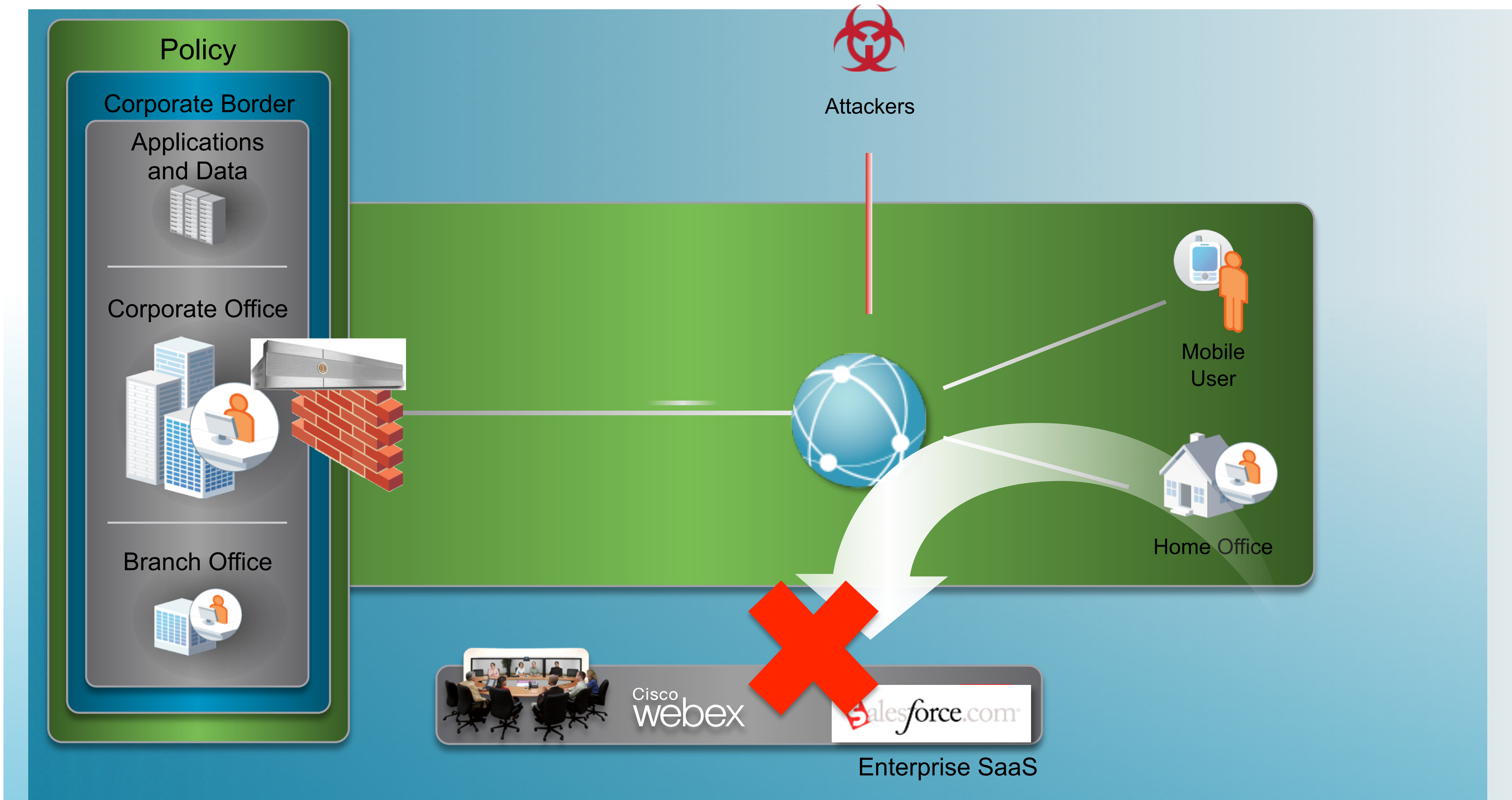
On-Premise Gateway or Cloud Policy Enforcement



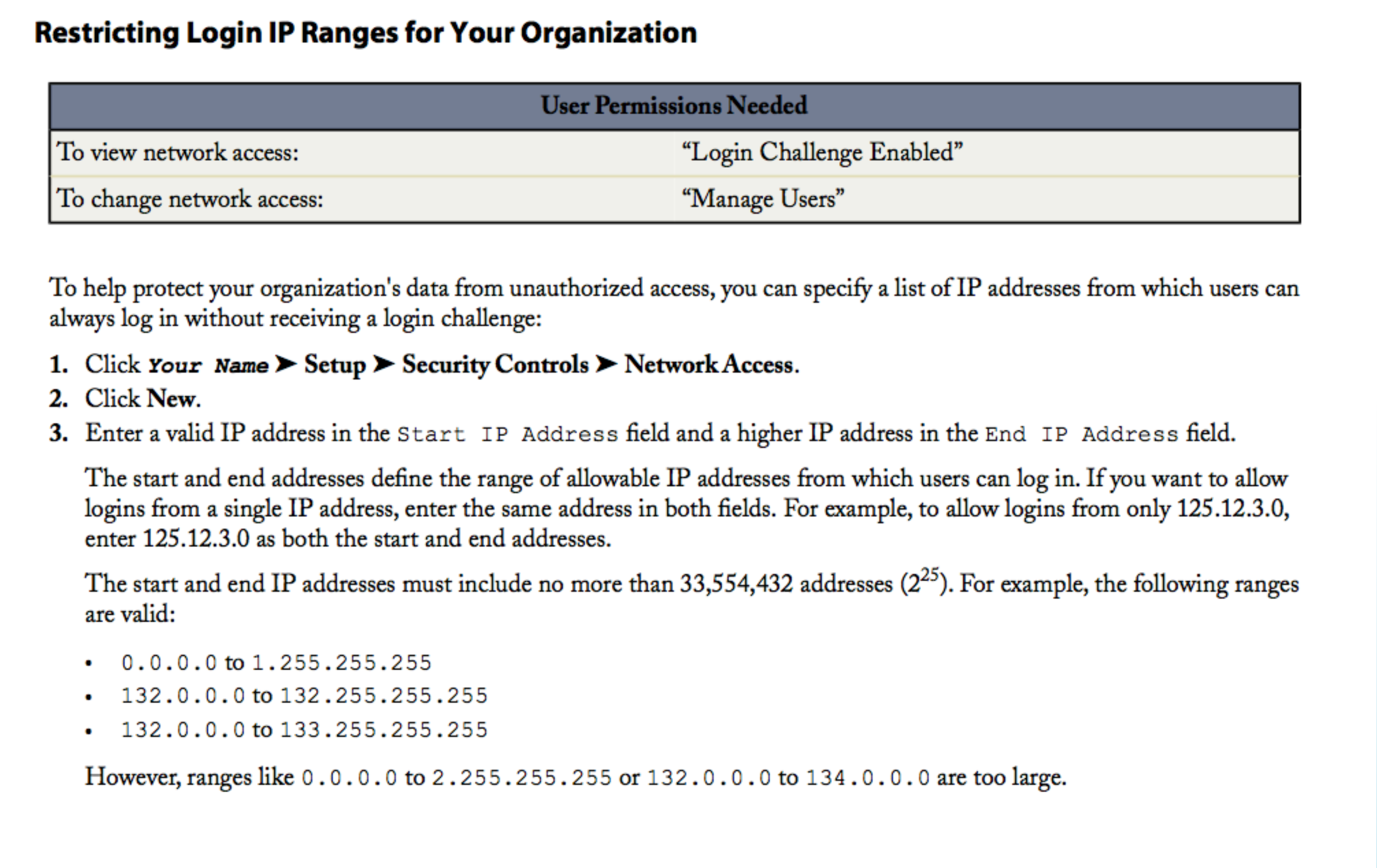
Mobile Users and Secured Cloud Access



Non Secured Users Should Be Filtered Out



Public Services Access Can Be Filtered Out



Restricting Login IP Ranges for Your Organization

User Permissions Needed	
To view network access:	“Login Challenge Enabled”
To change network access:	“Manage Users”

To help protect your organization's data from unauthorized access, you can specify a list of IP addresses from which users can always log in without receiving a login challenge:

1. Click *Your Name* ➤ **Setup** ➤ **Security Controls** ➤ **Network Access**.
2. Click **New**.
3. Enter a valid IP address in the `Start IP Address` field and a higher IP address in the `End IP Address` field.

   The start and end addresses define the range of allowable IP addresses from which users can log in. If you want to allow logins from a single IP address, enter the same address in both fields. For example, to allow logins from only 125.12.3.0, enter 125.12.3.0 as both the start and end addresses.

   The start and end IP addresses must include no more than 33,554,432 addresses (2^{25}). For example, the following ranges are valid:

   - `0.0.0.0` to `1.255.255.255`
   - `132.0.0.0` to `132.255.255.255`
   - `132.0.0.0` to `133.255.255.255`

   However, ranges like `0.0.0.0` to `2.255.255.255` or `132.0.0.0` to `134.0.0.0` are too large.

https://na1.salesforce.com/help/doc/en/salesforce_security_impl_guide.pdf

Considerations about the Private Cloud Security

First days of a Private Cloud
Anchored on Trust & Control

Trusted

Controlled

Reliable

Secure

CLOSED

Cloud Computing

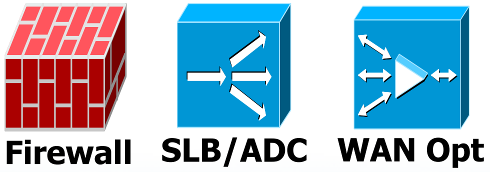
Targeting Agility and Efficiency

Highly Virtualized Data Centers and Cloud Computing

Trusted	Flexible
Controlled	Dynamic
Reliable	On-demand
Secure	Efficient

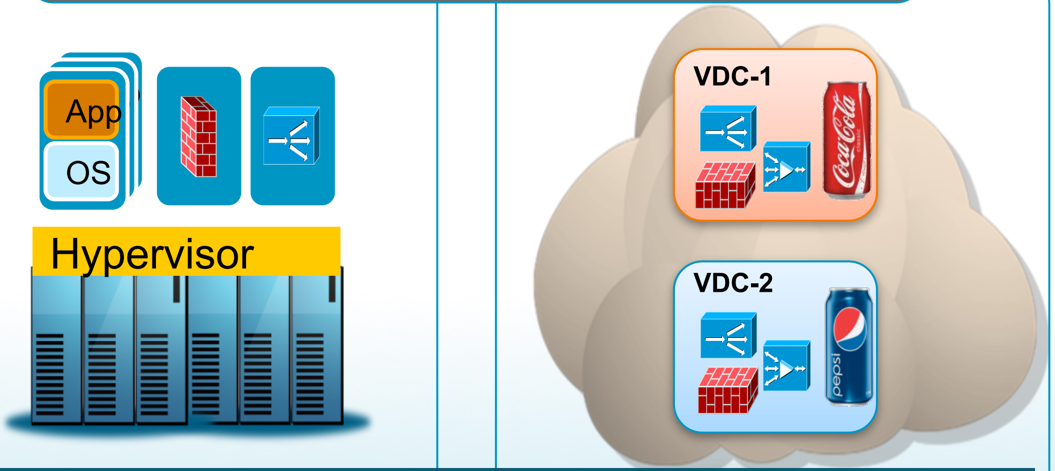
Virtualization & Cloud Driving New Requirements in Data Center

Dedicated Network Services



- Application-specific services
- Form factors:
  - Appliance
  - Switch module

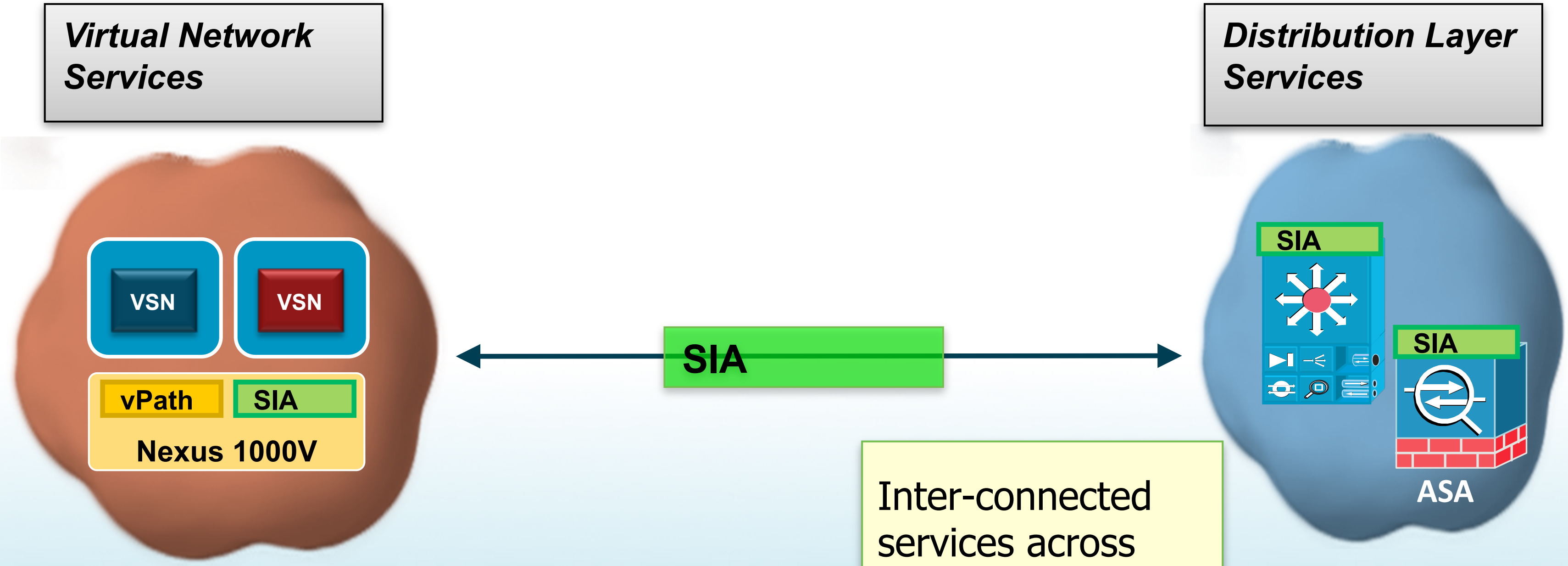
Virtual Network Services



Virtual Service Nodes (VSNs)

- Virtual appliance form factor
- Dynamic Instantiation/Provisioning
- Service transparent to VM mobility
- Support scale-out
- Large scale multi-tenant operation

Fully Inter-connected Network Services Vision



Inter-connected services across physical and virtual environments

SIA: Service Insertion Architecture

Data Center Security Challenges

- Virtualization
- Applications
- Data Loss
- Compliance
- Availability

Cloud-Specific Issues Emerging

- Organizational & Operational Misalignment
- Monoculture of Operating Systems, Virtualized Components & Platforms
- Privacy Of Data/Metadata, Exfiltration and Leakage
- Inability to Deploy Compensating or Detective Controls
- Segmentation & Isolation In Multi-tenant environments...

Cloud Happiness

The Cloud <u>can</u> provide the following security benefits:

- Centralized Data (sort of...)
- Segmented data/applications
- Better Logging/Accountability
- Standardized images for asset deployment
- Better Resilience to attack & streamlined incident response
- More streamlined Audit and Compliance
- Better visibility to process
- Faster deployment of applications, services, etc.

Key Takeaways

Key Takeaways (From A Customer's Perspective)

- Have a risk assessment methodology, classify assets and data.
- Interrogate vendors and providers; use the same diligence that you would for outsourced services today; focus on resilience/ recovery, SLA's, confidentiality, privacy and segmentation.
- The challenge is to match business/security requirements against the various *aaS model(s)
- Each of the *aaS models provides a delicate balance of openness, flexibility, control, security and extensibility
- Regardless of the model, **you** are still responsible for some element of security

References

- Cloud literature on Cisco.com
  http://www.cisco.com/en/US/netsol/ns976/index.html
- Cloud Computing Google Groups:
  - **Cloud Computing**
    http://groups.google.com/group/cloud-computing
  - **Cloud Computing Interoperability Forum**
    http://groups.google.com/group/cloudforum
  - **Cloud Storage**
    http://groups.google.com/group/cloudstorage
- Attend a local CloudCamp
- Join the Cloud Security Alliance & CloudAudit...