

# WEB Application Security

---

*il testimonial...*

*Infosecurity - FieraMilano, 8 Febbraio 2007*



# Agenda

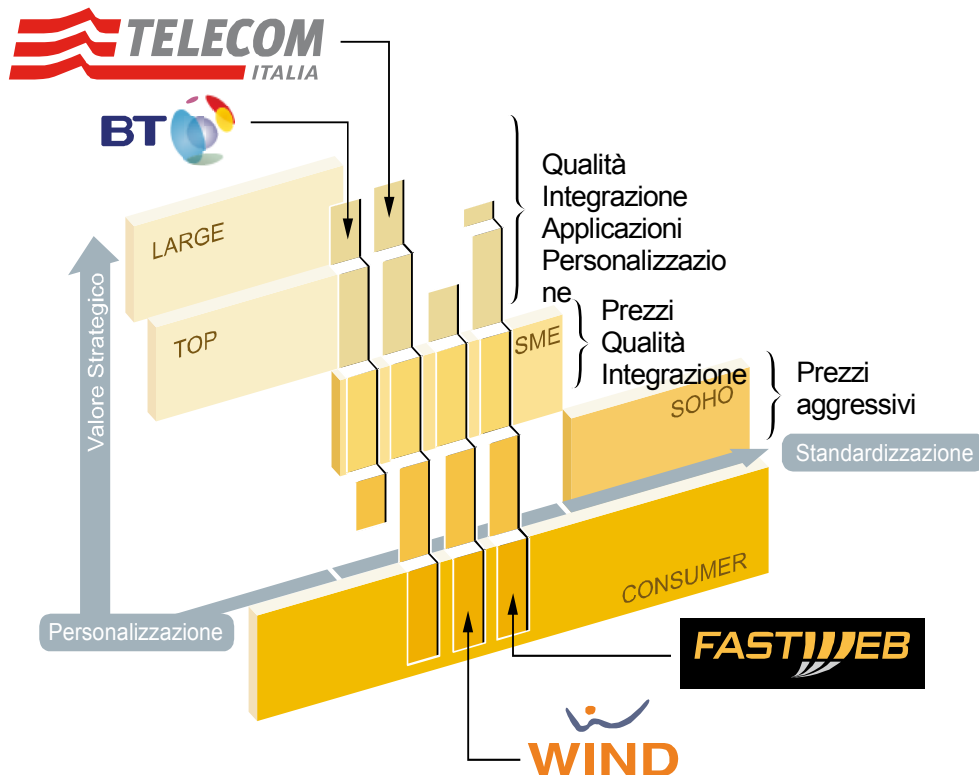
- ❑ BT Italia overview
  - ❑ *Posizionamento*
  - ❑ *Key Points*
  - ❑ *ed offerta*
  
- ❑ Il problema dDOS
  - ❑ *Evoluzione*
  - ❑ *Requisiti della soluzione*
  - ❑ *Descrizione della soluzione*
  - ❑ *Caratteristiche della soluzione*
  - ❑ *Benefici*

# BT Italia sul mercato

Il mercato totale TLC, segmento business, registrato nel 2005, è di circa 8,18 mld €.

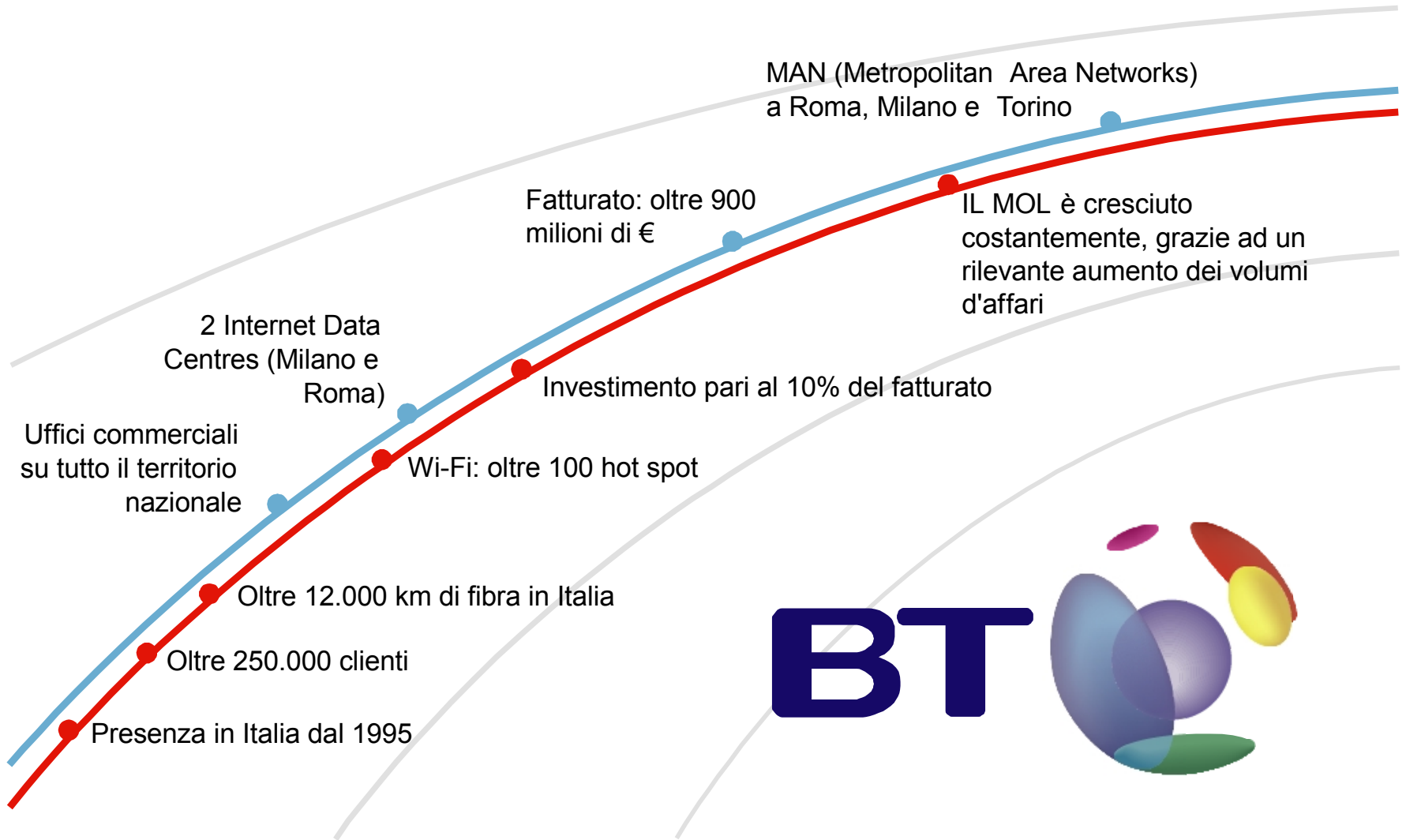
**BT Italia è l'unico operatore specializzato esclusivamente nel mercato business,**

**Top & Large Account, con una quota di circa il 9%**



- 11 Sedi
- Oltre 1.300 dipendenti
- Oltre 250.000 Clienti Business
- Fatturato Oltre 900 mln €

# Key Points


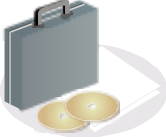


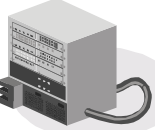



**BT**



# Il portafoglio dei Servizi

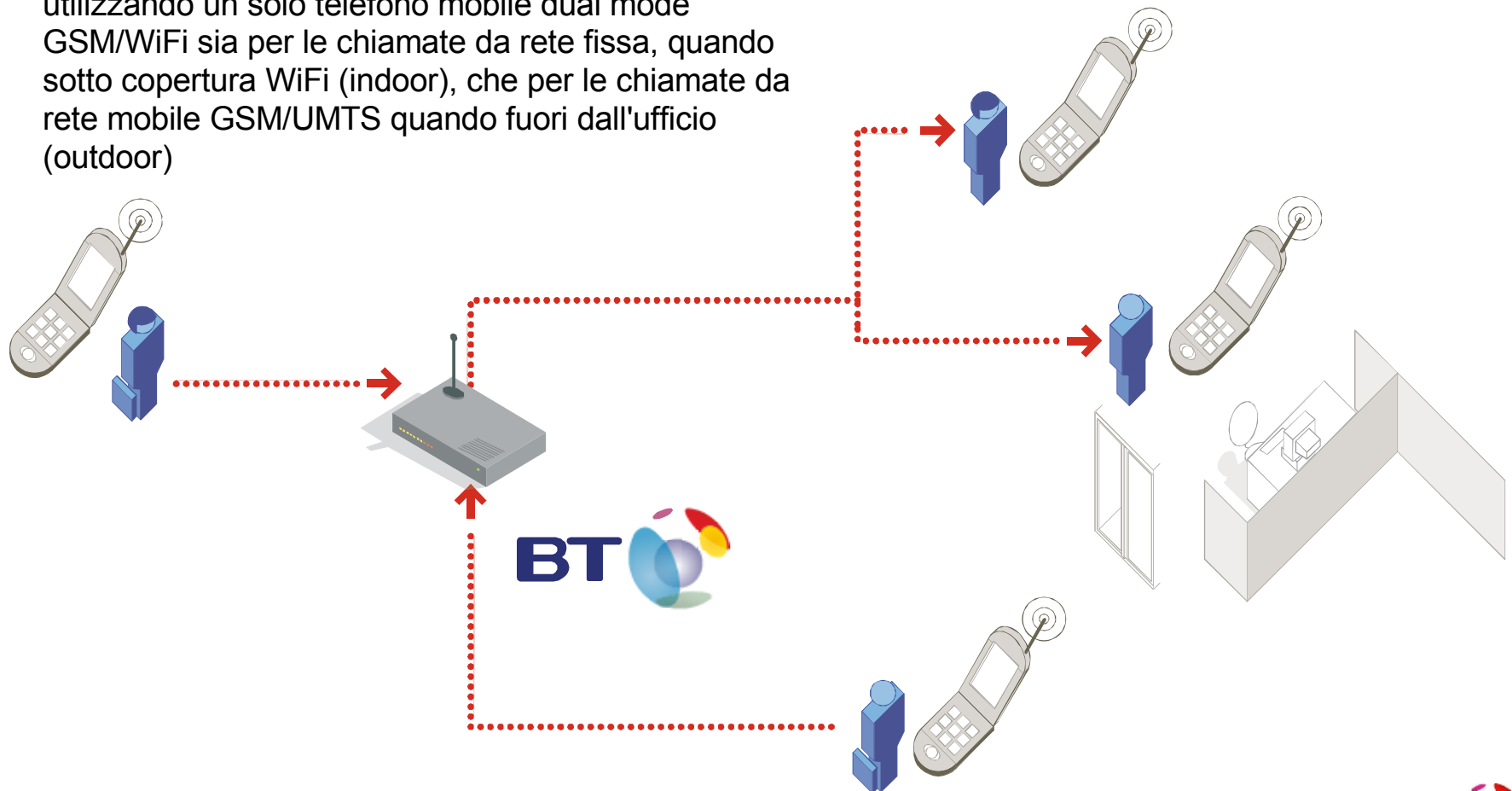
## Soluzioni ICT integrate

	Business services	Outsourcing di rete	Business process outsourcing	Enterprise security	Systems integration	Business & tech. consulting
	Servizi e applicazioni IT	E-commerce	Portali ed Intranet	Applicazioni CRM	Desktop gestito	BT Managed Applications
	Servizi a valore aggiunto	Hosted IP Telephony	BT Hosting & storage	Outsourced Call Centre	Hosted Contact Centre	Messaging
	Servizi gestiti	BT IP Voice	Gestione LAN/WAN	BT Contact Centre	Managed mobility	BT One Security
	Servizi di rete	BT Business Voice	BT Private Line	BT Frame/ATM	BT MPLS	BT Internet Access
	Reti e accesso	Wireless	Fibra	Linee affittate	DSL	Ethernet

# La nuova soluzione per le aziende

## BT Corporate Fusion

BT Corporate Fusion integra le soluzioni di mobilità utilizzando un solo telefono mobile dual mode GSM/WiFi sia per le chiamate da rete fissa, quando sotto copertura WiFi (indoor), che per le chiamate da rete mobile GSM/UMTS quando fuori dall'ufficio (outdoor)



## Il Problema dDoS

---



# Un'infrastruttura a prova di attacco: genesi problema dDoS

- Consapevolezza di attacchi saltuari su alcuni clienti
- Verifica decrementi prestazionali saltuari su alcuni target infrastrutturali
- Attacco a cliente finale con saturazione della banda e conseguente decremento prestazionale
- Esigenza di gestire un'infrastruttura di rete scevra da traffico malevolo o "sporco"
- Necessità di fornire un servizio di connettività sicuro e qualitativamente costante

# Un'infrastruttura a prova di attacco: requisiti della soluzione

- **Specificità della soluzione mirata a:**
  - rilevazione tempestiva dell'attacco
  - determinazione delle caratteristiche (provenienza, protocolli,...)
  - monitoring dell'evoluzione dell'attacco
  - remediation
- **Continuità delle applicazione critiche**
  - sotto attacco
  - non sotto attacco
- **Trasparente all'utenza**

# dDoS Mitigation: descrizione della soluzione

---

## Step 1

- Monitoring (Detection)
  - *Provider internazionali*
  - *Neutral Access Points (NAPs)*
  - *Peering nazionali*
- Due centri di remediation che operano il cleaning del traffico vicino alla sorgente dell'attacco

## Step 2

- Estende il monitoraggio alla totalità del backbone
- Attivazione di ulteriori centri di cleaning

# Un'infrastruttura a prova di attacco: caratteristiche della soluzione

- Funzionalmente e tecnologicamente innovativa (comportamento traffico in rete)
- Efficace nella prevenzione degli effetti e nel trattamento degli attacchi
- Modulare e scalabile
- Gestibile
- Non invasiva nei confronti del cliente finale

# Un'infrastruttura a prova di attacco: benefici della soluzione

- Incremento del livello di sicurezza del backbone
- Fornitura di servizi di connettività sicuri ed a performance costanti
  - Gestione della qualità x servizi multimediali
- Eliminazione di traffico malevolo/inutile presente in rete
- Protezione della service continuity cliente

*Una scelta di performance, di sicurezza,  
di qualità e affidabilità nel tempo*



**Marco Medici**

*Responsabile Rete & Architetture IP*

BT Italia

*Marco.Medici@bt.com*