



---

# Business Continuity

**Le implicazioni imposte da Basel 2**

**Come soddisfarle con la realizzazione di  
Infrastrutture IT ad Alta Disponibilità**

*Massimo Galbiati, System Engineer, APC Italia*

# Parleremo di ...



- **Basilea 2: le direttive per ridurre il rischio operativo**
- **Caratteristiche di un Sistema Informativo ad Alta Disponibilità: L'INFRASTRUTTURA**
- **Le tendenze tecnologiche nei CED: un rischio per la Business Continuity**
- **Ridurre il Rischio Operativo anche garantendo la continuità operativa grazie ad un SI ad Alta Disponibilità realizzato con infrastruttura per CED "on-demand"**



- **Basilea 2: le direttive per ridurre il rischio operativo**

# Accordo Basilea 2: in sintesi



- Basilea 2 è il nuovo accordo internazionale sui requisiti patrimoniali delle banche siglato dal G10 il 28 Giugno 2004.
- In base ad esso le banche dei paesi aderenti dovranno accantonare quote di capitale proporzionali al rischio derivante dai vari rapporti di credito assunti.
  - Maggior rischio = maggiori accantonamenti, quindi per la banca maggiori costi.
- Le banche dovranno classificare i propri clienti in base alla loro rischiosità, attraverso procedure di rating sempre più sofisticate.
  - Per le imprese più rischiose minor credito e a tassi più elevati.

*Appare quindi evidente la necessità che le imprese, ed in particolare le PMI, pongano in essere tutte quelle politiche, gestionali e di bilancio, atte a rafforzare la propria struttura e la propria immagine per affrontare serenamente l'esame dei rating*

*bancari → ADOTTARE LO STESSO RATING BASILEA 2 !!!*

# Accordo Basilea 2 per tutte le imprese



*(Obbligatorio per Istituti Internazionali o Banche Centrali)*

- **Documento guida per per diminuire il rischio d'impresa ed avere un miglior rating → minori costi bancari**

- **3 pilastri:**

- 📁 **Capitale minimo obbligatorio a garanzia del rischio**

- Cap.V: Il Rischio Operativo

- 📄 **Processo di revisione e controllo da parte delle Banche Centrali**

- 📄 **Miglioramento della disciplina di mercato grazie a dettagliata trasparenza al pubblico**

# Accordo Basilea 2 – Il Rischio Operativo



## Cap. V - Definizione di rischio operativo

- **644. Il rischio operativo è definibile come il rischio di perdite derivanti dalla inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni.**
  - **Il Rischio Operativo** include rischi di ogni tipo, dai disastri naturali al dolo del personale, errori di inserimento dati, rischi interni ed esterni, e **si applica a tutta la infrastruttura ICT**
- **Eventi di Rischio (all.7):**
  - **Guasti nei Sistemi Informativi:**
    - **Perdite causate da guasti o malfunzionamenti di HW, SW e telco**
    - **Interruzione o problemi di energia elettrica o di componenti di alimentazione**

# Accordo Basilea 2: i passi

---



- Basilea 2 entrerà in vigore a fine 2006 ma dato che le banche dovranno dimostrare l'aderenza alle direttive per almeno 3 anni, in realtà è da inizio 2004 che molte si sono adeguate e già sono noti gli effetti di questa stretta creditizia
- Uno dei principi della gestione del Rischio operativo:
  - “E' necessario garantire la **Business Continuity**”

*Ci sono accadimenti da cui è necessario cautelarsi e che vanno al di là di ogni ragionevole controllo: disastri naturali, **mancaanza di alimentazione elettrica**. Una veloce ripartenza dei sistemi è essenziale!!*



- 
- **Altri riferimenti sulla sicurezza dei SI e la Business Continuity:**
    - La legge 196/03 sul trattamento dei dati
    - Le raccomandazioni COBIT by ISACA
    - OCSI

# D. Lgs. n. 196/2003 (96/45/CE e 2002/58/CE)



## Art. 34

### Trattamenti con strumenti elettronici

- Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
  - a) .....
  - f) adozione di procedure per la custodia di copie di sicurezza, **il ripristino della disponibilità dei dati e dei sistemi**

# COBIT by ISACA



L'Information Systems Audit and Control Association (ISACA) è stata fondata negli USA nel 1967 e raggruppa più di 28.000 professionisti nelle aree dell' IS Auditing ed IT Security.



“Control Objectives for Information and related Technology” (COBIT), giunto alla terza edizione, è un framework sviluppato da ISACA che aiuta le organizzazioni a gestire i rischi IT e ad assicurare che i processi IT siano coerenti con le necessità di business.

# COBIT by ISACA: obiettivi



L'obiettivo della “Sicurezza delle Informazioni” è proteggere gli interessi di coloro che fanno affidamento sull'informazione e sui sistemi e sulle comunicazioni che forniscono l'informazione dai danni causati dalla mancanza di **disponibilità**, riservatezza e integrità.

La DISPONIBILITA' è garantita quando:

- **Il Sistema Informativo è disponibile** ed utilizzabile quando richiesto, **e può resistere** adeguatamente ad attacchi e **ripristinarsi dopo una interruzione**



## *Cosa si intende per “sicurezza...”*

*Nell’ambito dello Schema nazionale, la ‘sicurezza nel settore della tecnologia dell’informazione’ è definita come la protezione della riservatezza, integrità, disponibilità delle informazioni mediante il contrasto delle minacce originate dall’uomo o dall’ambiente, al fine di impedire, a coloro che non siano stati autorizzati, l’accesso, l’utilizzo, la divulgazione, la modifica delle informazioni stesse e di garantirne l’accesso e l’utilizzo a coloro che siano stati autorizzati*

=

# BUSINESS CONTINUITY

# L'accezione della "Sicurezza dei SI"



## ■ La Sicurezza dei Sistemi Informativi:

Sicurezza contro accessi fisici	+
Sicurezza contro accessi logici	+
Sicurezza contro eventi socio-politici	+
Sicurezza contro eventi atmosferici	+
Sicurezza contro disastri naturali	=

-----  
**DISPONIBILITA' DEI DATI AL 100%**

**=**

**BUSINESS CONTINUITY**

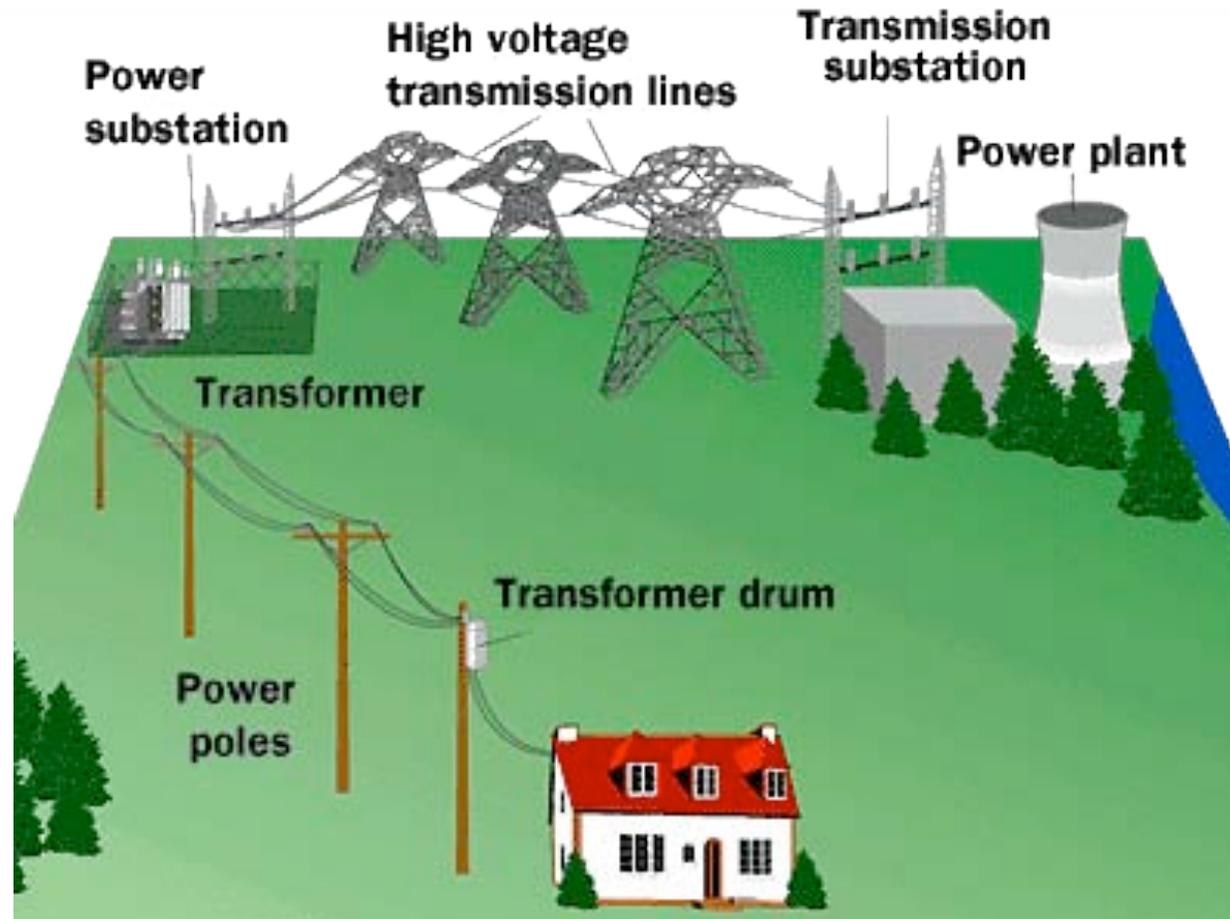


# Sicurezza: Imposizione o Necessità?

---

- **Implementare la sicurezza: Perché?**
  - Lo faccio perché me lo impone la legge?  
**(REAZIONE)**
  - Lo faccio perché è necessaria per la mia Azienda?  
**(AZIONE)**

# Quanti Punti Critici Esistono?

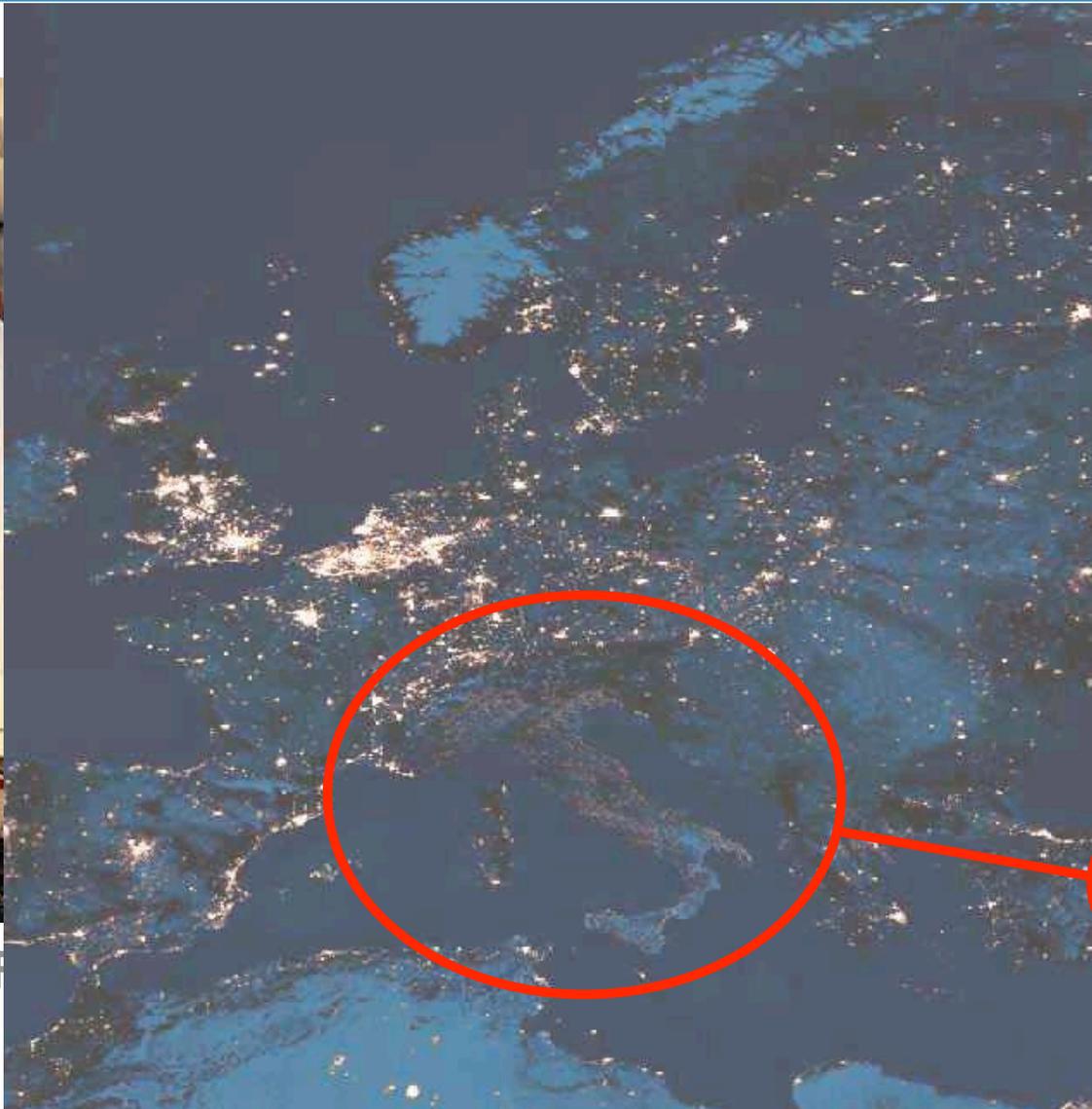


**Impossibile Prevederlo!!**

# Siete Pronti a Gestire.....



Madrid – P



94

**Italia**  
**28 Sett. 2003**

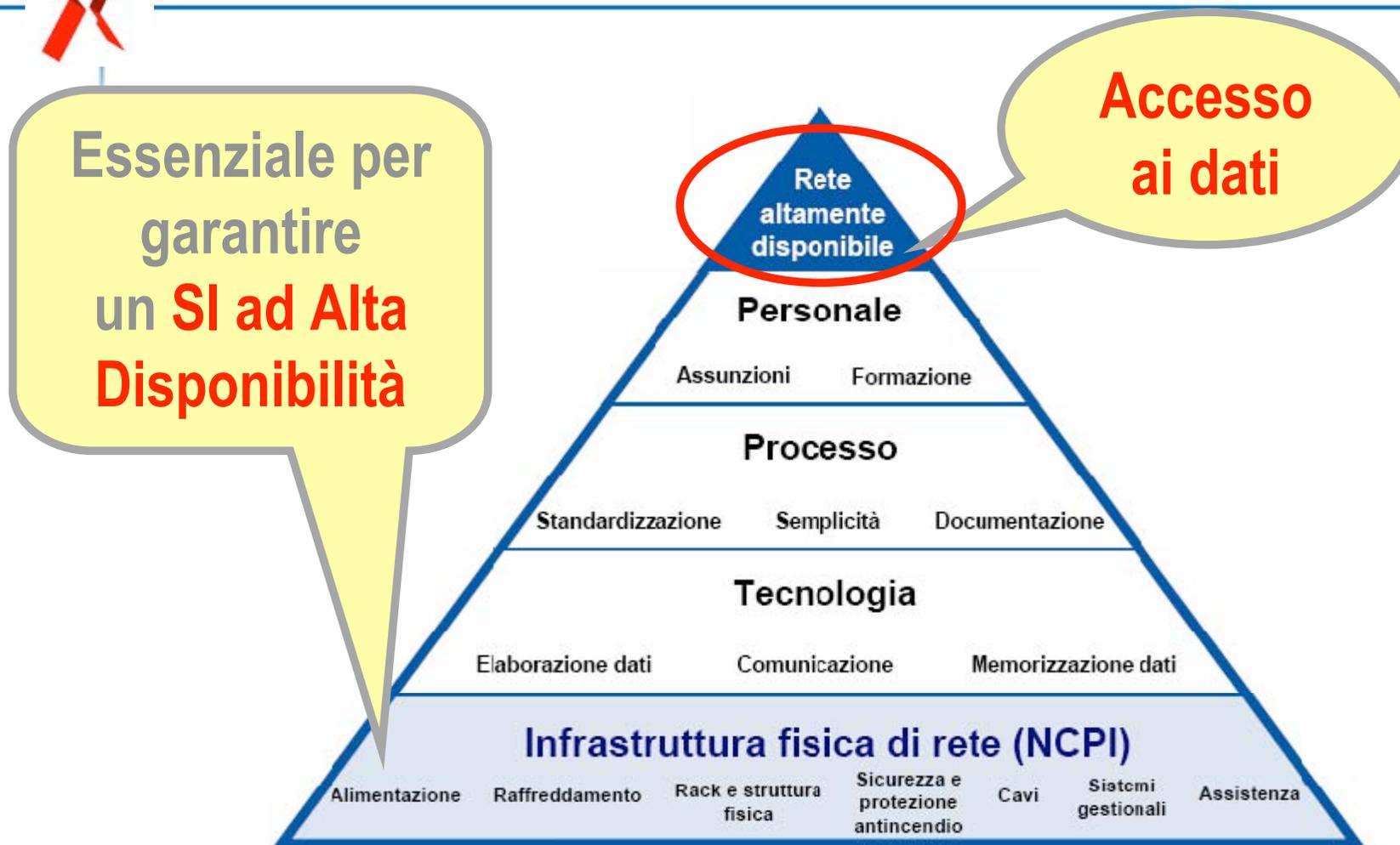
**ciscoexpo**  
**2005**

**APC**  
Legendary Reliability™

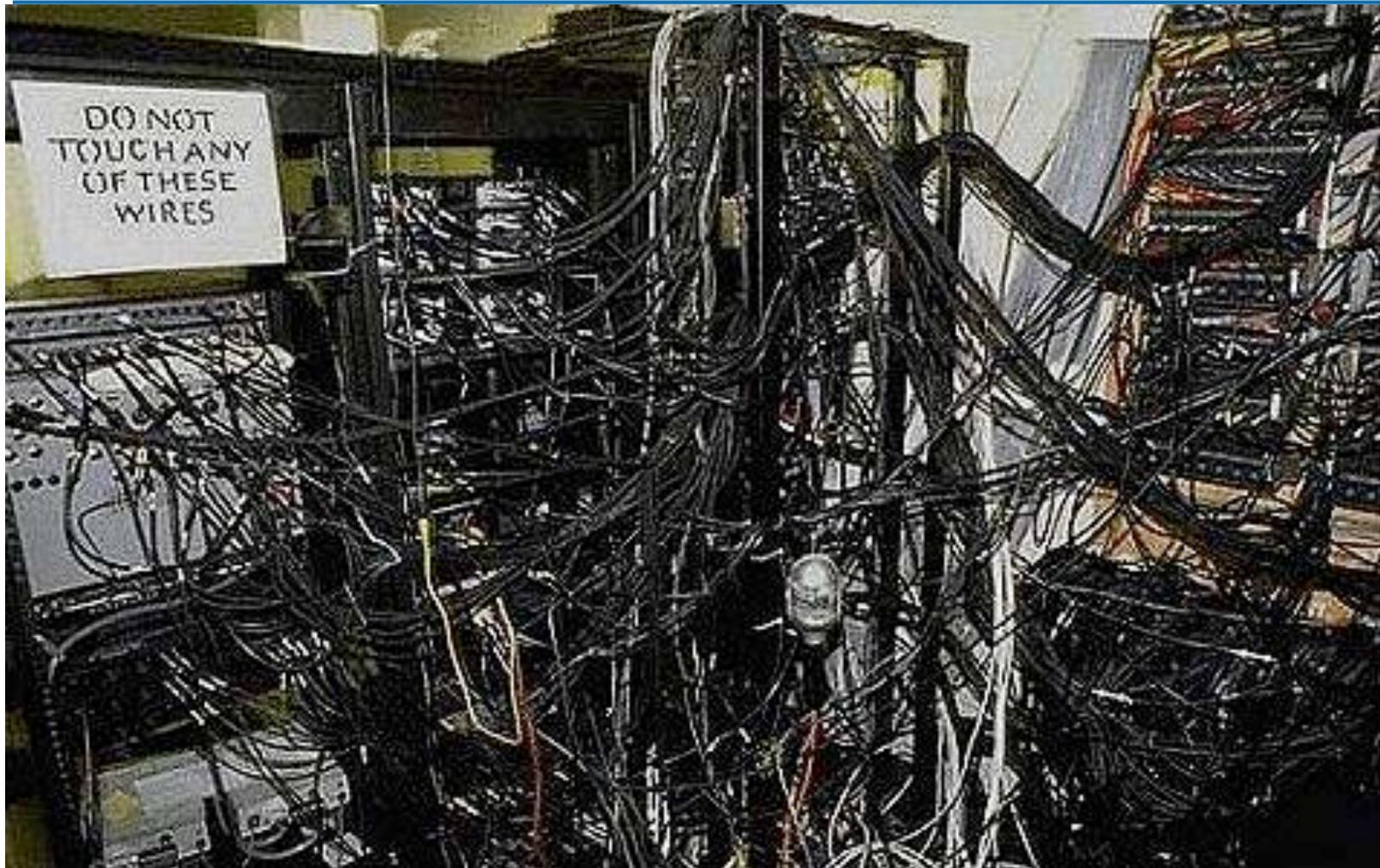


- **Caratteristiche di un Sistema Informativo ad Alta Disponibilità: L'INFRASTRUTTURA**

# La Piramide della Business Continuity



## Infrastrutture ...

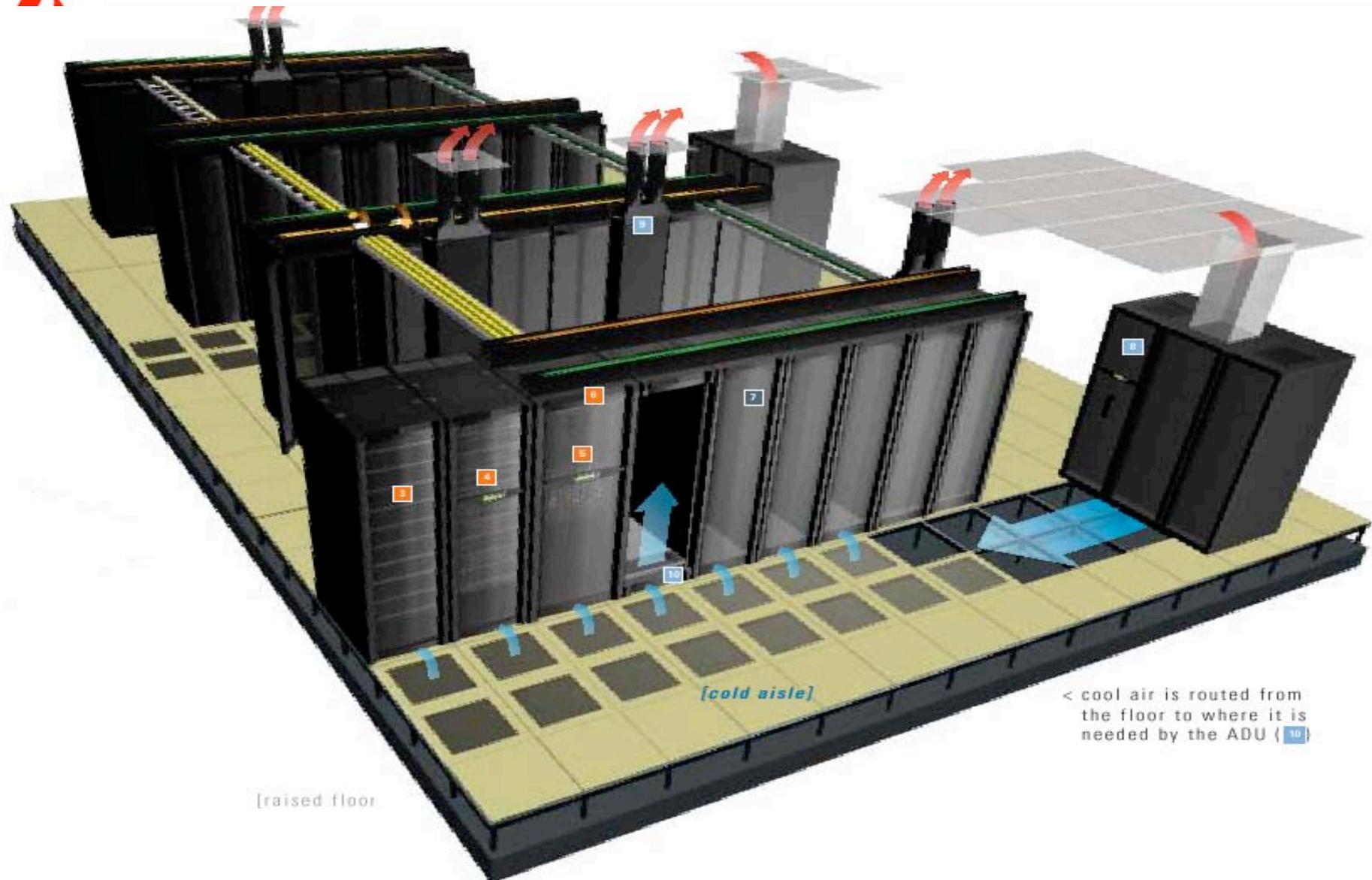


**Come garantire la Business Continuity con  
infrastrutture fisiche simili ?**

**ciscoexpo  
2005**

**APC**  
Legendary Reliability™

# Infrastrutture Fisiche di Rete



[raised floor]

[cold aisle]

< cool air is routed from the floor to where it is needed by the ADU (10)



- **Le tendenze tecnologiche nei CED: un rischio per la Business Continuity**

# I CED evolvono: quali rischi per la BC ?

---

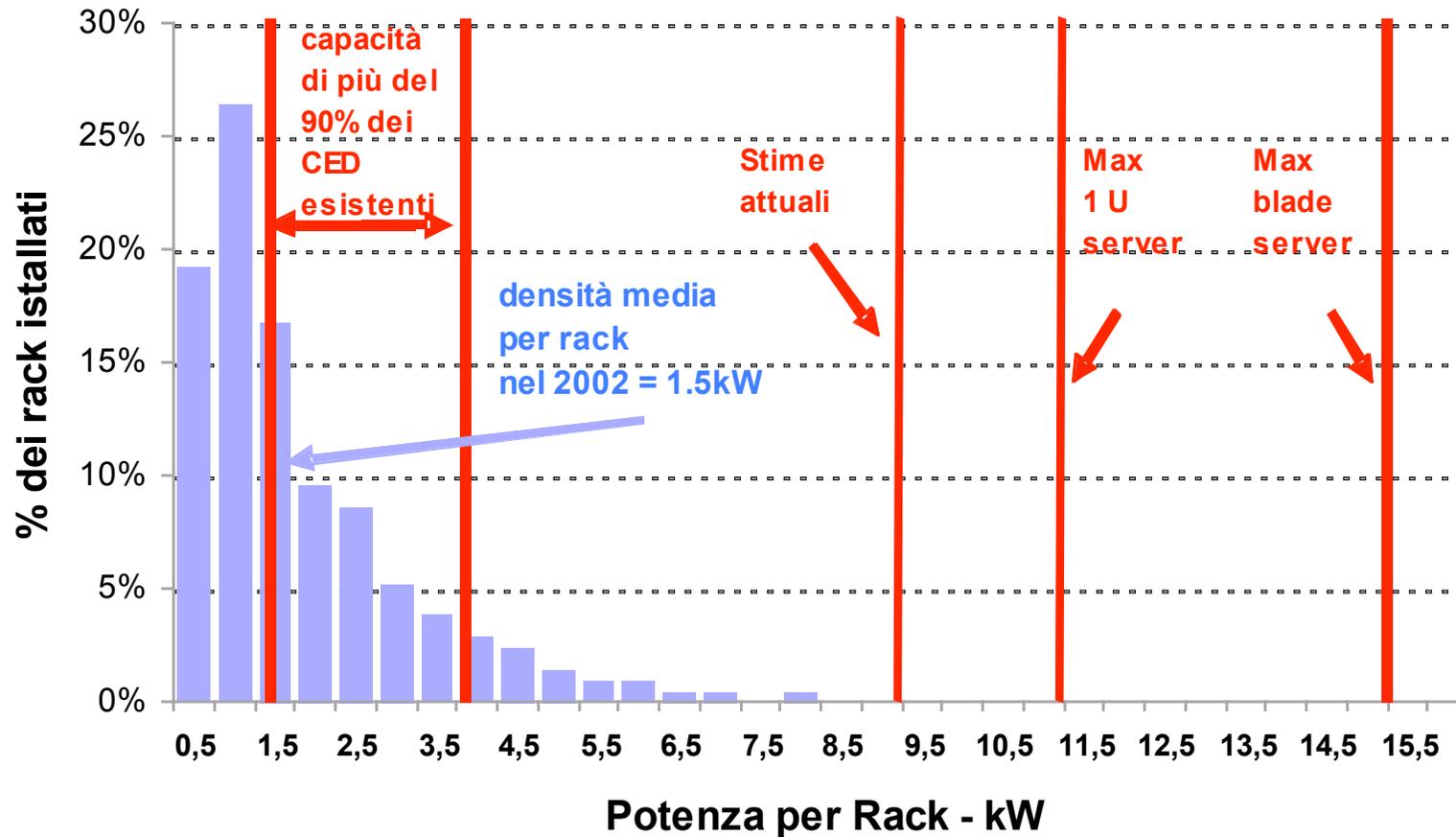


- **Problema 1: Aumento della potenza per singolo rack con server a tecnologia BLADE rende necessario il raffreddamento ad alta densità**
- **Problema 2: Modularità e Flessibilità dell'Investimento**

# Armadi da 15KW e più



# Armadi da 15KW e più

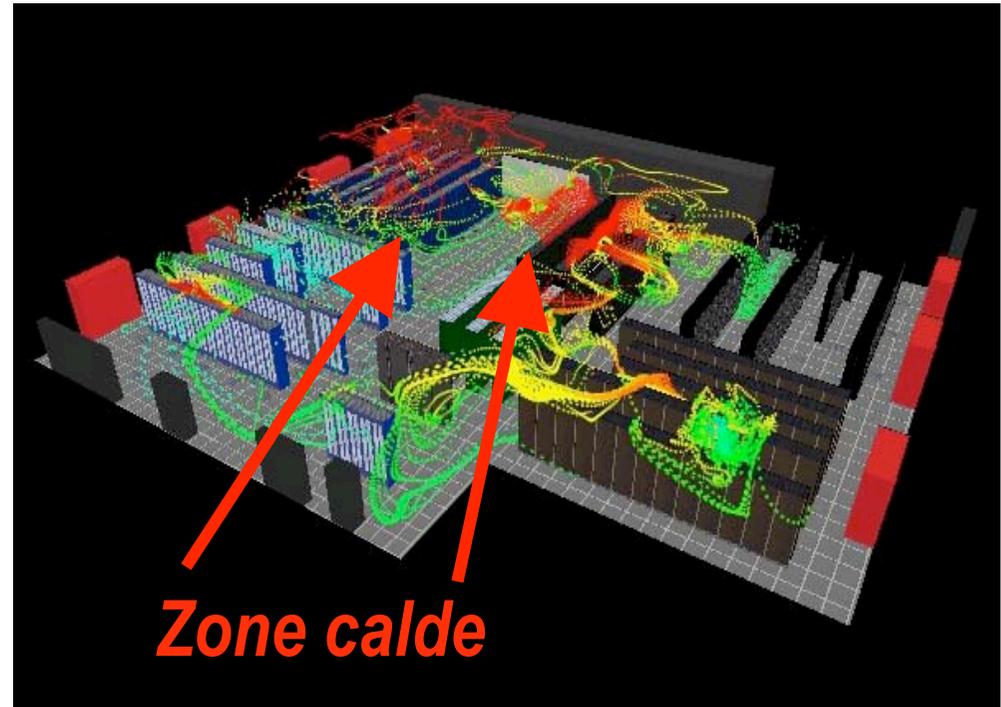


*90% dei CED attuali può gestire densità fino a 4KW per rack max.  
I rack ad Alta Densità hanno bisogno di 8-15KW ...o più!*

# Problema 1: raffreddare i rack ad alta densità



- La potenza assorbita è totalmente dissipata in calore
- Gli switch possono assorbire 8.5KW o più
- In un solo rack si possono inserire fino a 11KW di server 1U e 15KW di blade server
- Ma i CED attuali progettati anni fa sono dimensionati per 1.5KW per rack ...



***... il raffreddamento tradizionale non basta in un CED ad Alta densità !***

# I CED evolvono: quali rischi per la BC ?

---



- Problema 1: Aumento della potenza per singolo rack con server a tecnologia blade rende necessario il raffreddamento ad alta densità
- **Problema 2: Modularità e flessibilità dell'investimento**

# Quanto costa un CED non modulare ?



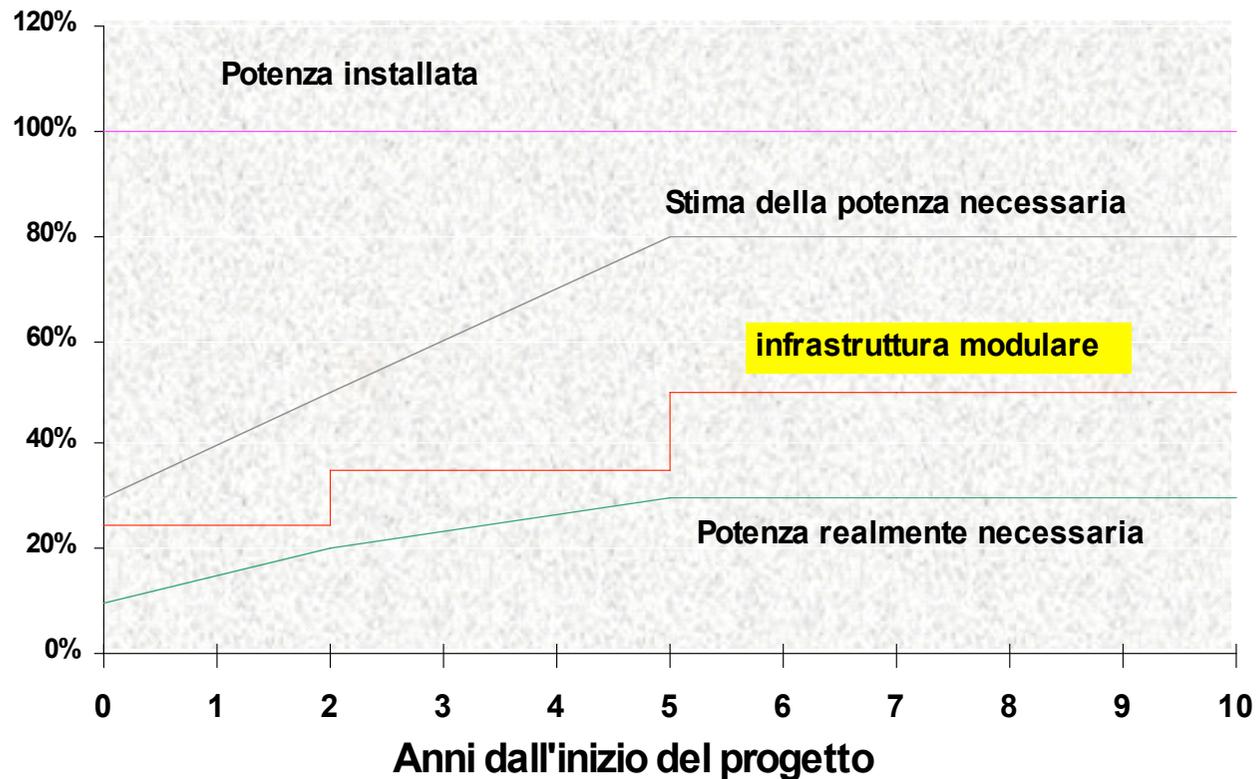
I CED tradizionali sono stati progettati per il massimo della capacità.  
Mediamente i CED utilizzano il 30% della potenza elettrica installata



# Quanto conviene un CED modulare ?



Progettando un CED “on-demand” si utilizza solo l’infrastruttura necessaria, garantendo la Business Continuity ottimizzando gli investimenti





- **Garantire la continuità operativa realizzando un SI ad Alta Disponibilità grazie ad una infrastruttura per CED “on-demand”**

# APC - Global, End-to-End, Nonstop Networking™



## ■ La Visione

La **Business Continuity** è la *conditio sine qua non* per qualsiasi azienda per stare nel mercato

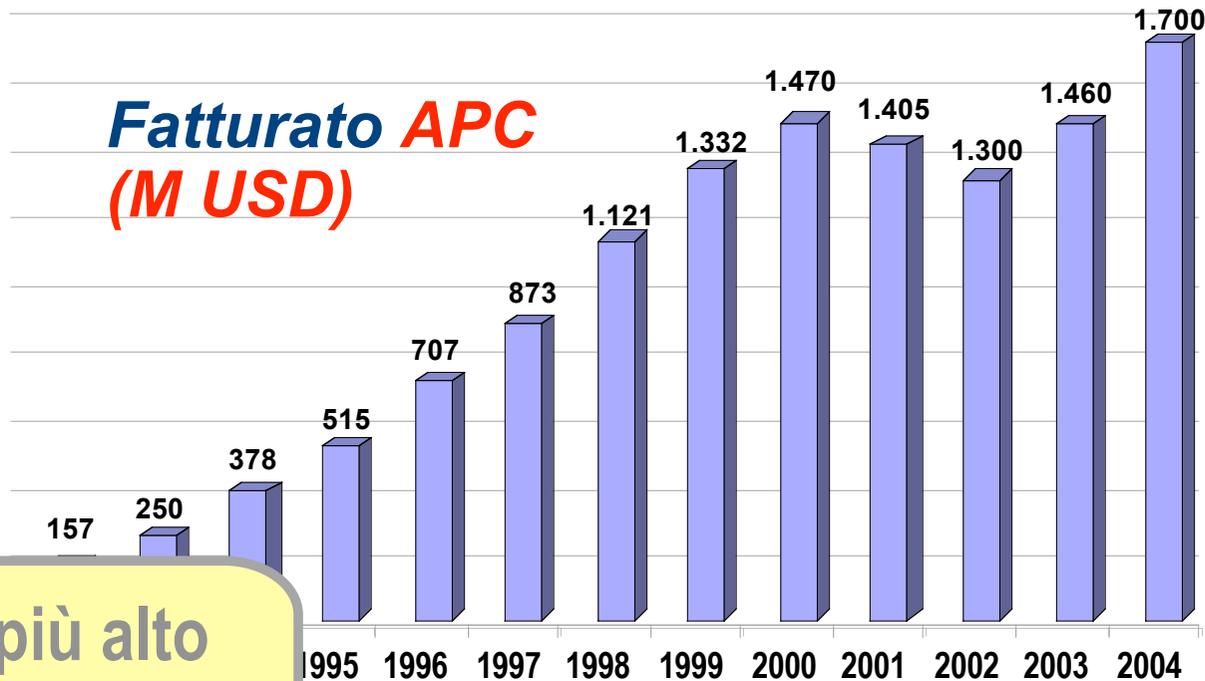
## ■ La Missione

Garantire a tutti i nostri clienti la **Business Continuity** aumentando la gestibilità, la disponibilità e le prestazioni dei Sistemi Informativi grazie a soluzioni innovative e di rapida implementazione

# Una tradizione di Innovazione



**Fatturato APC**  
**(M USD)**



Il più alto  
Budget  
R&S del  
settore

Utile Netto: **\$181.5M**

Debito: **\$0**

**Spesa R&S: \$120M nel 2005**



Forbes Platinum 400  
"Best Big Companies"



S&P 500



#755 on Fortune 1000



"Most customer-centric  
companies"



"Most innovative users  
of technology"

ciscoexpo  
2005

**APC**  
Legendary Reliability™

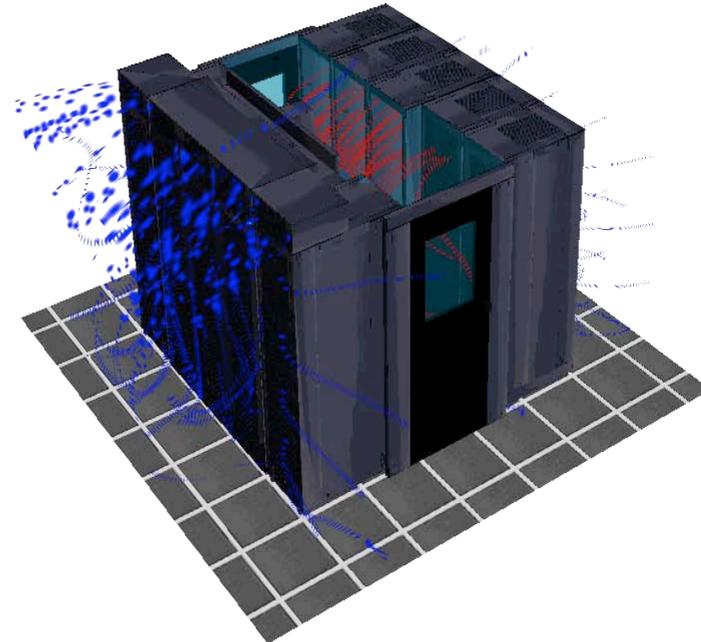
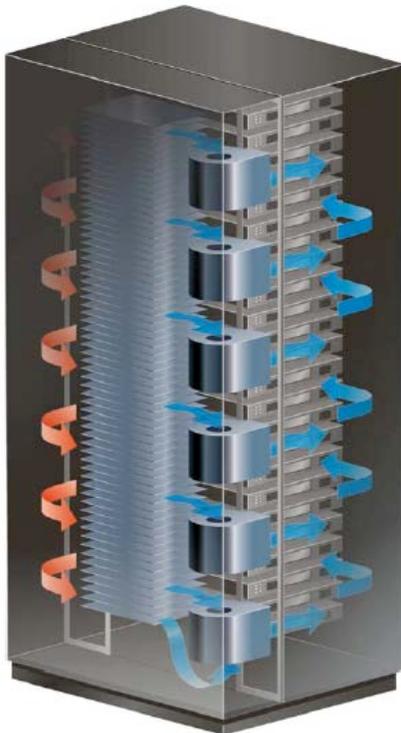
- UPS Symmetra Power Array™ modulare e Fault Tolerant fino a 1.6MW
- Armadi Netshelter™ 19 o 23", aperti o chiusi, da 25U a 47U
- Sistema di cablaggio dati e alimentazione sopra gli armadi
- Sistemi di distribuzione alimentazione centrale e a livello rack, modulari e gestibili
- Sistema di condizionamento di precisione dal singolo armadio all'intero CED con gestione "hot-spot" fino a 20KW per rack

# Raffrescamento per Alta Densità



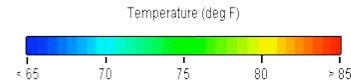
## Singolo rack raffrescato

- Rack sigillato con sistema A/C
- Può raffrescare **fino a 18KW**
- Scalabile, Flessibile, Riposizionabile



## “InfrastruXure High Density”

- CED sigillato ad Alta Densità
- **Fino a 20KW** in ogni singolo rack
- Può essere inserito in un CED a bassa densità per applicazioni ad alta densità senza dovere riprogettare il CED
- Scalabile, Gestibile, Alta Disponibilità



- Sistema di allarmi **accesso, fumi, gas, incendio, liquidi ecc.**
- SW di gestione **basato su IP con GUI HTML ed integrato con NMS (HP Openview, Tivoli, Unicenter, ecc.) e Building Management Systems**
- **Remote Monitoring System 7x24**
- **CED interamente progettato da APC**
- **Pre-testato e assemblato in fabbrica, consegnato ed installato in breve tempo**
- **Soluzione "chiavi in mano" incluse opere edilizie**

# Concludiamo

---



- **La sicurezza dei sistemi non può prescindere dalla disponibilità degli stessi**
- **Per garantire l'Alta Disponibilità dei sistemi IT occorre garantire una solida base infrastrutturale**
- **L'infrastruttura deve avere precise caratteristiche di modularità, espandibilità, ridondanza, velocità di implementazione, gestibilità e manutenibilità**
- **APC InfraStruXure è l'architettura "on-demand" per l'infrastruttura IT e costituisce le fondamenta di un SI ad Alta Disponibilità**

# Best Practice

---



**Visitate con noi i CED  
realizzati da APC**

*[www.apc.com/it](http://www.apc.com/it)*

*[Massimo.Galbiati@apcc.com](mailto:Massimo.Galbiati@apcc.com)*