INTRODUZIONE al BYOD

Stefano MARRONE

Contenuti

- BYOD: cos'è e perché oggi è rilevante
- Come affrontarlo nella realtà
- Il progetto di una soluzione BYOD
- L'aspetto tecnologico del BYOD
- CONCLUSIONI

Cosa significa “BYOD”?

- Bring Your Own Device
- In senso stretto:

  BYOD identifica la possibilità di consentire l’accesso ai dati, ai servizi e alle applicazioni di una specifica organizzazione da dispositivi non di sua proprietà

- In senso più generale:

  BYOD è l’etichetta che oggi si dà al problema di come consentire l’accesso ai dati, ai servizi e alle applicazioni dell’organizzazione mediante PC e/o dispositivi atipici, come tablet e smartphone, non sotto il controllo dell’ICT aziendale o non di proprietà

Tanti altri acronimi, stesso problema

- COPE
  - Company Owned, Personally Enabled
- BYOC
  - Bring Your Own Cloud
- BYOT
  - Bring Your Own Technolo
- BYOA
  - Bring Your Own App

Scenari più comuni 1/2

1. Accesso ai servizi, come la posta elettronica, da dispositivi personali o, in ogni caso, non dell'istituto (es. di dipendenti o consulenti)
2. Accesso alle applicazioni istituzionali da dispositivi personali o non
   (es. di dipendenti, collaboratori o consulenti)
3. Uso di PC personali per l'accesso remoto a servizi e applicazioni istituzionali (es. home working);

Scenari più comuni 2/2

4. Accesso autorizzato e sicuro alla rete istituzionale, Wi-Fi o cablata, da parte di personale esterno
   (es. dipendenti con dispositivi propri; collaboratori, consulenti o ospiti con i propri dispositivi)
5. Accesso sicuro da uffici e postazioni non direttamente connessi con la rete scolastica e non controllati dall'istituto (es. da parte di partner, collaboratori, fornitori, clienti che accedono da remoto)

Alcuni tra i possibili approcci 1/2

- Approccio n. 1

  «Non sono ammessi dispositivi non scolastici»

- Approccio n. 2

  «Sono ammessi solo dispositivi certificati»

- Approccio n. 3

  «I dispositivi non scolastici potranno essere usati solo per accedere alla posta elettronica»

Alcuni tra i possibili approcci 2/2

- Approccio n. 4

  «I dispositivi sono utilizzabili solo se il dipendente accetta l'uso degli strumenti di gestione istituzionali»

- Approccio n. 5

  «Prima di poter usare dispositivi mobili non istituzionali, occorre definirne le politiche di utilizzo»

- Approccio n. … VARI ed EVENTUALI

LA SFIDA

- Avere una rete molto:
  - Efficiente;
  - Sicura sia all'interno che all'esterno;
  - Efficace piena di contenuti e che sia predisposta a riceverne molti altri.

L’approccio "completo" 1/2

- Definire gli ambiti d’uso dei dispositivi mobili
- Definire i limiti e le modalità di utilizzo dei dispositivi mobili non istituzionali (o istituzionali, quando abilitati anche all’uso personale)
- Definire le responsabilità della scuola e quelle personali nell’uso dei dispositivi
  - La disciplina deve essere necessariamente diversa nei casi di BYOD e di COPE

L’approccio "completo" 2/2

- Definire i servizi, le applicazioni e i dati che devono essere accessibili dai dispositivi
- Fare un’analisi dei rischi dell’adozione del BYOD
- Definire l’infrastruttura tecnologica necessaria
- Definire le misure di sicurezza da adottare
- Definire le politiche di licensing più appropriate
- Definire i sistemi di monitoraggio, di gestione e di supporto

Le "componenti" da considerare

- Economica
- Organizzativa
- Tecnica
- Licensing
- Legale
- Sicurezza

La “componente” economica

- Una soluzione BYOD può richiedere:
  - Investimenti in infrastruttura
  - Contributi all’acquisto dei dispositivi
  - Contributi alle spese inerenti l’uso dei dispositivi
  - Costi legati alle licenze
  - Costi legati alla gestione
  - Costi legati al supporto
  - Costi organizzativi vari

La “componente” organizzativa

- Selezione dei dispositivi consentiti
- Definizione di un disciplinare di utilizzo
- Definizione dei referenti interni per la gestione dei dispositivi non istituzionali
- Processi di gestione appropriati per i dispositivi
  - Richiesta/autorizzazione all’utilizzo
  - Denuncia di furto/smarrimento
  - …
- Approntamento delle strutture di supporto

La “componente” tecnica

- Le richieste BYOD possono coprire un ampio ventaglio di esigenze e, di conseguenza, richiedere diverse soluzioni di tipo tecnico
  - Infrastruttura (rete, server, servizi, connettività)
  - Piattaforma (virtual desktop e applicazioni)
  - Applicazioni (generiche, dedicate)
  - Sicurezza → *vedere dettaglio successivo*
  - Dispositivi (PC, tablet, smartphone)

La “componente” relativa al licensing

- Il licensing dei servizi e delle applicazioni usate dai dispositivi deve prevedere:
  - L’accesso da dispositivi primari e “companion”
  - L’accesso da dispositivi di proprietà e non
- Ogni elemento coinvolto deve essere correttamente licenziato
  - Server e applicativi scolastici
  - Utenti
  - Dispositivi

La “componente” legale

- Definizione delle responsabilità
  - Relativamente all’uso del dispositivo
  - Relativamente ai dati personali sul dispositivo
  - Relativamente ai dati aziendali sul dispositivo
  - Relativamente alle normative rilevanti (D.Lgs 196/2003; D.Lgs 231/2001, altre)
- Definizione delle modalità di accettazione, da parte degli interessati, delle regole di utilizzo dei dispositivi, aziendali e non

La sicurezza: Infrastruttura

- Protezione da accessi non autorizzati
- Segregazione del traffico di rete
- Riduzione della superficie di attacco di sistemi e apparati di rete
- Rilevamento dei tentativi di intrusione
- Monitoraggio degli account e dei dispositivi
- Imposizione e rispetto forzato delle scadenze
  - Account/dispositivi; sessioni di lavoro…
- Sistemi di audit

La sicurezza: Dati & Applicazioni

- Pubblicazione delle applicazioni
  - Diretta (es. app locale con Web Services, browser)
  - Indiretta (es. accesso tramite desktop virtuale)
- Definizione dei profili di utilizzo consentiti
  - Accesso locale (collegamento alla rete aziendale)
  - Accesso remoto (collegamento tramite Internet)
- Distinzione tra dati personali e dati aziendali
  - Definizione e uso dei profili utente
- Politiche di “Data Loss Prevention”

La sicurezza: Dispositivi utente

- Riconoscimento dei dispositivi autorizzati
  - Autenticazione dispositivo
  - Connessione sicura alla rete aziendale
- Verifica di conformità dei dispositivi alle policy aziendali definite
  - Accesso root, sblocco privilegi (es. jailbreak)
  - Cifratura dei dati memorizzati localmente
  - Antivirus/antimalware
- Controllo sulle app installate
  - Black/White list delle app consentite

La fase progettuale

1. Definire requisiti e obiettivi della soluzione
2. Definire le componenti della soluzione
3. Definire l'High Level Design della soluzione
   - Infrastruttura on premise
   - Cloud
4. Definire e indirizzare tutte le questioni non tecniche della soluzione ipotizzata
5. Implementare la soluzione individuata
6. Test
7. Deployment
8. Esercizio e supporto

Requisiti e obiettivi

- In questa fase verrà definito l'ambito della soluzione e i risultati che si desidera raggiungere
  - Obiettivi e requisiti di business
  - Vincoli di sicurezza e tecnologici
- In base all'ambito individuato, sarà possibile determinare l'architettura di riferimento della soluzione BYOD da implementare
- L'architettura scelta permetterà poi di individuare i componenti tecnologici

L’architettura tecnologica

- Infrastruttura di rete
- Servizi di Directory
- Public Key Infrastructure
- Servizi di virtualizzazione
  - Desktop
  - Sessioni
  - Applicazioni
- Piattaforma applicativa
- Storage condiviso
- Sistemi di supporto
- Strumenti di monitoraggio
- Strumenti di gestione (MDM)
- Distribuzione delle applicazioni (MAM)
- Strumenti di protezione
  - Locale
  - Perimetrale
  - Dei dati

Soluzioni tecnologiche: Network

- Sistema di autenticazione
  - Es. Active Directory; PKI, RADIUS
- Sistema di controllo degli accessi LAN
  - Es. NAC o NAP; IEEE 802.1x, WCS
- Sistema di controllo degli accessi WAN
  - Es. UAG, AnyConnect, OpenVPN

Soluzioni tecnologiche: Piattaforma

- Sistemi di virtualizzazione
  - Hypervisor: Hyper-V, ESXi; XenServer
  - Sessione: RDS; XenApp
  - Desktop: RDS; View; XenDesktop
- Pubblicazione delle applicazioni
  - Applicazioni: RDS; XenApp; Horizon
  - Web: IIS; Apache; Web Services
- Condivisione dello storage
  - Interna: SkyDrive Pro; AppSense; Horizon
  - Cloud: SkyDrive Pro; SkyDrive; Dropbox Spider Oak; Google Drive

Componenti: Sicurezza

- Mobile Device Management (MDM) & Mobile Application Management (MAM)
  - Prodotti dedicati
    - AirWatch; SmartMan; MobileIron; Zenprise
  - Suite dei vendor più importanti
    - Microsoft; IBM; Symantec; Sybase; Citrix; VMware
  - Soluzioni Cloud
    - Microsoft; AirWatch
- Antivirus/antimalware
  - Es. Symantec; Kaspersky; ESET; McAfee; F-Secure

Licensing, questioni legali, eccetera

- Oltre a un'architettura tecnologica, ogni soluzione BYOD deve prevedere:
  - Un disciplinare interno di utilizzo dei dispositivi
  - La definizione delle responsabilità interne
  - La definizione delle responsabilità dell'utente
  - L'identificazione delle licenze necessarie a sostenere la soluzione BYOD scelta
  - Le procedure di gestione e di supporto

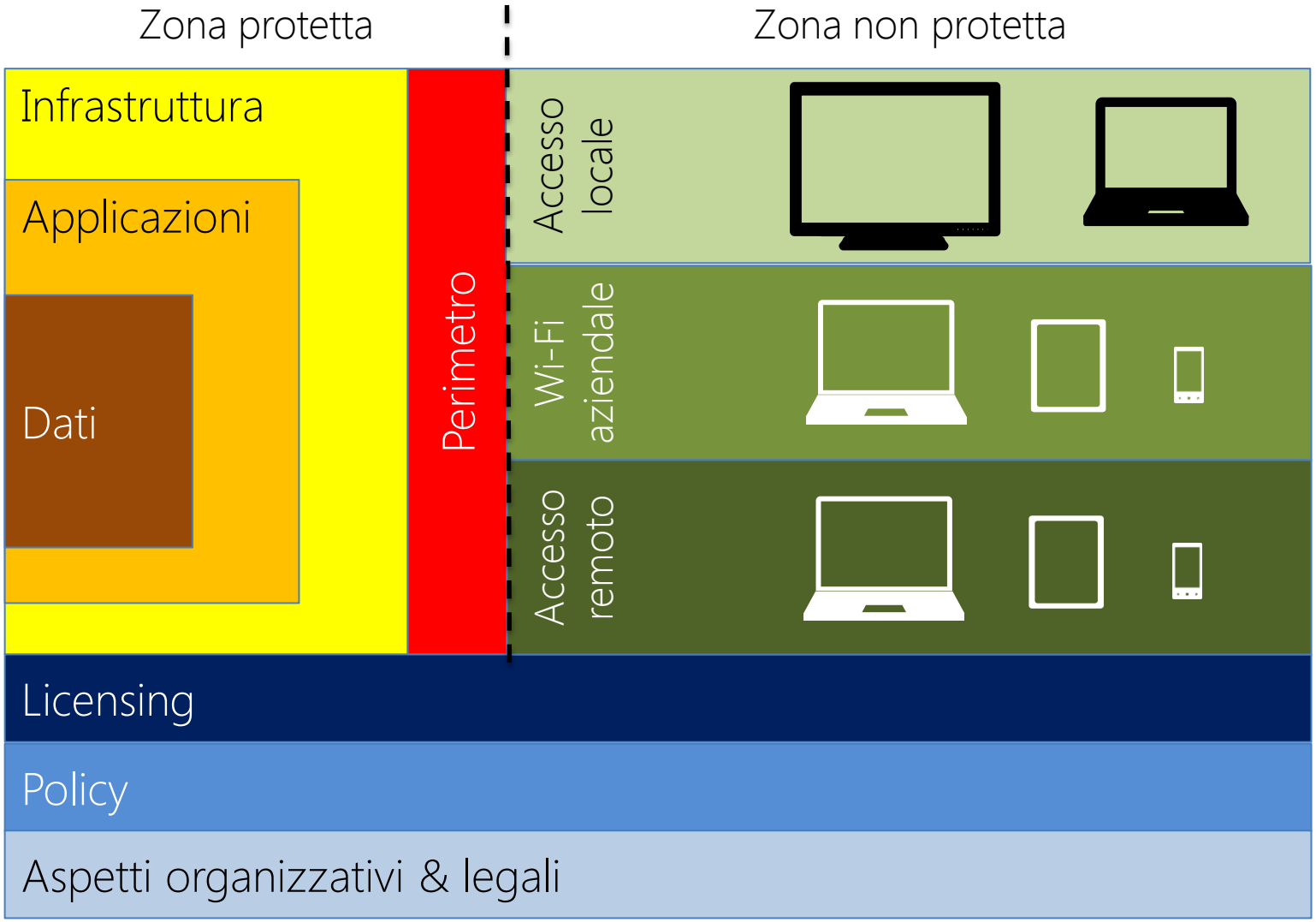
Le fasi realizzative della soluzione

- Implementazione
- Test
- Deployment
- Esercizio
- Supporto

Il Team byod

- Specialisti di problematiche organizzative
- Specialisti di problematiche di sicurezza
- Specialisti di problematiche economiche
- Specialisti di problematiche legali
- Specialisti di problematiche tecniche
- Specialisti di problematiche legate al licensing

“Concept” di una soluzione BYOD



La metodologia di progetto 1/3

- La metodologia elaborata dal Team byod considera e definisce i seguenti elementi:
  - le fasi di progetto
  - i deliverables
  - i ruoli necessari
- Nello staff di progetto sono sempre previsti:
  - persone dell'organizzazione cliente
  - specialisti del Team byod

La metodologia di progetto 2/3

- Fasi:
  1. Vision
  2. Scope
  3. Pianificazione
  4. Sviluppo
  5. Test
  6. Roll out

La metodologia di progetto 3/3

- Ruoli & Deliverables

Ruolo	Figure del team BYOD	Figure del team del cliente
MNGMT	*Project Manager*	*Program Manager*
COORD	*Project Coordinator*	*Logistic Manager*
DEVEL	*Specialist*	*Area Relationship Manager*
BUILD	*Specialist*	*ICT Relationship Manager* *Business Relationship Manager*

Tipo	Fasi coinvolte	Titolo Documento	Propedeutico a	Azione successiva
Feasibility	*1. VISION*	*Documento di Vision*		
	2. SCOPE	*Documento di Scope*	Approvazione	Pianificazione attività
Preparation	*3. PLAN*	*Piano del Progetto*	Avvio attività	Esecuzione attività
	4. DEV	*Documento di Design*		
	5. TEST	*Protocollo di Test*	Progetto pilota	Fase realizzativa
Roll out	*6. ROLL OUT*	*Piano di Roll out*	Implementazione	Avvio in produzione

I servizi del Team byod

- **Servizi di consulenza (Consulting Services)**
  - Studio di fattibilità
  - Analisi di giustificazione economica
  - Analisi dei rischi
  - Analisi dell’impatto organizzativo
  - Analisi del licensing BYOD necessario

I servizi del Team byod

- **Servizi di progetto (Design Services)**
  - Design dell'infrastruttura necessaria per il BYOD
  - Design della soluzione di gestione per il BYOD
  - Design del servizio di supporto per il BYOD
  - Security design
- **Servizi di implementazione (Delivery Services)**
  - Sviluppo e realizzazione del progetto BYOD

I servizi del Team byod 3/4

- **Servizi di formazione (Education Services)**:
  - Addestramento alla problematica di Network;
  - Workshop:
    - Panoramica su BYOD (quello di oggi…)
    - Focus sulla sicurezza
    - Focus sulle problematiche legali
    - Focus sul licensing
    - Tavola rotonda con gli esperti
  - Eventi:
    - BYOD Conference

I servizi del Team byod 4/4

- **Servizi specifici (Custom Services)**
  - In quest'area ricadono le attività che non si possano inquadrare nei servizi più generali elencati sopra oppure che siano di portata più limitata e, quindi, possano essere erogati senza adottare la metodologia BYOD. Esempi:
    - Stesura della policy per l'adozione del BYOD
    - Assessment della situazione esistente
    - Analisi dell'impatto del BYOD su normative specifiche (es. D.Lgs 196/2003, D.Lgs 231/2001)