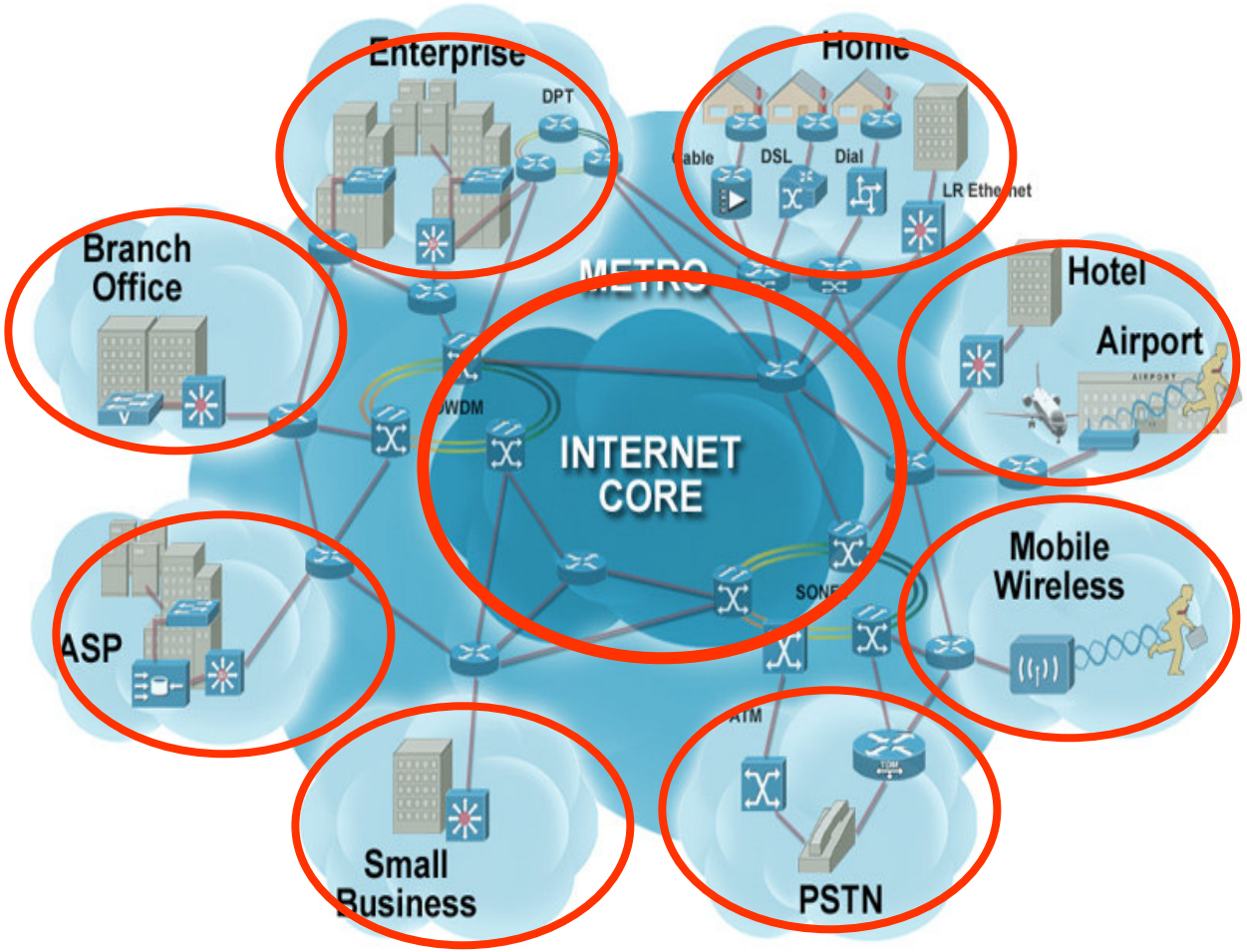
L'initiative « Self Defending Networks » de Cisco Systems

Philippe Cunningham – phcunnin@cisco.com

Business Developpement Manager Sécurité

Séminaire Cisco/Tivoli - 24 Mai 2004

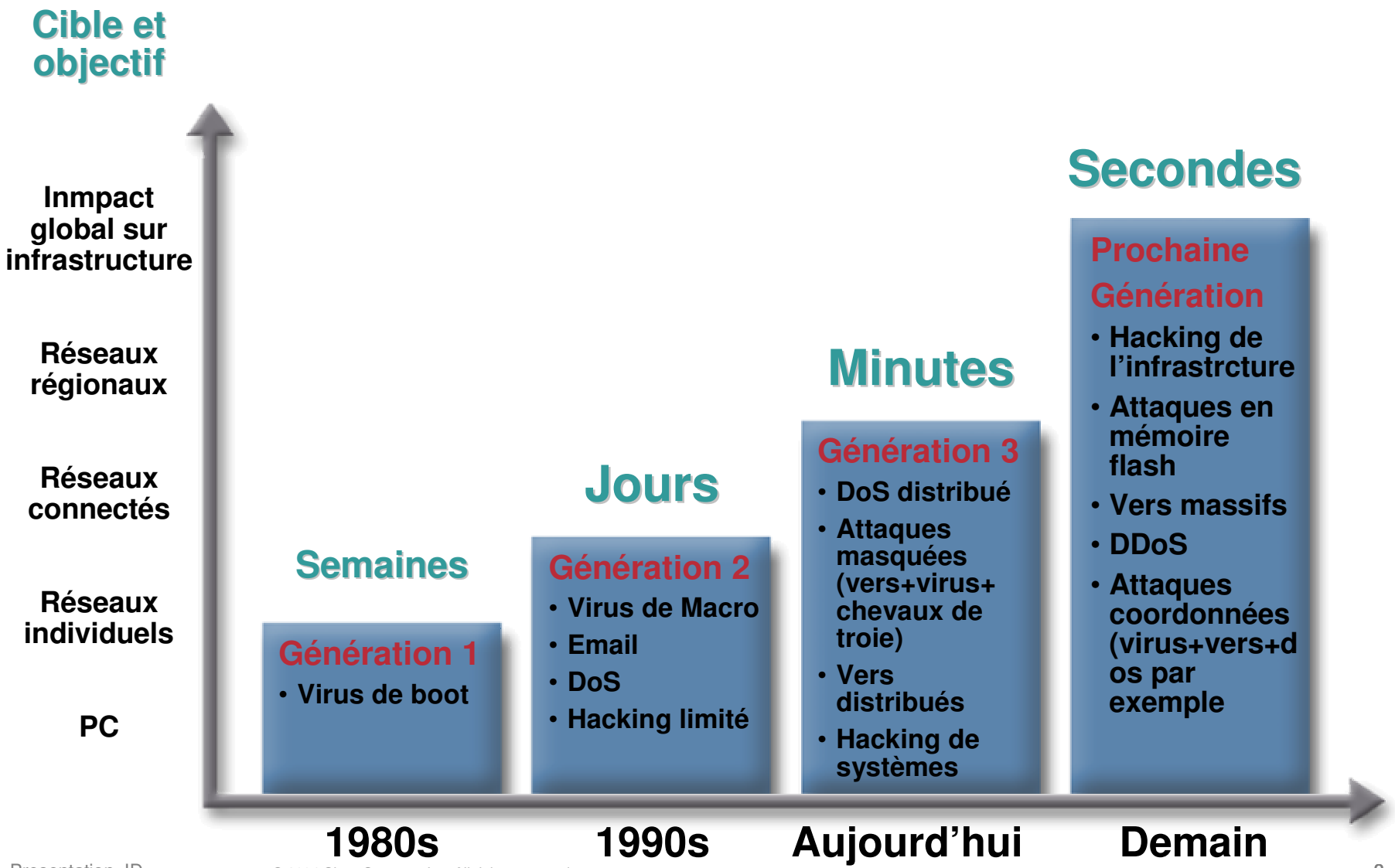
Réseaux des années 2000



Mobilité :

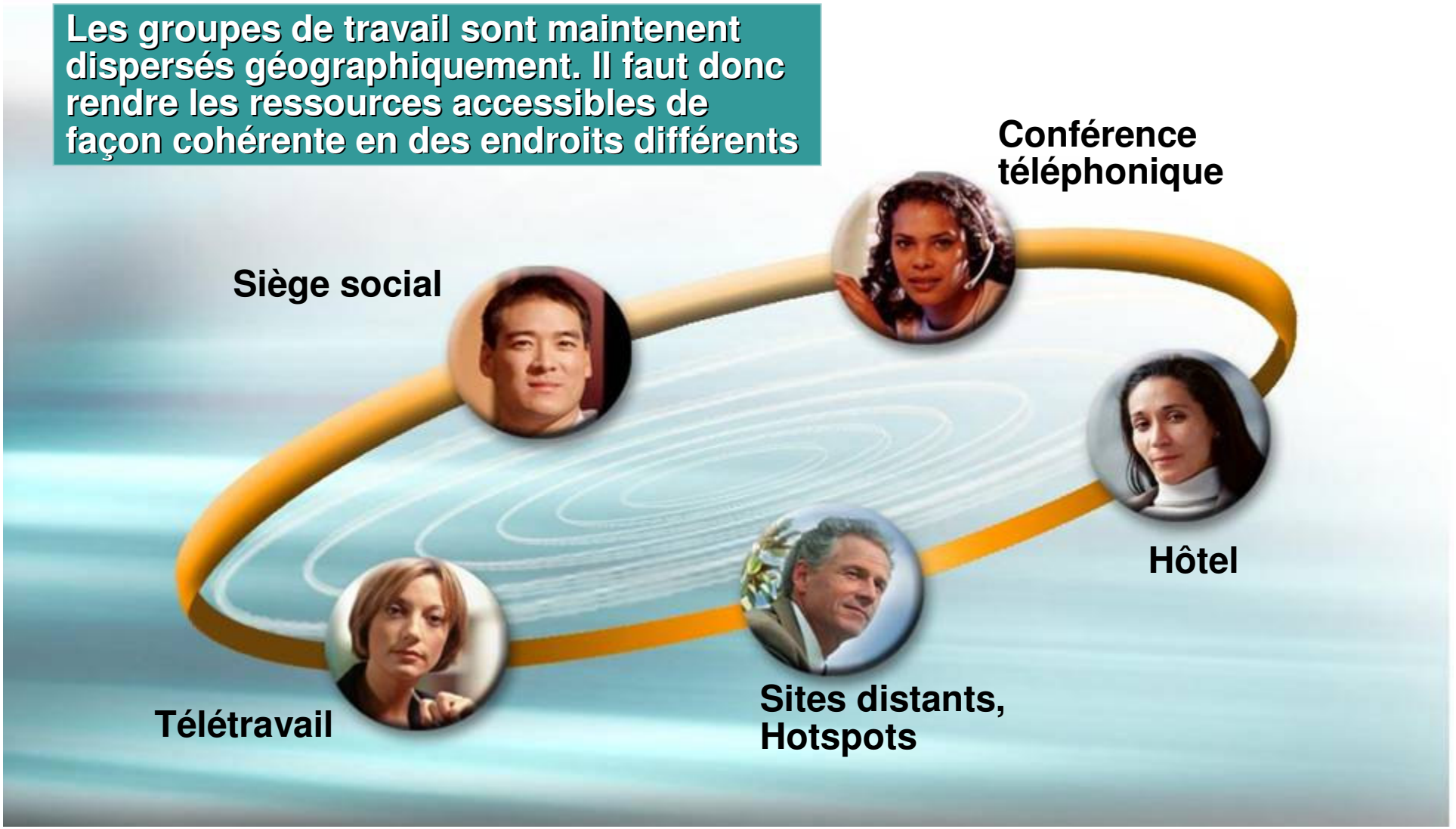
- Nouvelles méthodes d'accès au réseau :
  - Accès VPN
  - Accès Wireless
- Besoins d'ouverture des datacenters
- Généralisation de la messagerie électronique
- Généralisation des technologies Web
- Généralisation d'OS et d'applications cibles privilégiées d'attaques

Les attaques évoluent



Nouvelles méthodes de travail

Les groupes de travail sont maintenant dispersés géographiquement. Il faut donc rendre les ressources accessibles de façon cohérente en des endroits différents



Des approches en silos

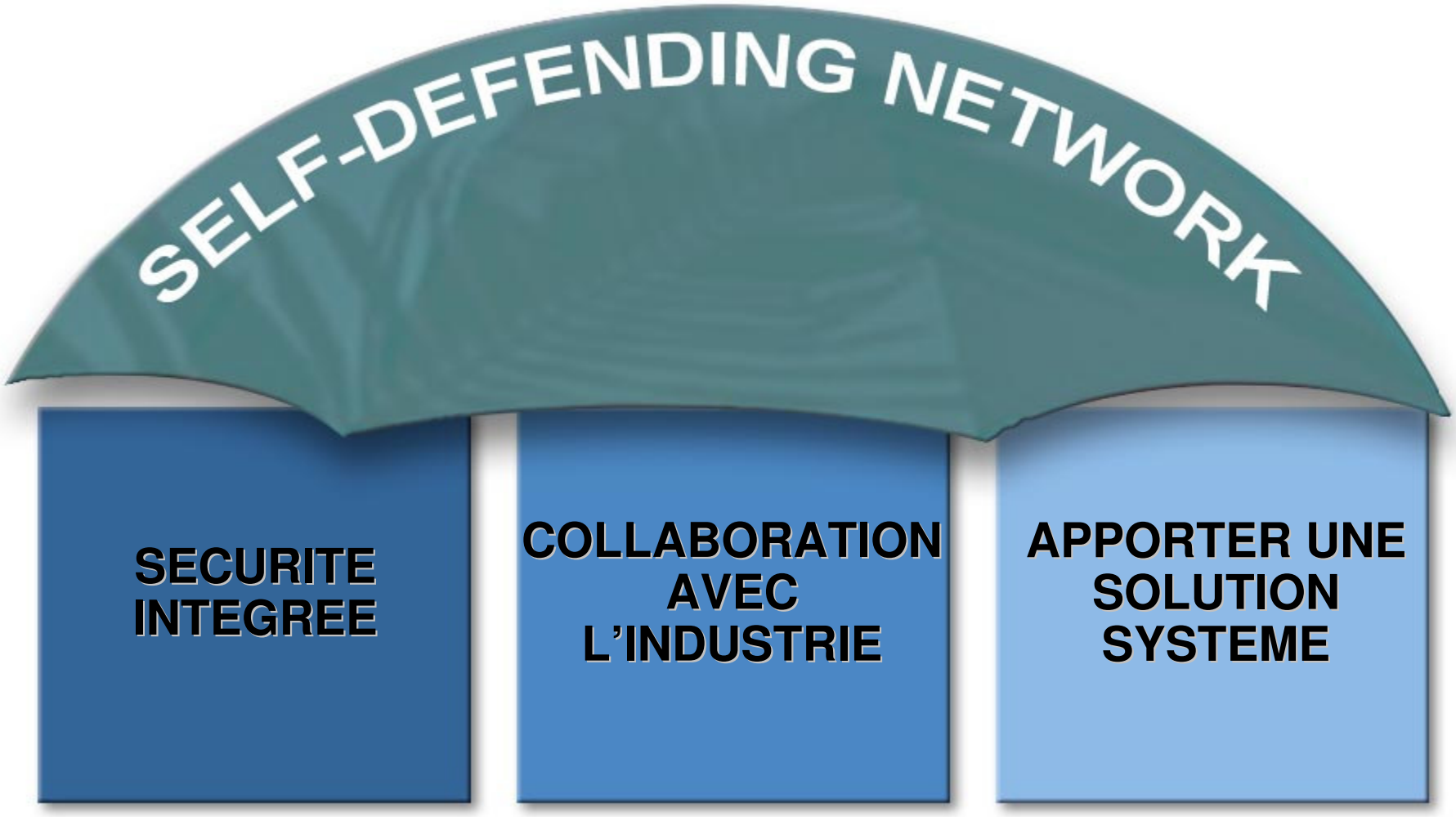
Infrastructure	Extrémités	Contrôle	Applications
TRANSPORT Sécuriser, fiabiliser les infrastructures de communication	**INTERFACE UTILISATEUR** Téléphones IP, terminaux vidéo, PC, PDA et autres terminaux	**GESTION DES SYSTEMES** Infrastructure et protocoles, management et exploitation	**COMPOSANTS A VALEUR AJOUTEE** Messagerie, CRM et autres applications Métier

IP Communications System

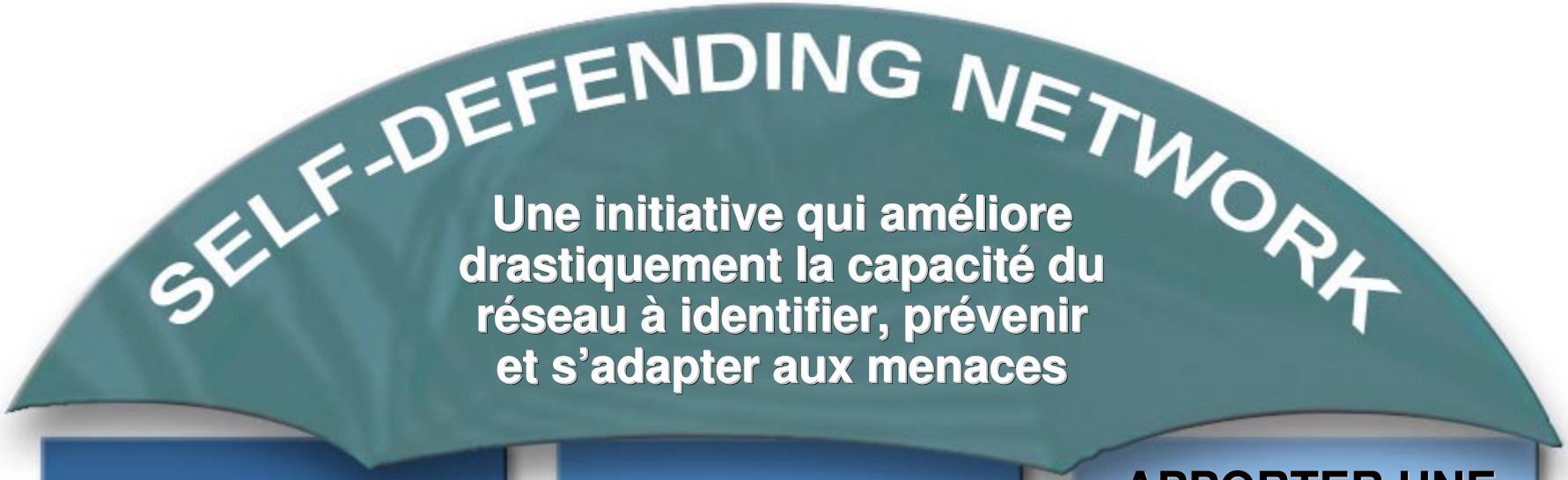
L'approche stratégique de la Sécurité

Les phases de développememt de Cisco

La vision de la Sécurité par Cisco



La vision de la Sécurité par Cisco



SECURITE INTEGREE

- Connectivité sécurisée
- Défense contre les menaces
- Gestion des identités

COLLABORATION AVEC L'INDUSTRIE

- Programme NAC (Network Admission Control)

APPORTER UNE SOLUTION SYSTEME

- Identification, prévention et réponses dynamique aux attaques
- End-to-End

Une approche globale de la sécurité réseau

Protéger des menaces

Protéger la périphérie
- **FW+IDS intégrés**
  - Prévenir et détecter les attaques extérieures

Protéger l'intérieur
- **Sécurité intégrée aux Catalysts**
  - Protéger contre les attaques internes

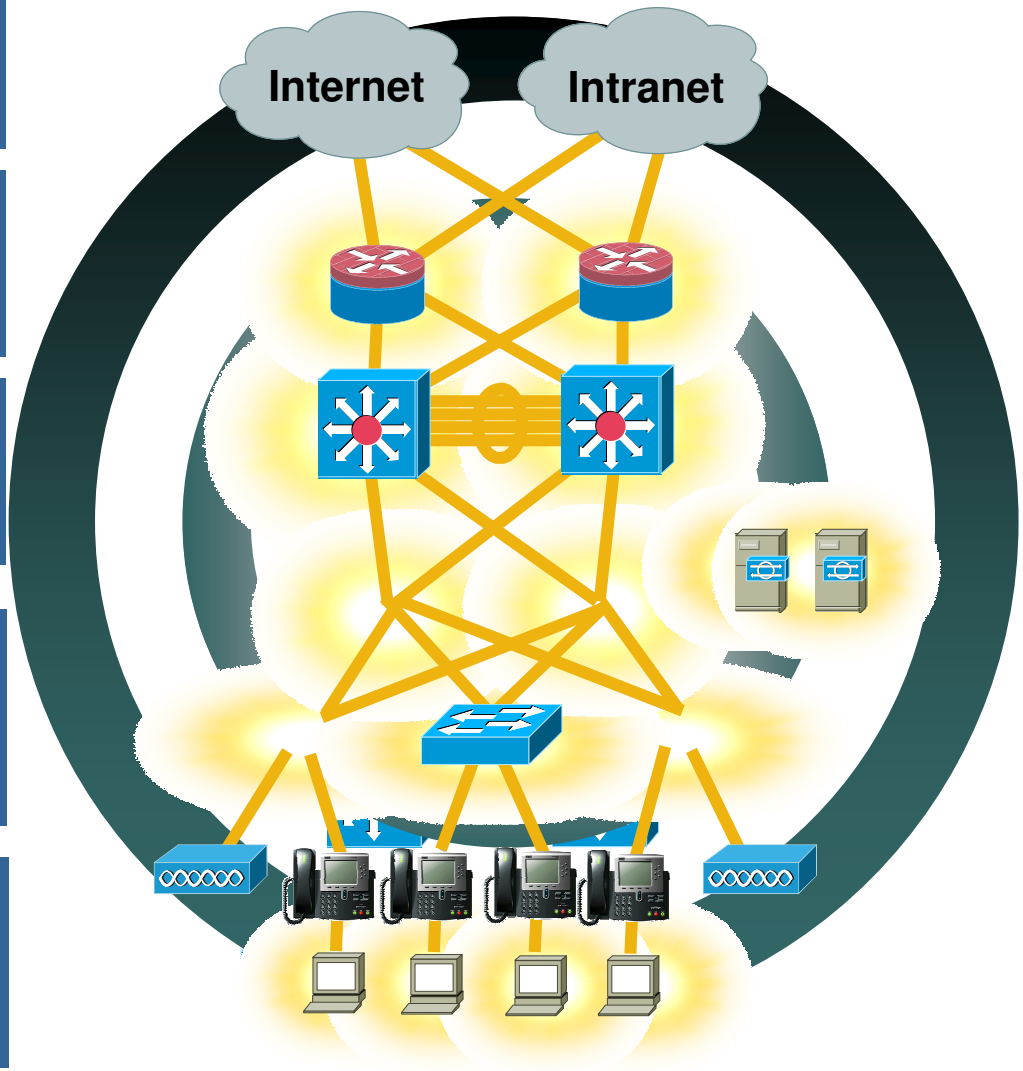
Protéger les systèmes
- **Cisco Security Agent (CSA)**
  - Clients et serveurs

Identité et confiance

Contrôler les utilisateurs et les machines
- **Identity-Based Networking/NAC**
  - Contrôler qui/quoi accède au réseau

Sécurité des comms.

Sécuriser le transport
- **VPN (IPSEC, MPLS, etc…)**
  - Protéger la confidentialité des données et de la voix



La collaboration de l'Industrie est clé !

Cisco Systems

Programme Cisco Network Admission Control

Network Associates

symantec.

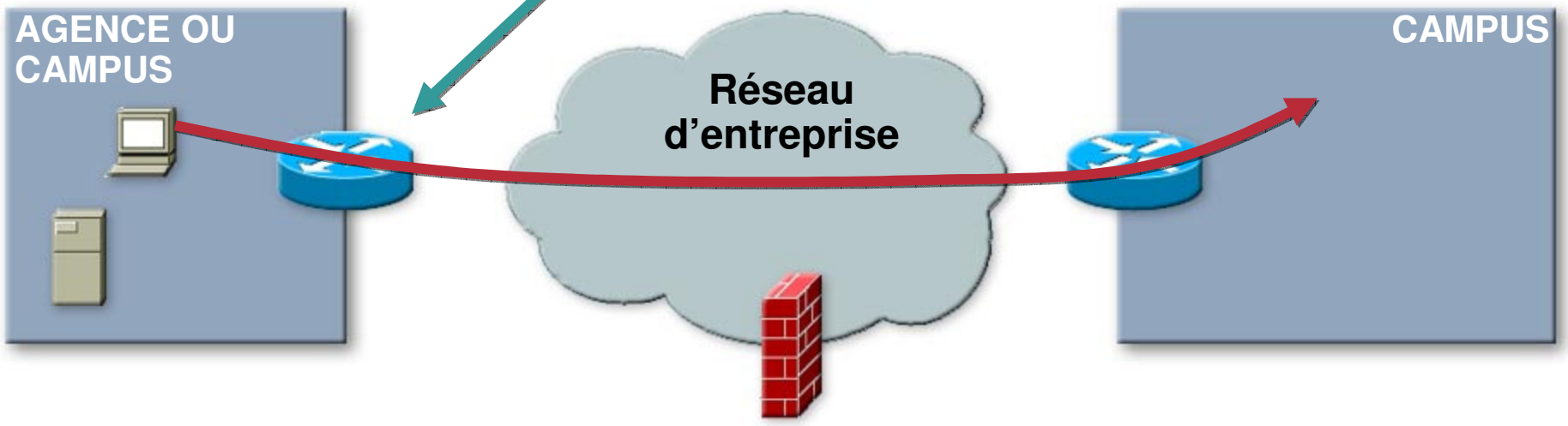
TREND MICRO

Pourquoi NAC ?

1. Un poste client non conforme se connecte

2. Connexion autorisée

3. Diffusion de l'infection, postes d'extrémités exposés



Cisco NAC : Principe de fonctionnement

Logiciel de protection des postes d'extrémité + Equipement d'accès au réseau + Serveur de règles Cisco + Solution tierces (Anti-Virus, serveur de règles)

Tivoli software

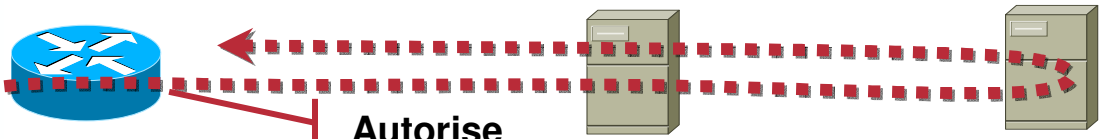
Cisco Security Agent

Cisco Systems

Anti-Virus Client

Cisco Trust Agent

Validation de la conformité de bout en bout



Autorise
Refuse
Isole
Solution alternative

Network Associates

symantec.

TREND MICRO

Contrôle et exécution des politiques de sécurité

Création des politiques de sécurité

Evaluation de la conformité (Anti-Virus, applications tierces)

Tivoli software

Tivoli software

Quelles implications pour vous ?

Cisco.com

Aujourd'hui : Protection des postes d'extrémité

- Minimiser le gestion de patches
- Adresser la problématique de la protection à "T0"

CSA

NAC

Court terme : Network Admission Control

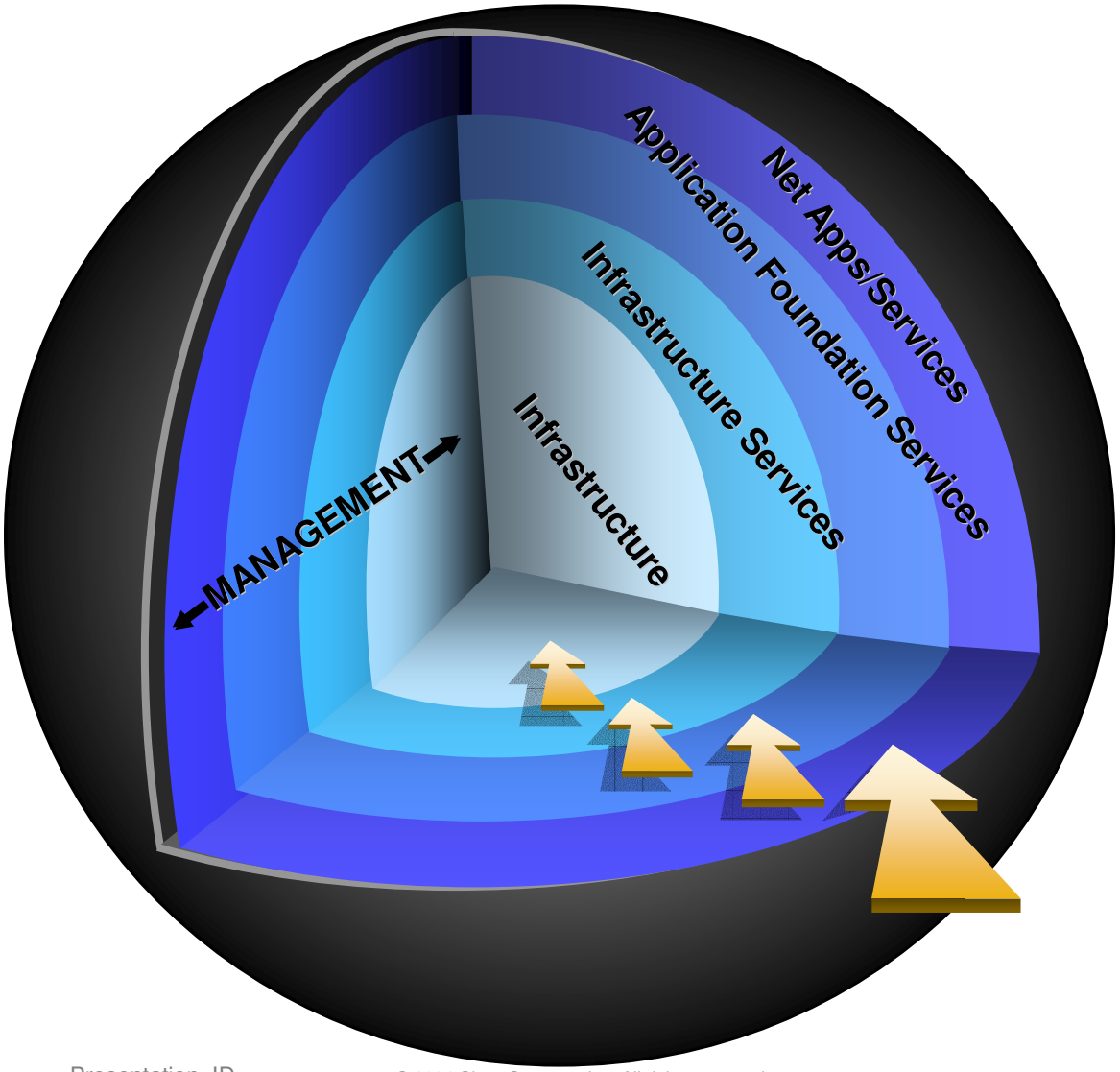
- Contrôle total de l'exécution des règles de sécurité définies
- Droits d'accès basés sur l'elligibilité de l'équipement
- Pérennise l'investissement fait sur les anti-virus et la protection des systèmes

Futur : Isolation pro-active des infections

- Détecter, Isoler, Traiter et Réparer les infections basés sur les informations des autres équipements
- Gérer l'ensemble des service réseau sur le même mode

IBNS

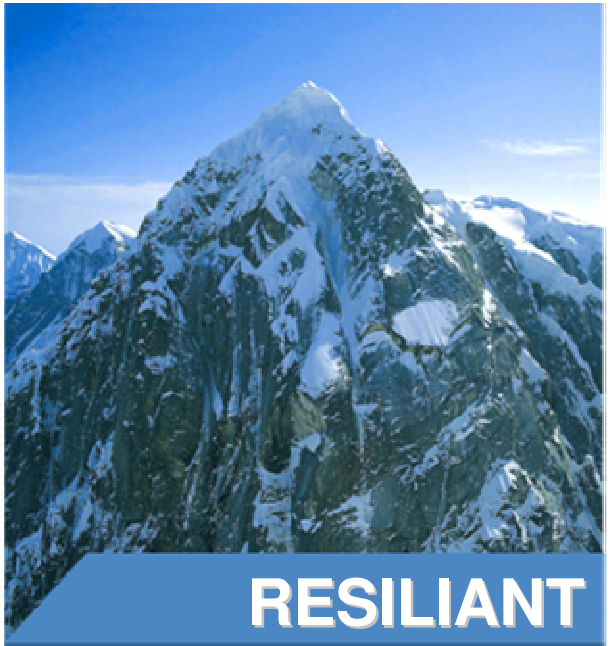
Vous permettre de vous concentrer sur votre métier



- Le réseau devient le relais actifs des règles que vous fixez
- Les règles et politiques que vous définissez ne sont plus limitées par des contraintes techniques ou d'architecture
- Vous vous concentrez sur votre métier et vos process, notre approche système permet au réseau de s'adapter

Les points clés d'un réseau "intelligent"

Cisco.com

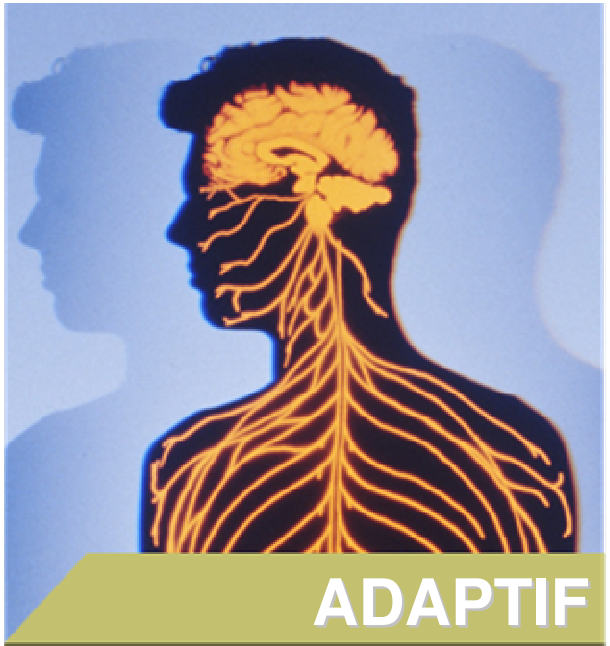


RESILIANT

- Haute disponibilité
- Sécurité multiniveaux
- Services de virtualisation
- Evolutif

INTEGRE

- Sécurité, Wireless, LAN/WAN, etc.
- Orienté Applications
- Manageable
- Modulaire



ADAPTIF

- Auto-Provisioning
- Auto-Optimisation
- Auto-défence

Tivoli software | IBM Software Group

IBM-Cisco Security Alliance Briefing

May, 2004

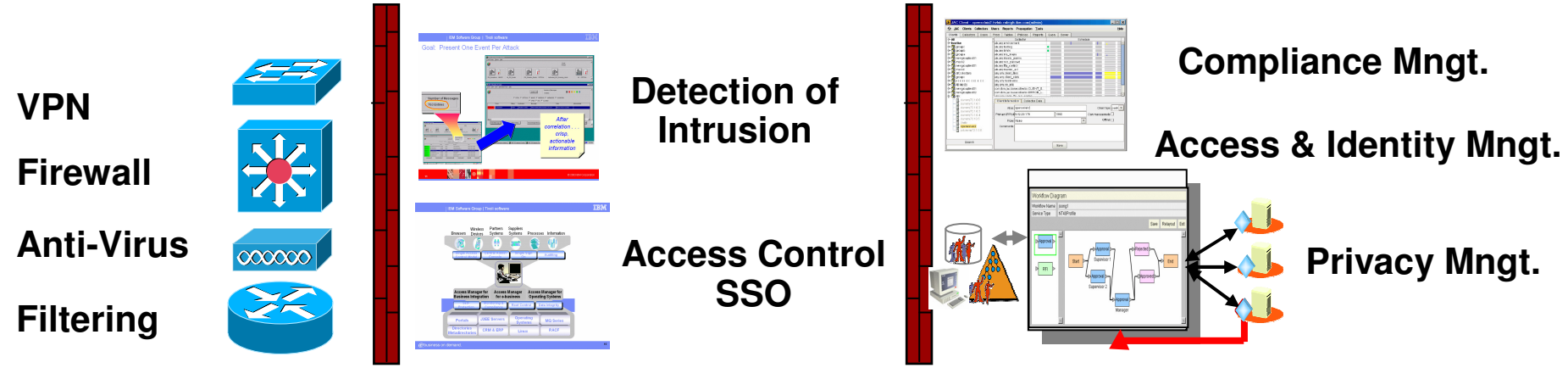
Jean-Charles Cointot
EMEA Strategic Alliances Manager, Tivoli Security

e-business on demand.

Past Security Approach

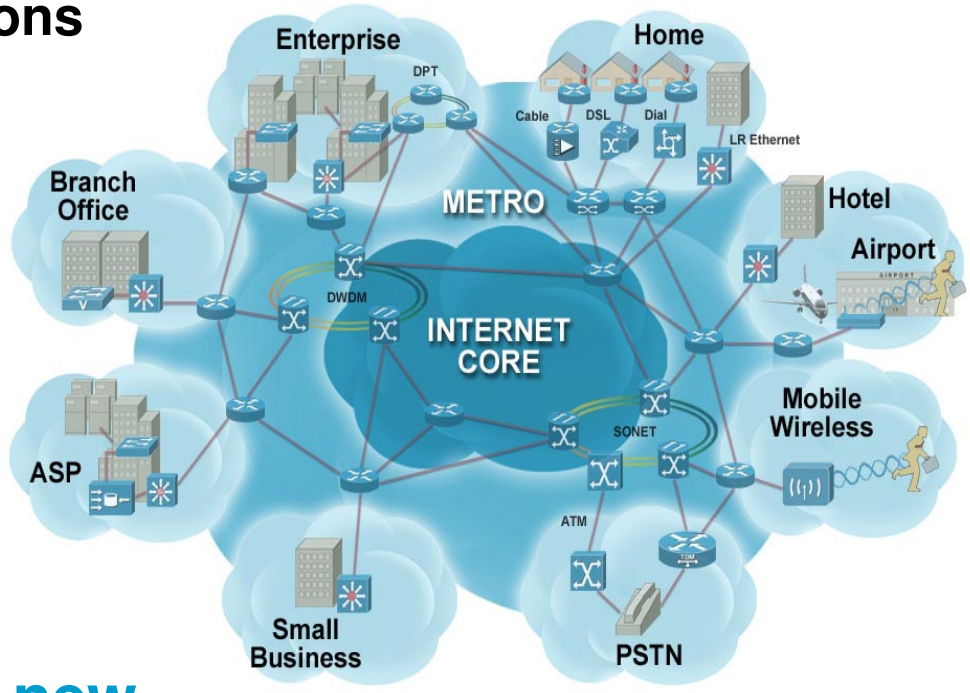
Security used to be treated in silos
- 1st step-urgency : perimeter Defense
- 2nd step- : Control accesses
- 3rd level : Manage security

No consistency in security policies
- Brieches in security = NO SECURITY
- Low productivity (redundant tasks, support)
- Overcharge



The Evolved Network & Security

- **Network perimeter indefinable**
  - **Distributed Internet applications**
  - **Ubiquitous access**
  - **Expanded constituencies**
- **Every network ingress point is a conduit to the network**
  - **Viruses, Worms**
  - **Hackers**
- **New technologies introduce new risks**
  - **Content and interactive apps**
  - **VoIP, Wi-Fi, storage**



Relationship Premise

Cisco Systems
Empowering the Internet Generation℠

A market leader in Network Security Products

Security Leadership investments in:

- **VPNs**
- **Firewalls**
- **Intrusion Detection**
- **End point Security**

+

IBM

A market leader in Security/Identity Management & Services

Security Leadership investments in:

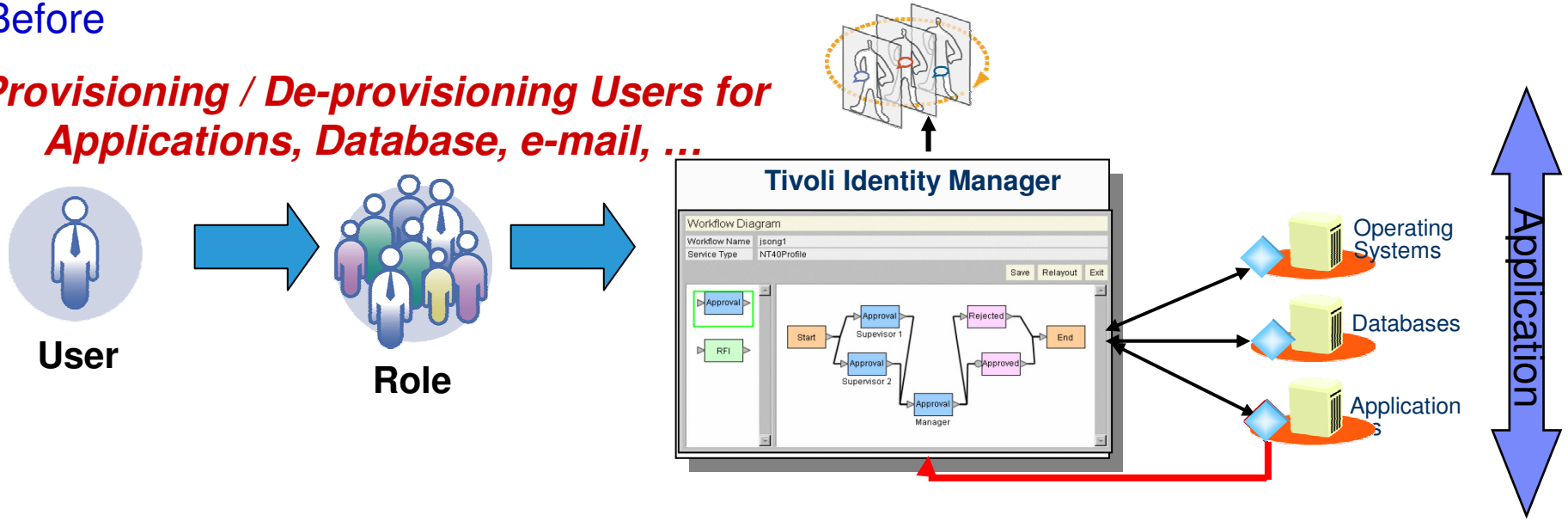
- **Identity & Policy Management**
- **Security Services**
- **Laptop & Desktop subsystems**
- **Embedded Server Security**

Customers expect comprehensive security from complementary, trusted leaders

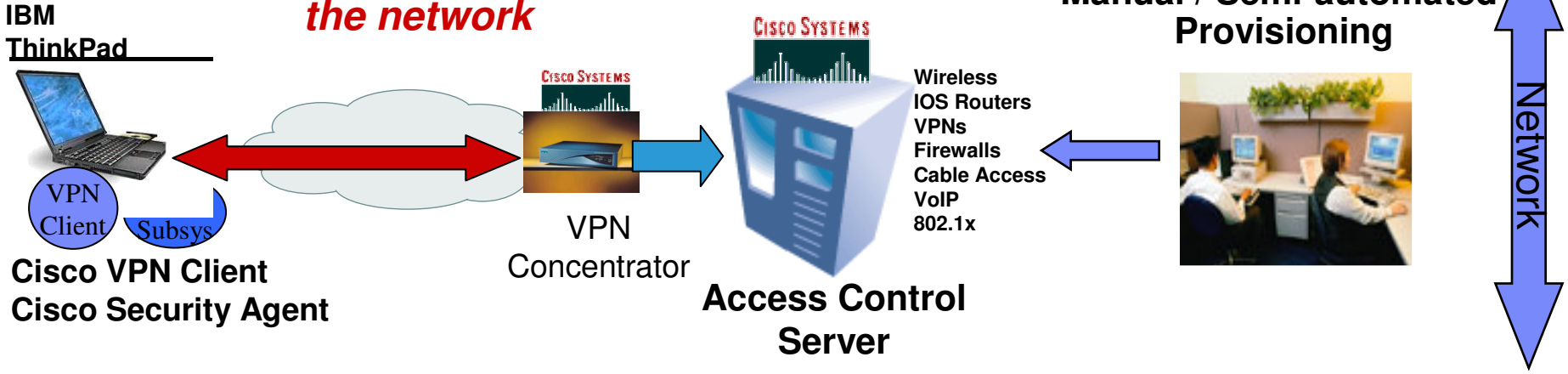
Tivoli Identity Manager + Cisco

Before

Provisioning / De-provisioning Users for Applications, Database, e-mail, …



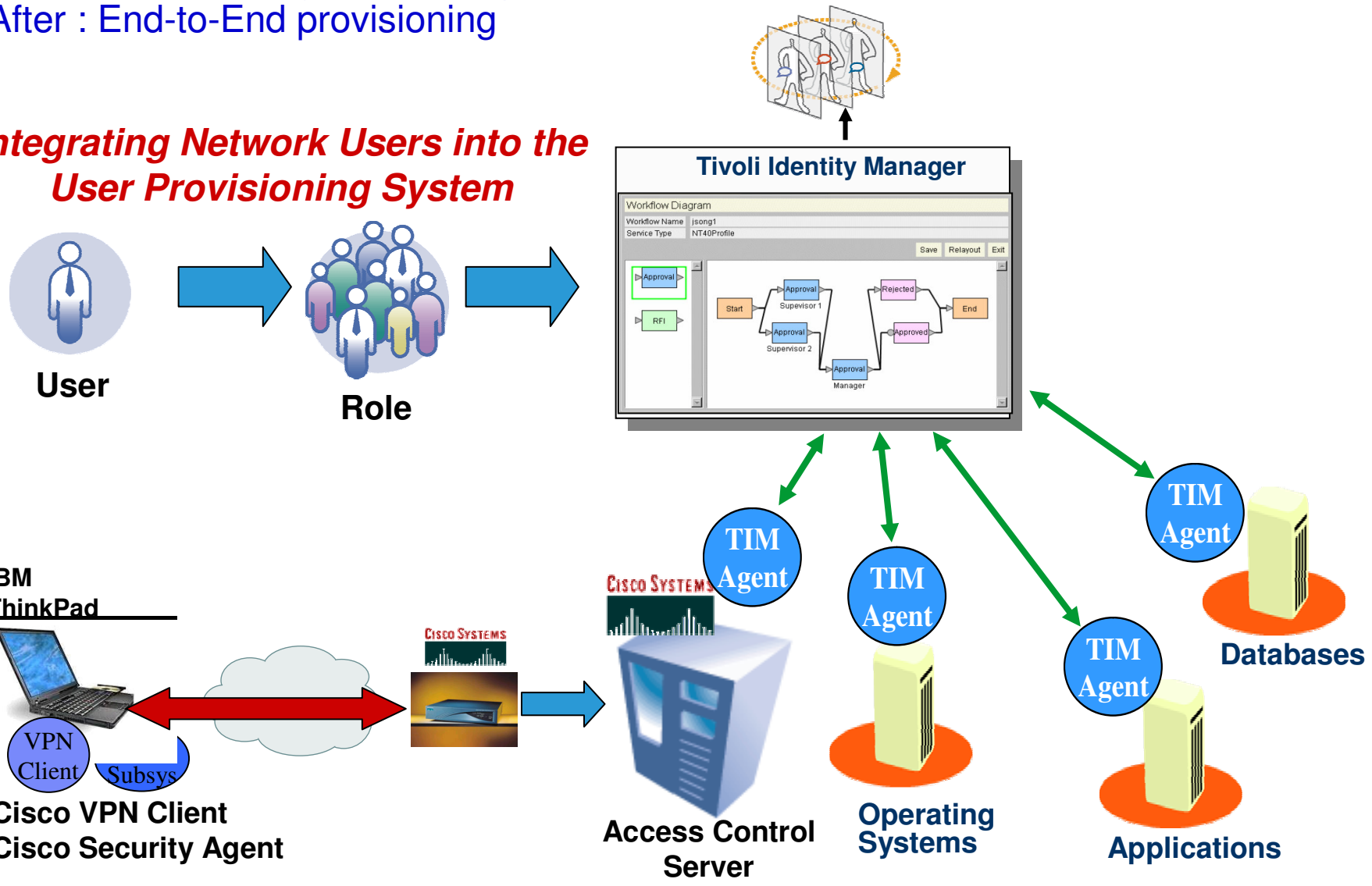
Provisioning / De-provisioning Users on the network



Tivoli Identity Manager + Cisco

After : End-to-End provisioning

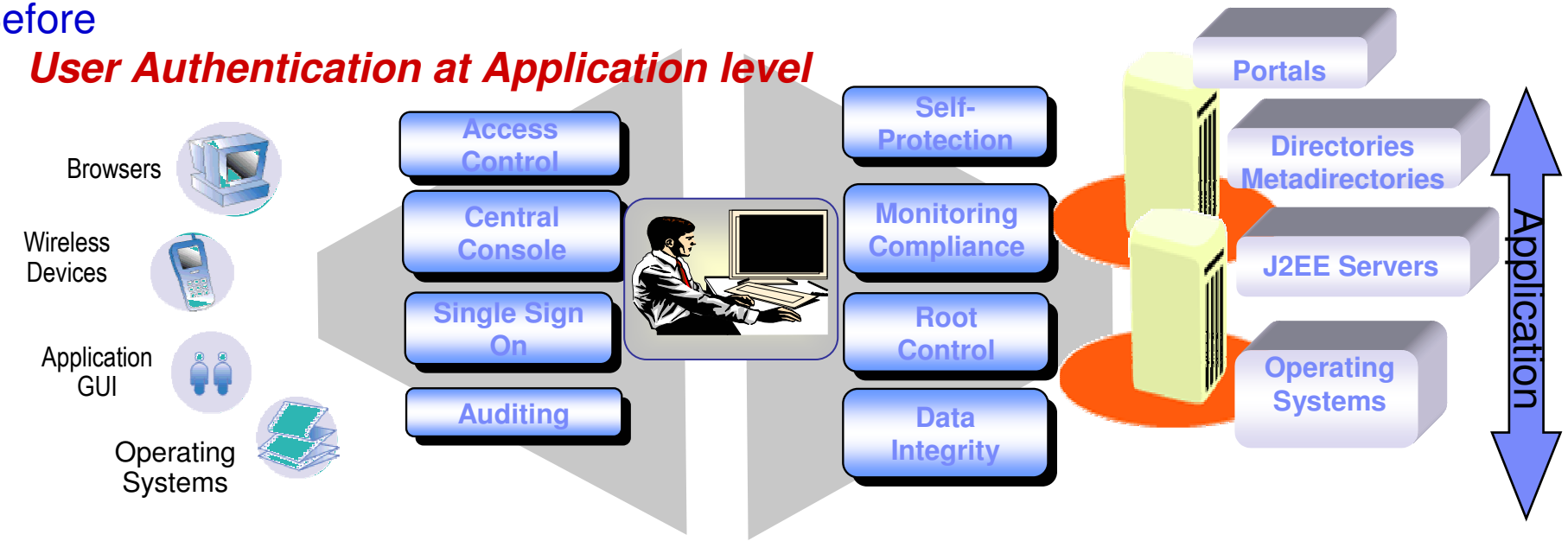
Integrating Network Users into the User Provisioning System



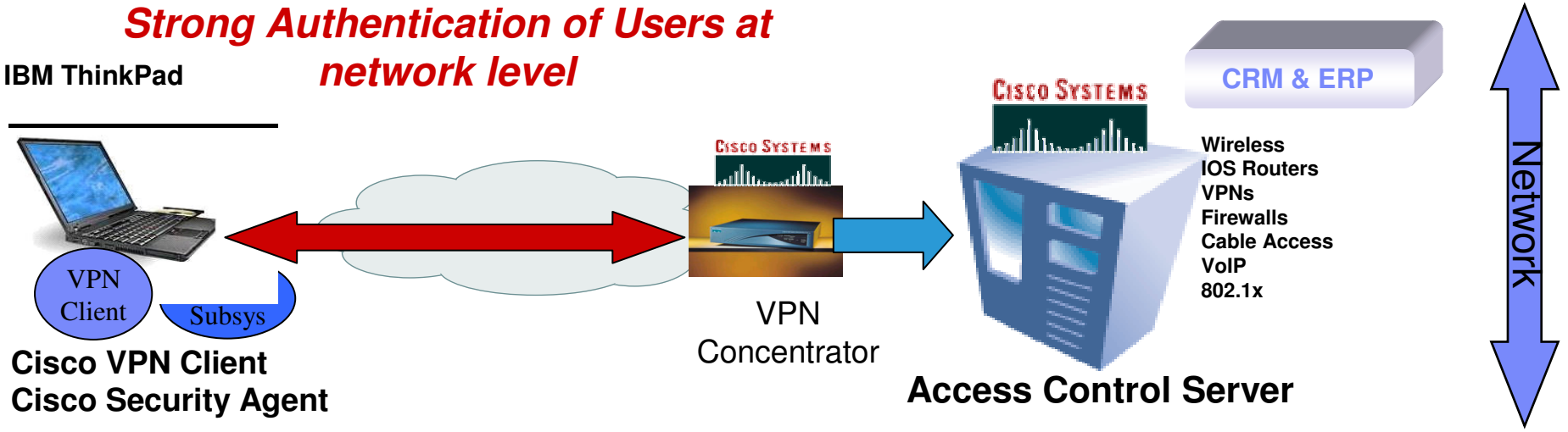
Tivoli Access Manager + Cisco

Before

User Authentication at Application level

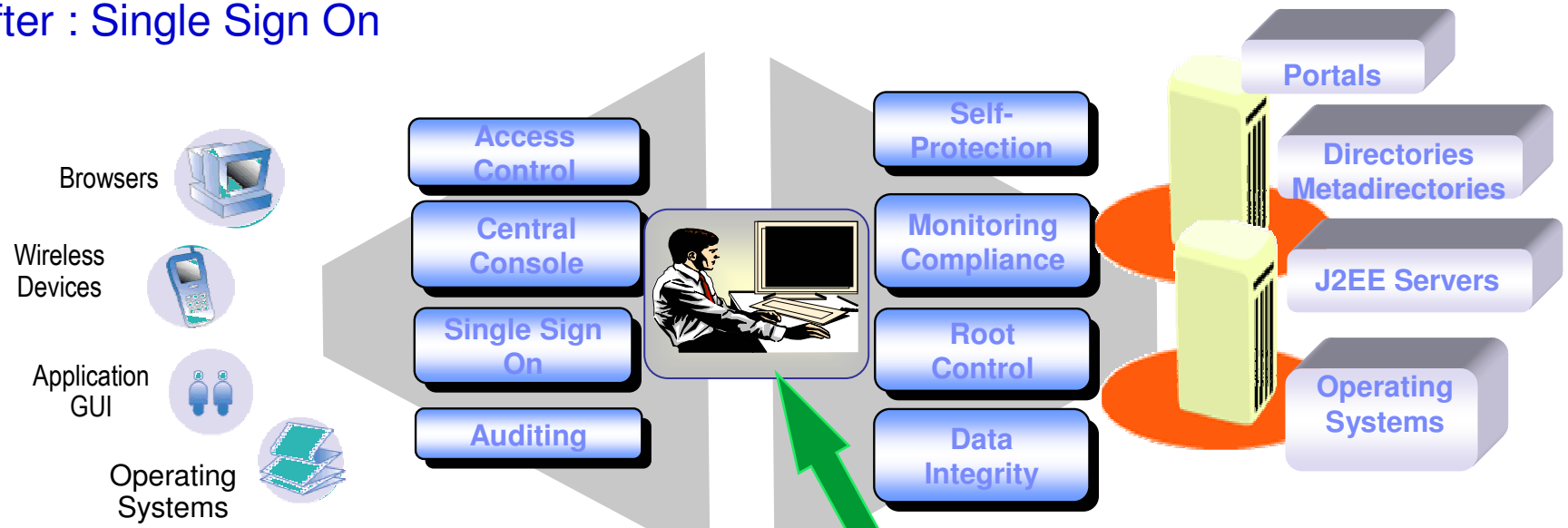


Strong Authentication of Users at network level



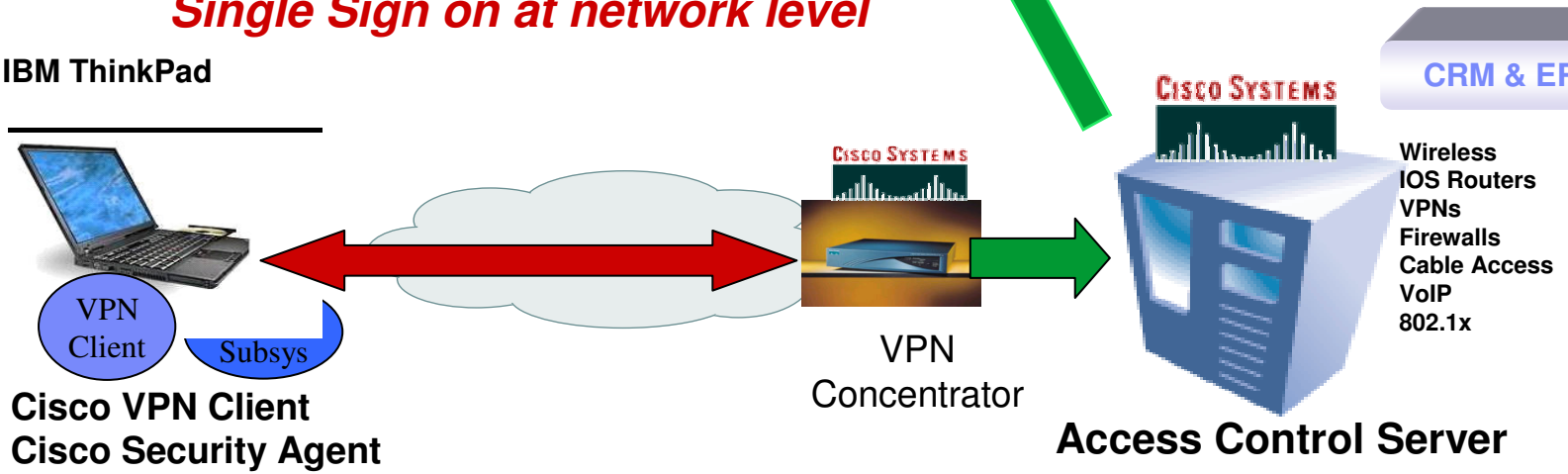
Tivoli Access Manager & Cisco

After : Single Sign On



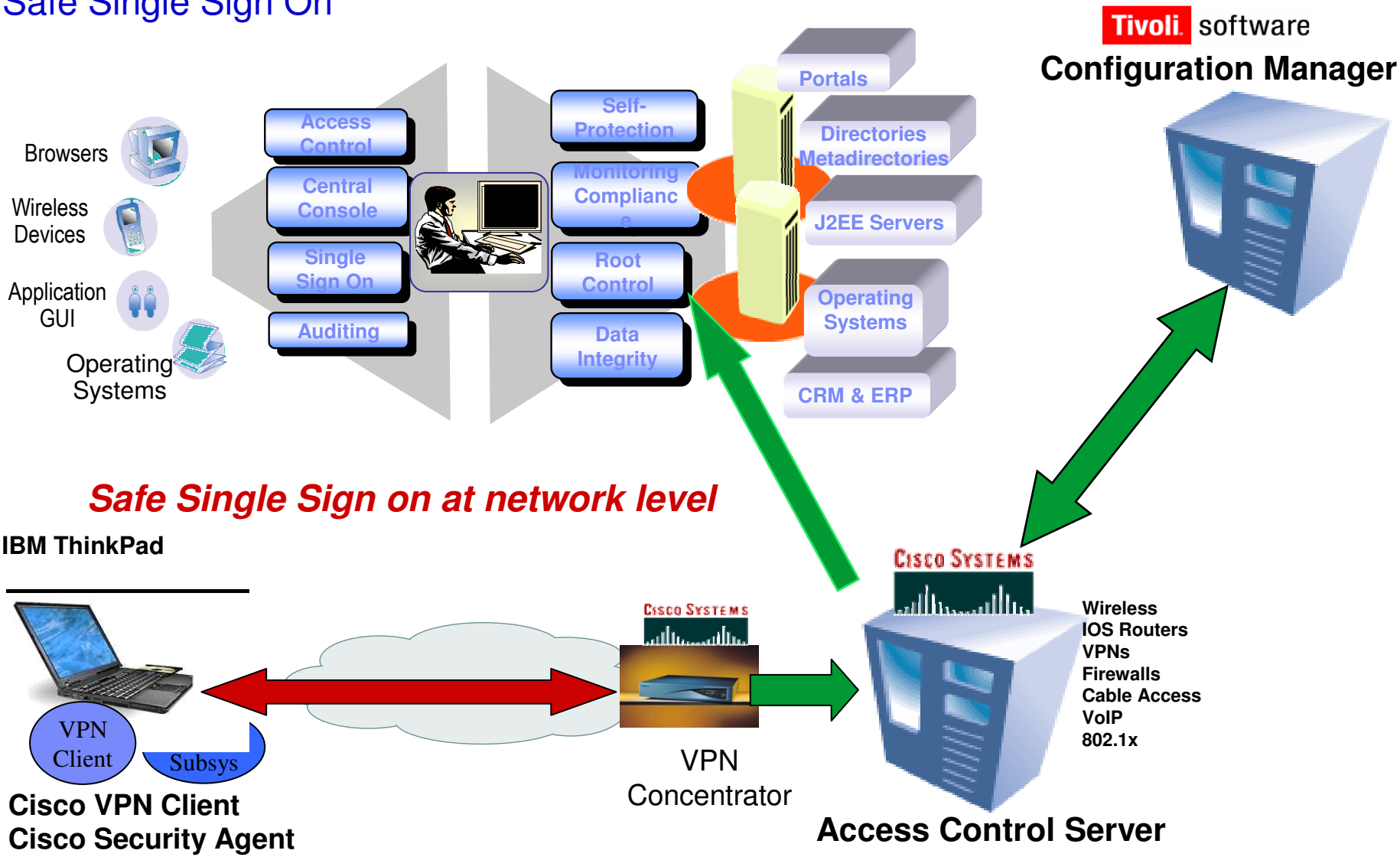
Single Sign on at network level

IBM ThinkPad



Tivoli Access Manager & Cisco - Extension

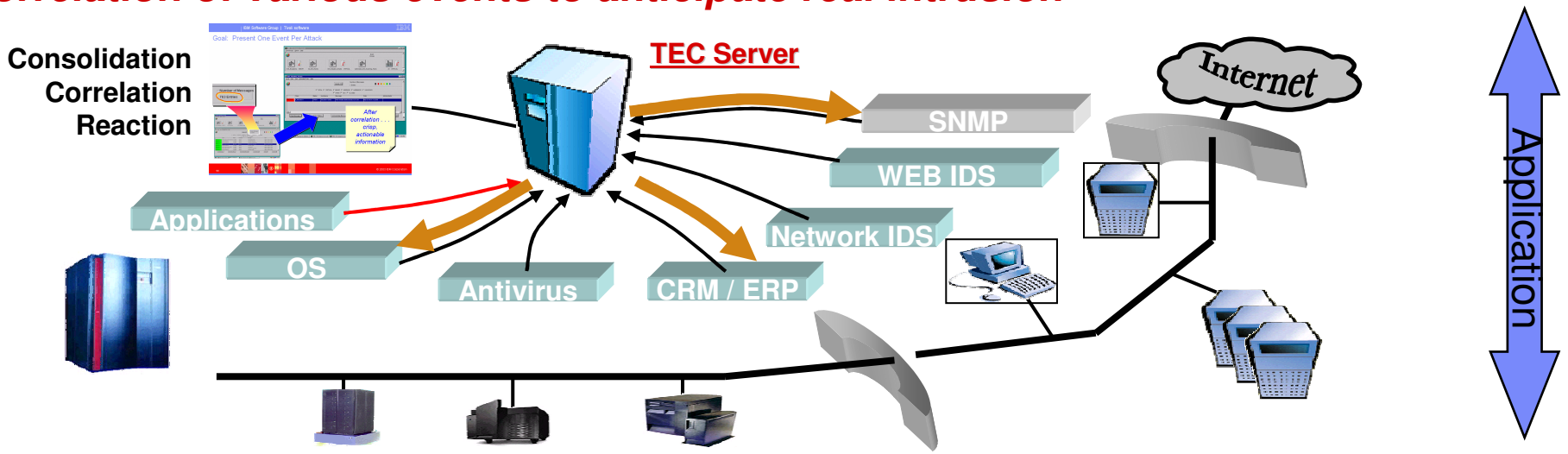
Safe Single Sign On



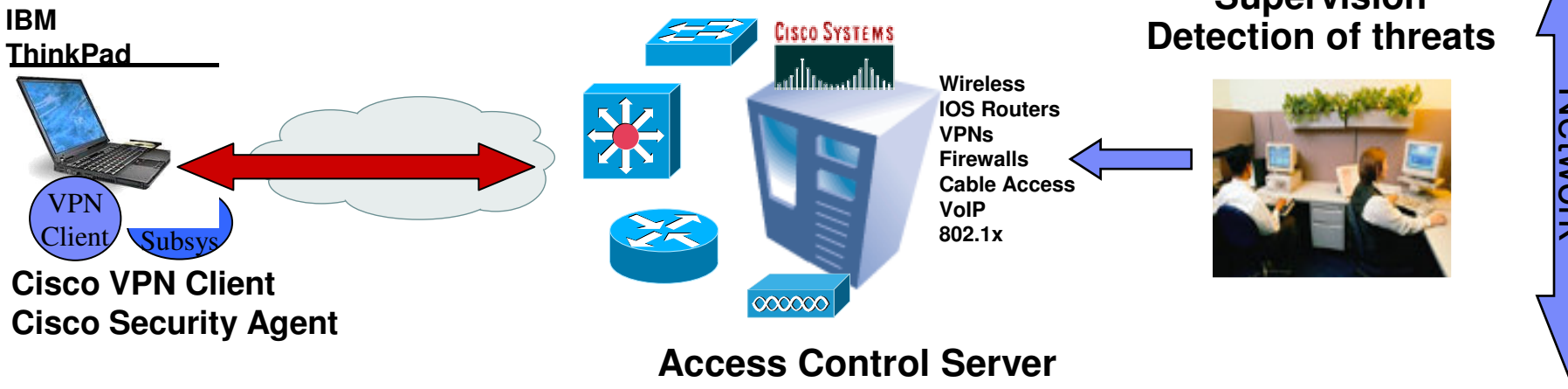
Tivoli Risk Manager + Cisco

Before

Correlation of various events to anticipate real intrusion



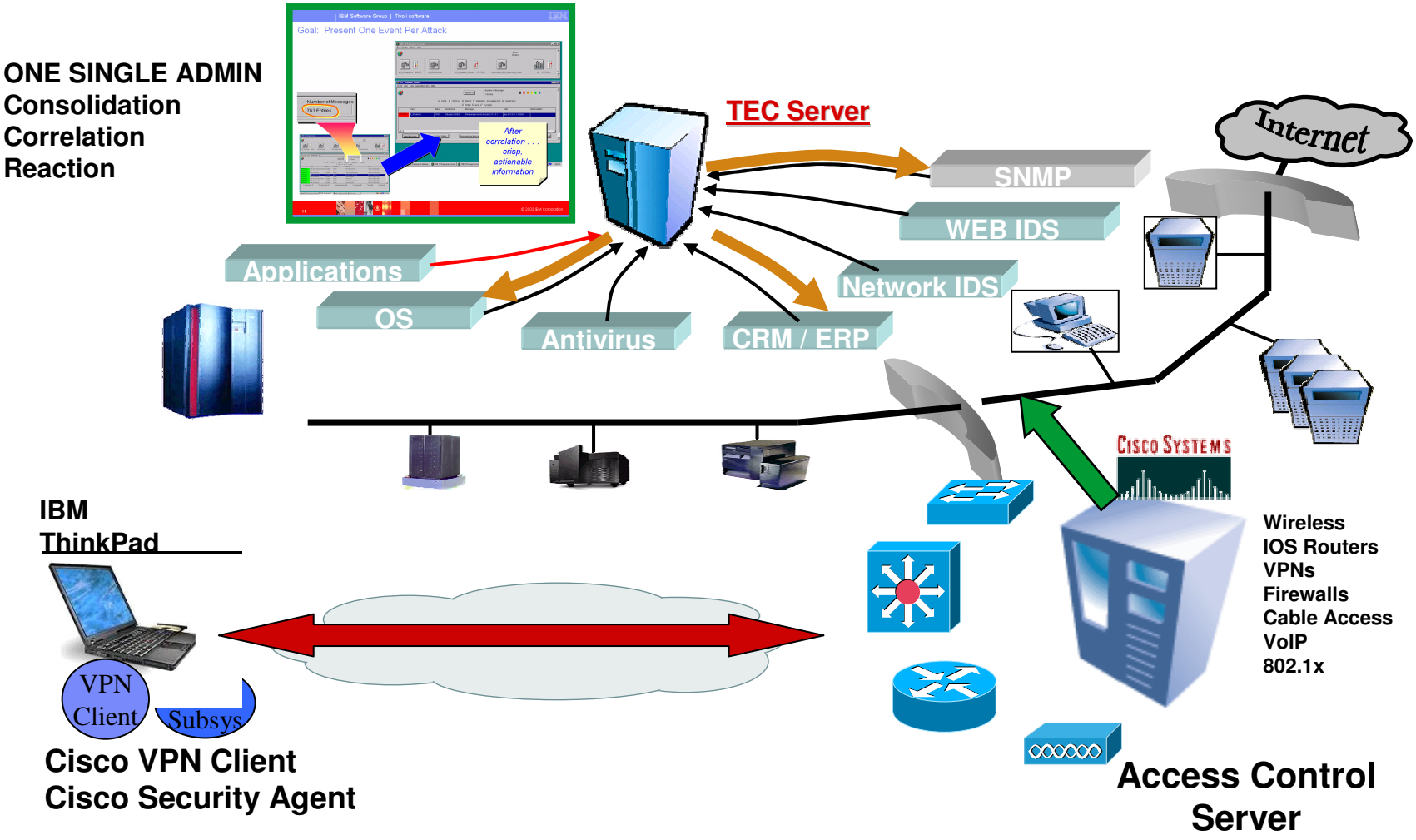
Detection of intrusion



Tivoli Risk Manager + Cisco

After integration

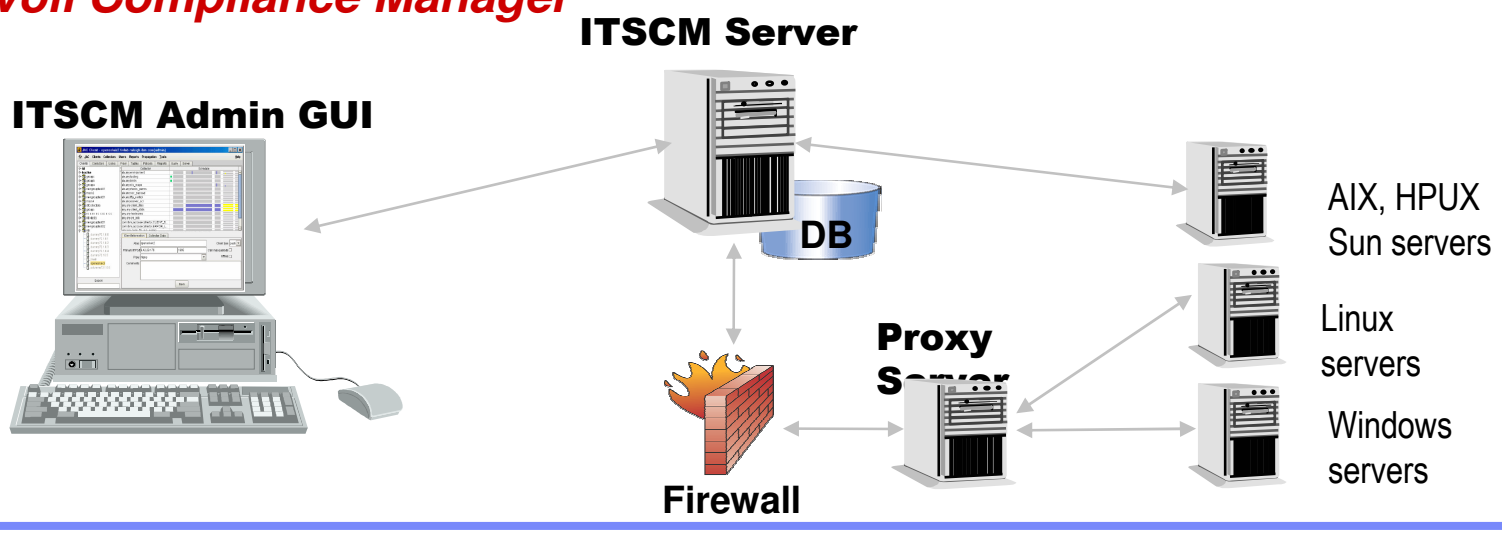
Correlation of various events including network events to anticipate real intrusion



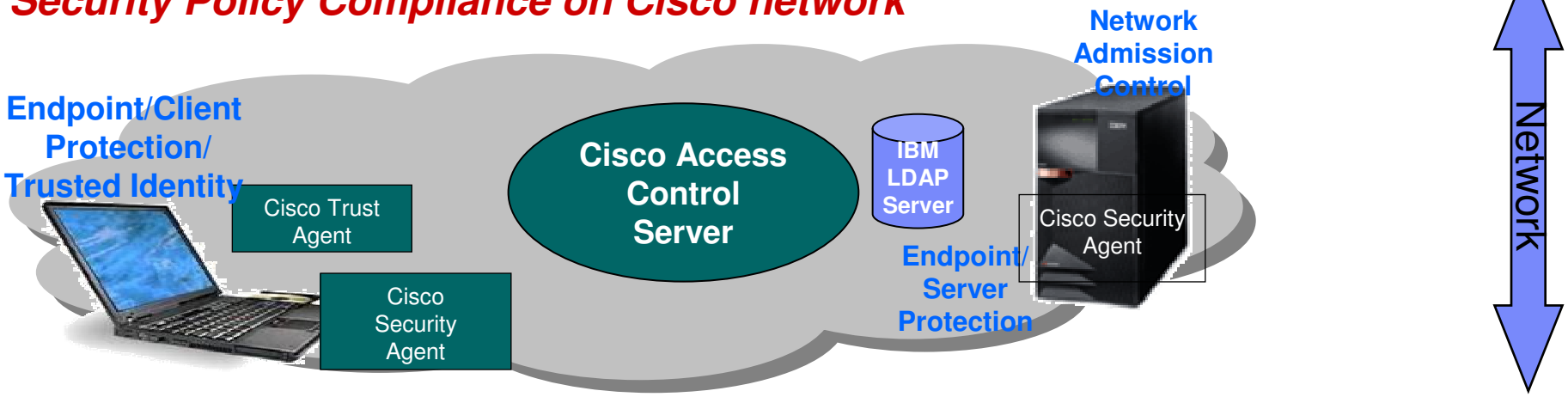
Tivoli Identity Manager + Cisco

Before

Tivoli Compliance Manager



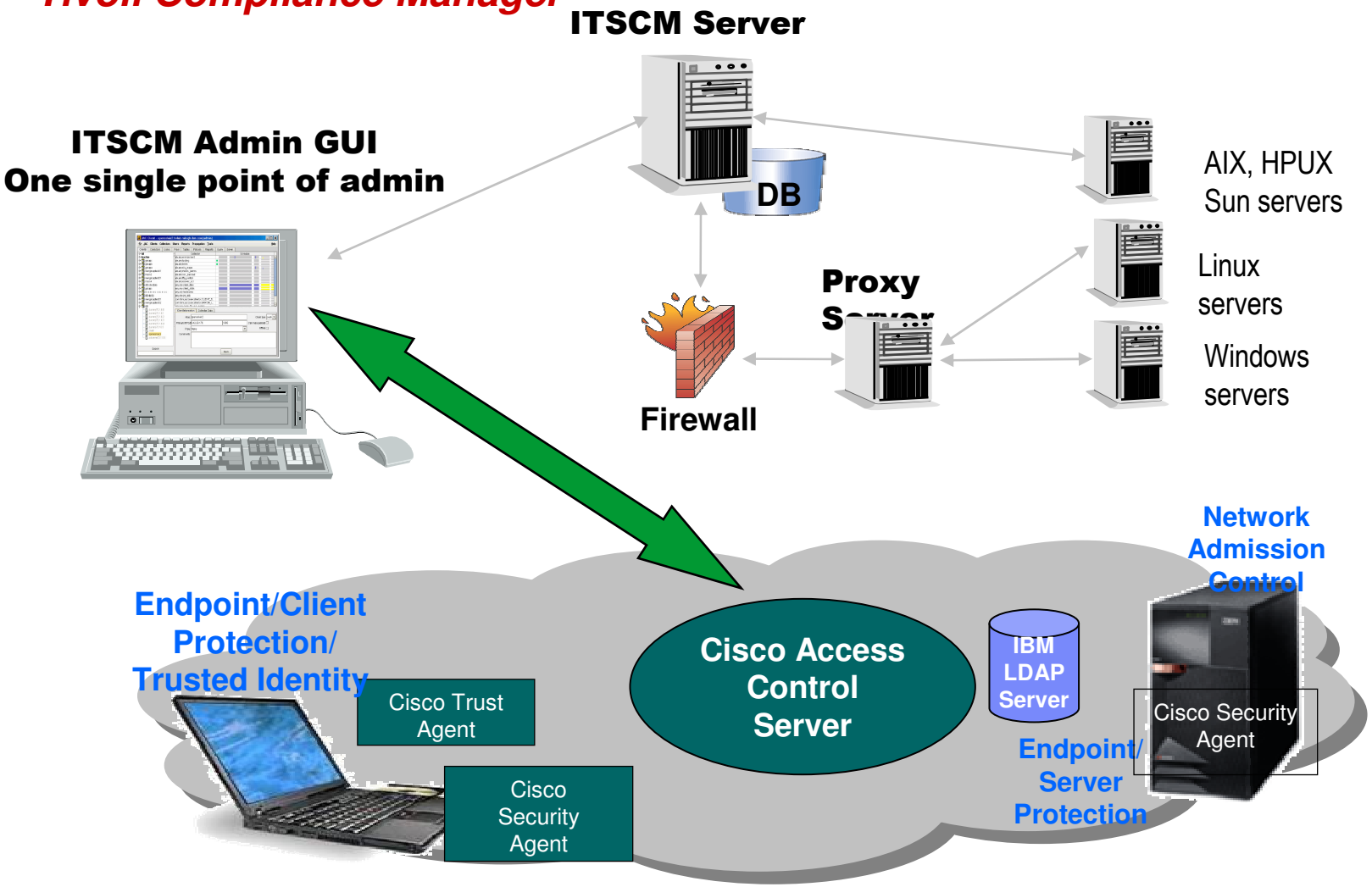
Security Policy Compliance on Cisco network



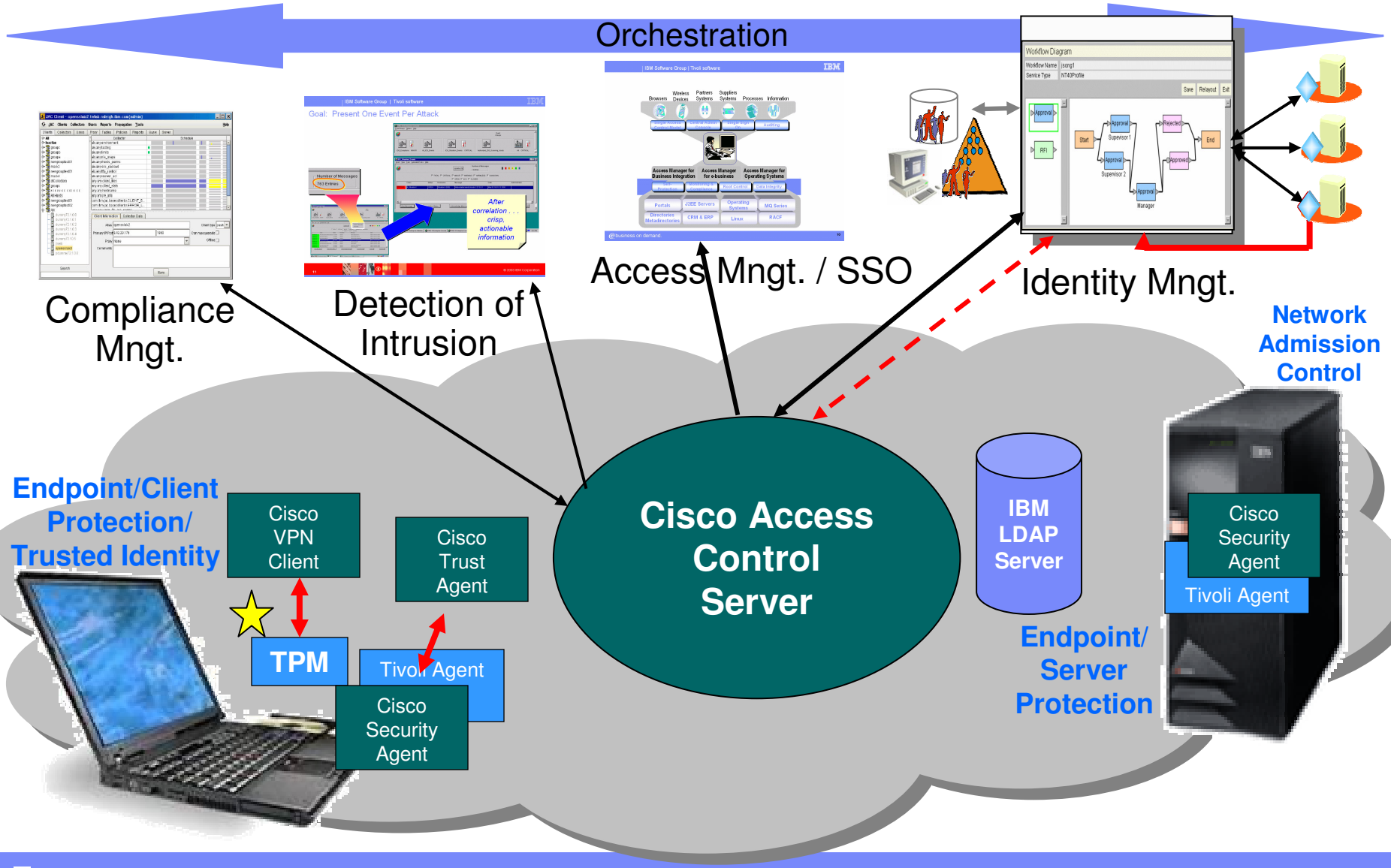
Tivoli Compliance Manager + Cisco

After : End to End integration

Tivoli Compliance Manager

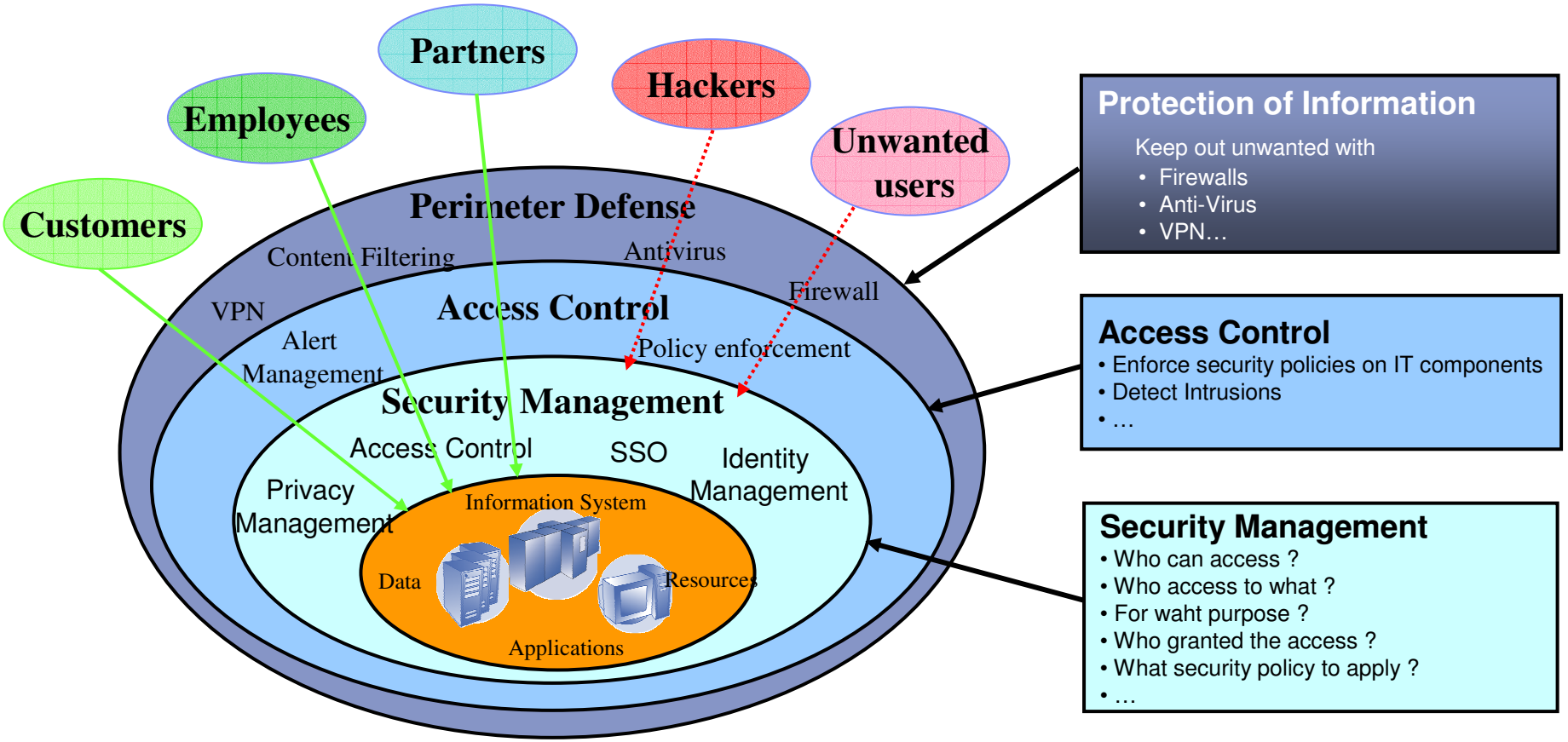


IBM/Cisco - The Big Picture



An Holistic Approach of Security

- The marriage of threat management with identity management to provide an holistic view of the protection of information in an open environment and reduce ongoing operations costs
- Increased Return on Security Investment through better optimization of security, identity and management resources



Security Solution