



MOVILIDAD SEGURA Y SIMPLE EN EL SECTOR PÚBLICO

Jorge Villarreal
Post Sales Service Manager
Enterasys México & NOLA



3 de Septiembre 2013

- La importancia de la movilidad en las redes
- Imperativos de movilidad en sector público
- El BOOM de la movilidad : BYOD
- ¿Qué es BYOD?
- ¿Cuál es la importancia de BYOD?
- BYOD Incrementa la productividad
- Tendencias de BYOD en México
- La experiencia del usuario
- Necesidades y cómo las resolvemos
- ¿Como se hace BYOD correctamente?



La importancia de la movilidad en las redes

La nueva Realidad

Escalabilidad

- 3 dispositivos por usuario → 7 dispositivos por usuario en 2015
- Millones de dispositivos inteligentes entregando información rica y detallada que necesita más inteligencia para ser analizada
- Máquina –a-máquina

Acceso Inalámbrico Completo

- Alta densidad/Desempeño, confiabilidad y seguridad
- Durante 2015, 80% de los clientes tendrán que mejorar las WLANs que han sido implementadas recientemente



Convergencia de Red

- Voz, datos, video, virtualización en medio alámbrico/Inalámbrico
- Gran ancho de banda, muy baja latencia y optimización de flujos
- Colectar y almacenar en forma masiva información de TODO (Analytics)

TI Inteligente

- Industrias Inteligentes
- Requiere redes inteligentes → Proporcionar movilidad mientras se mantiene la administración simple



La importancia de la movilidad en las redes

Retos a los que se enfrenta el sector público

- Bajo la anterior perspectiva, no habrá ancho de banda que alcance ...
- Bajo la anterior perspectiva, los recursos humanos asociados a la operación de las redes estarán saturados modificando el comportamiento de las mismas a cada momento



La importancia de la movilidad en las redes

Lo que brinda la movilidad

- **Reconocimiento de automático de aplicaciones**
 - Asignación de QOS automático de acuerdo a su importancia
 - ¿ con cuales aplicaciones habla el usuario?
 - ¿ de que habla el usuario con esas aplicaciones?
- **Identificación automática de perfiles de usuario**
 - Independiente a su punto de acceso a la red
 - Independiente a la forma de acceso a la red
 - Considerando además: Teléfonos IP, Impresoras, cámaras, etc...
- **Asignación automática de políticas de uso aceptable de red (seguridad)**



Imperativos de movilidad en sector público

Focalizado en necesidades a nivel global

Dispositivos

Dispositivos
del empleado

Dispositivos
del
Corporativo

Dispositivos
de invitados

Dispositivos
con
cumplimiento

Dispositivos
utilizados por
usuarios en
casa

Ubicación

Dentro del
Corporativo

Dispositivos
usados en
casa

Redes
públicas

Sucursales

Aplicación

Aplicación
VDI

Aplicaciones
sociales

Aplicaciones
en la nube

Otras

Usuarios

Usuarios
Privilegiados

Empleados

Consultores

Contractors

Invitados

Otros



BYOD Done Right

- BYOD es el nombre que se le ha dado a la tendencia mundial en la que los empleados, visitantes, proveedores o cualquier otro tipo de usuario que se conecte a una red lo hagan con un dispositivo propio, en lugar de uno provisto por la misma empresa o controlado por el área de IT de la misma.
- BYOD ha existido desde hace mucho tiempo, sobre todo en las Universidades pero ahora con la proliferación de nuevos dispositivos como PDA's, Smart Phones, Tablets, Lap Tops, Unidades de Juegos, etc. su rol toma mayor importancia.



- Esta misma tendencia ha llegado a las empresas y cada vez hay mas usuarios con mas dispositivos esperando poder hacer su trabajo de una forma mas móvil y con el dispositivo de su elección.



- **Reducción de Costos para el sector público, al proveer acceso a aplicaciones internas y servicios externos como Internet, sin la inversión directa en hardware o software en equipos para usuarios finales**
- **Potencia nuevos estilos de trabajo:**
 - Nuevos esquemas de colaboración
 - Esquemas de nube
 - VDI (Infraestructura virtual de escritorios)



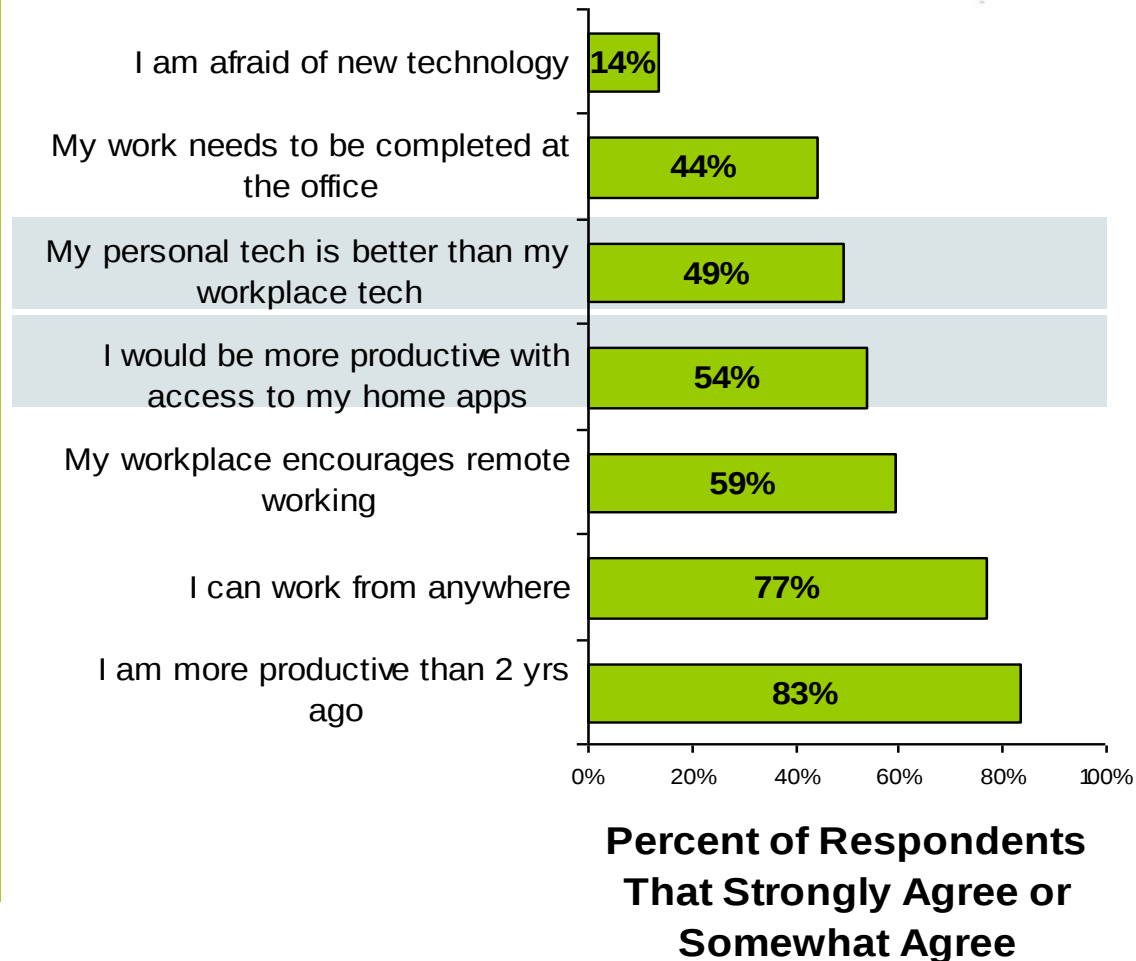
¿Cuál es la importancia de BYOD?

- Me gusta mi dispositivo móvil y me gusta trabajar con el
- El reto de ofrecer una red BYOD es cuando en los dispositivos propietarios se pretende tener acceso a datos o aplicaciones de negocio que puedan incrementar los riesgos de seguridad, confidencialidad o continuidad de negocio.



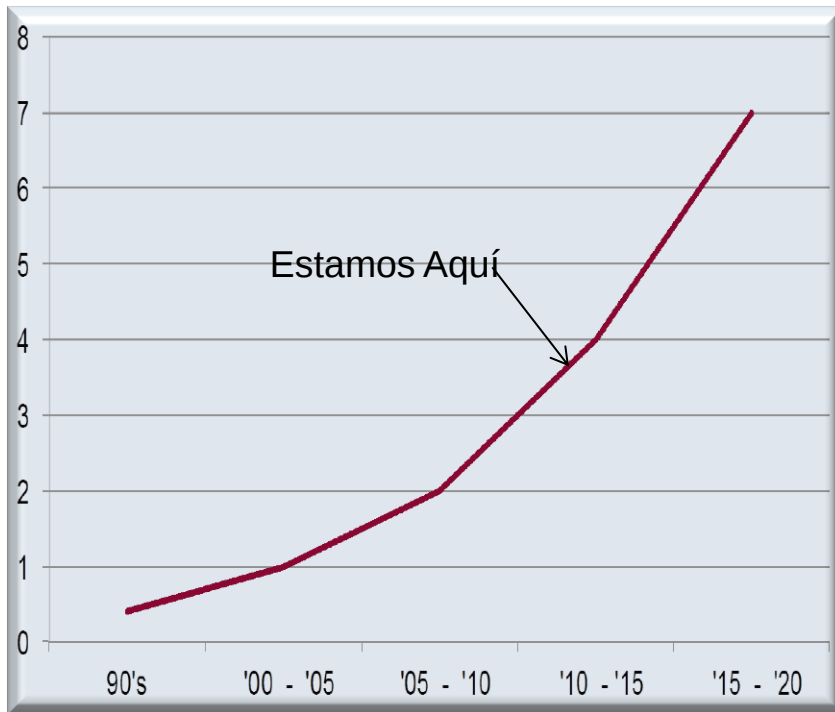
- En promedio, los empleados usan 4 herramientas de consumo en su día de trabajo
- Los empleados piensan que son más productivos a causa de BYOD
- Muchos usuarios piensan que los dispositivos propios son mejores que los dispositivos corporativos

In the context of workplace productivity, please rate your agreement with the following statements.



Survey of NA based corporate workers

- En los siguientes 4 años el mercado de wireless va a duplicarse, 81% de los empleados llevarán consigo al menos un dispositivo personal para hacer negocio y el 90% de las empresas no están totalmente conscientes de los dispositivos que acceden sus redes.

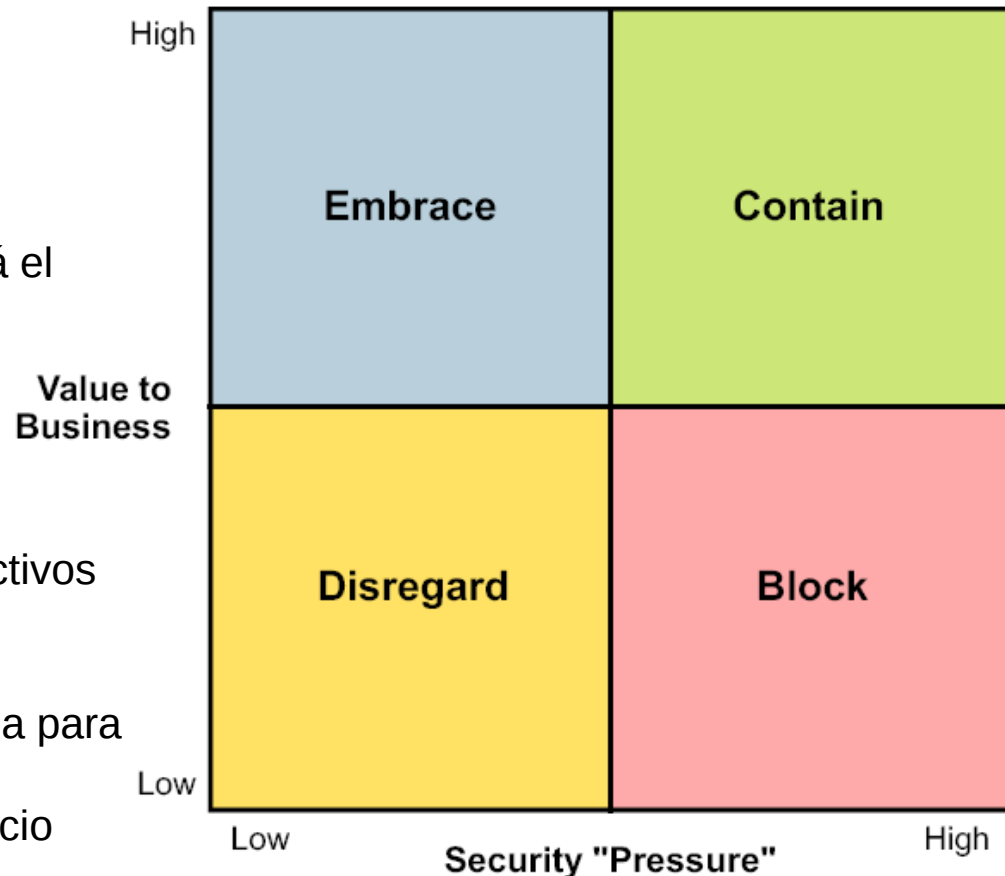


Número promedio de dispositivos propiedad de un solo usuario: 3



■ Gartner - Balanceando riesgo y valor de negocio

1. Desestimar BYOD
 - Casi imposible
2. Bloquear BYOD
 - Esto reducirá el riesgo pero limitará el potencial del negocio
3. Contener BYOD
 - Posiblemente el primer paso para muchos campus
 - Aislar de BYOD ciertos servicios/activos
4. Ceñirse a BYOD
 - Implementar la tecnología necesaria para administrar el riesgo
 - Alcanzar el potencial total del negocio



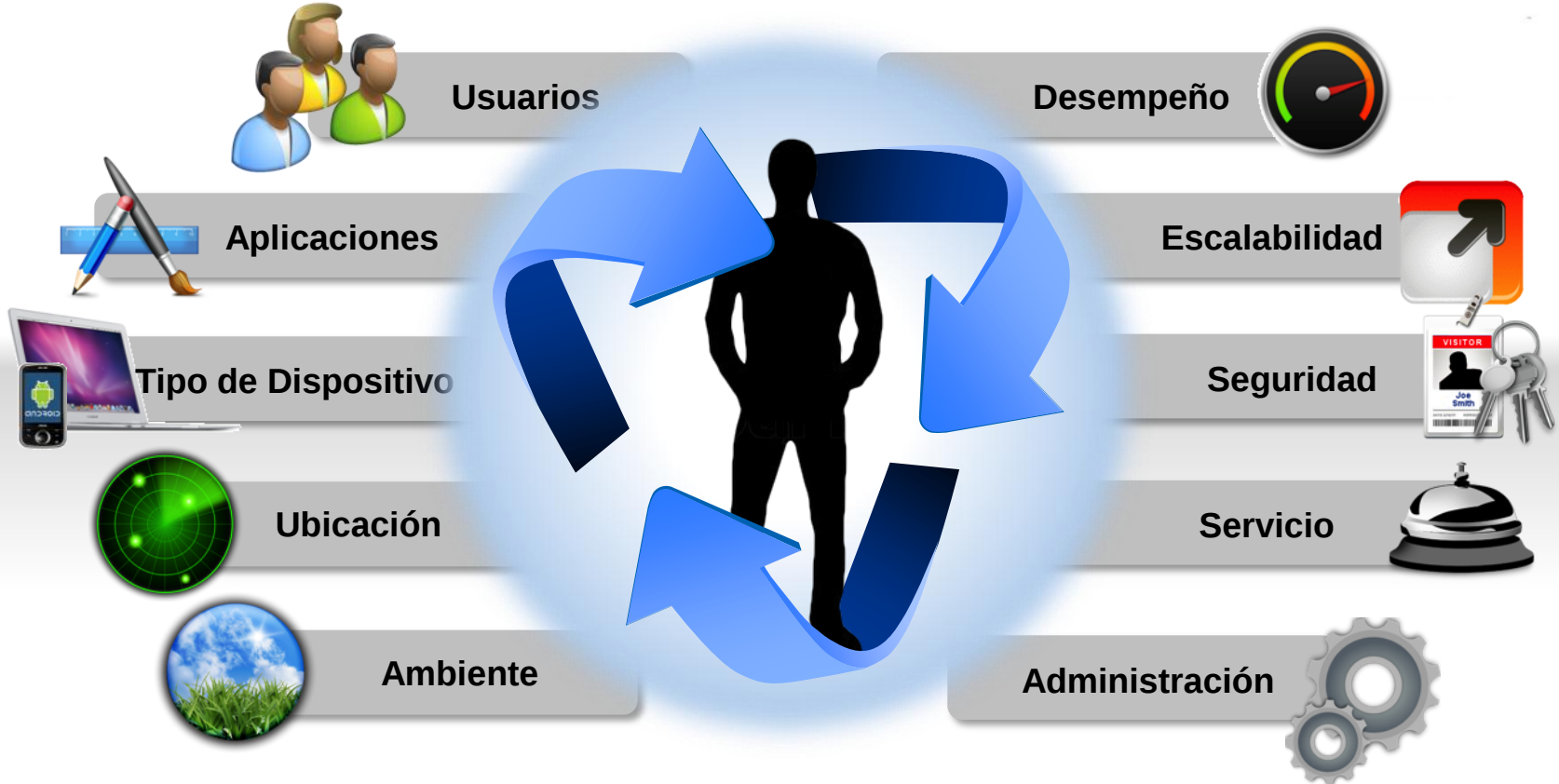
¿Como se hace BYOD correctamente?

- Una solución BYOD “Bien Hecha”, cubre BYOD tanto las redes inalámbricas como alámbricas haciéndolas funcionar como una sola red independiente del medio físico
- Lo haríamos sin segmentar la red y analizando hasta 50 atributos para definir una postura de conexión y de seguridad, dentro de los mas importantes están: Autenticación del usuario, tipo de dispositivo, sistema operativo, lugar y hora de conexión.
- Tradicionalmente, la segmentación ha sido la manera de proteger la red y diferenciar los accesos y privilegios por grupos de usuarios y dispositivos, iríamos mucho más allá de esta manera tradicional y limitada de dar acceso y seguridad por grupos
- No nos limitaríamos a que los dispositivos de red sean de una sola marca, a que BYOD sea aplicada únicamente en las redes inalámbricas o a que se haga por Vlan o SSID, podríamos implantar una solución BYOD para cada necesidad.



La experiencia del usuario

10 Factores claves



Necesidades y cómo las resolvemos

Usuarios que buscan tener los mismos niveles de acceso a la red desde su dispositivo móvil que desde los dispositivos que provee la empresa

BYOD de Enterasys permite el uso de los recursos de la red basándose en el perfil o rol del usuario y el dispositivo que está utilizando.

La necesidad del negocio de soportar soluciones BYOD sin impactos severos en costo y buscando un retorno de inversión

Un único appliance para trabajar sobre la infraestructura actual cableada e inalámbrica – reducción de la complejidad y de costos!!

Conocimientos y experiencia para poder implementar efectivamente soluciones BYOD

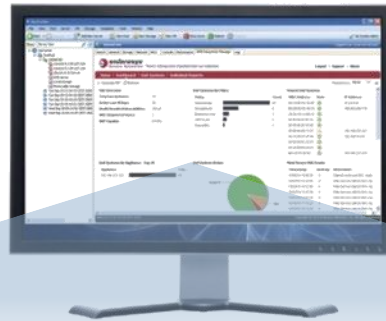
Instalación garantizada a través de integradores y con soporte directo del fabricante

Administración y resolución de problemas para la solución de BYOD

Consola de administración unificada (una sola para toda la red). Aplicación de políticas desde un solo punto para el acceso a aplicaciones, y aplicación de QoS para usuarios, dispositivos, servicios, etcétera.

¿Como? OneFabric

OneFabric™



OneFabric Control Center
(Unified security and management)



OneFabric Data Center



OneFabric Edge



OneFabric Security



Identificación total del “ciudadano digital”

Identidad – Joe Smith

Tipo de acceso?

Wireless
Associated AP: wifi-243
SSID: Prod-Guest
BSSID: 0-1a-e8-14-de-98

Identidad del dispositivo virtual?

Windows v7.5.3

Dispositivo?

Apple MacBook Air
Samsung Galaxy Note

Ubicación?

Building-A
Floor-2
Conference Room-7b

Tiempo del día?

Wednesday, April 11, 2012
9:41:00 AM EST

Uso de aplicaciones?

Web (HTTP): 5Mb download
Email (SMTP): 2Mb download
All other Services: DISABLED

Autenticación?

MAC-Auth: 28:37:37:19:17:e6
PWA: 00:00:f0:45:a2:b3
802.1X: 00:0D:3A:00:a2:f1

Identidad del dispositivo físico?

Apple Lion OSX v10.7
Android v4.0.4

Salud?

Symantec Anti-Virus: Enabled
Signature Update – v10.4.3
OS Patches – Up to date
Peer2Peer Service: DISABLED
43 Services Running

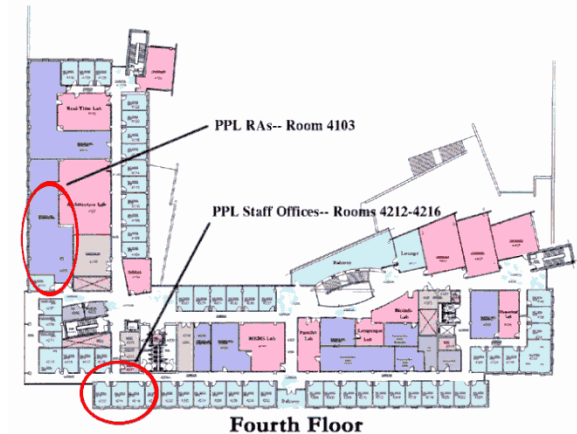
Autorización?

Role: Sponsored Guest
Sponsor: Jane Doe
Internet Access
Shared Engineering Servers



■ Acceso controlado dependiendo del usuario, localización, dispositivo, aplicación

- Ancho de banda alto para VDI a directores
- Ancho de banda alto para video a directores
- Acceso a información confidencial unicamente a directores
- Aprovisionamiento Automatico para visitantes y consultores
- Ancho de banda controlado para visitantes
- Acceso de alta prioridad para dispositivos denominados críticos



■ Localización y reporte por usuario, dispositivo, localidad

- Cumplimiento de regulaciones

■ Único y simple visor para control por parte de TI

- Capacidad de escalar sin necesidad de agregar mas recursos (HW o SW)

Controladoras Inalámbricas

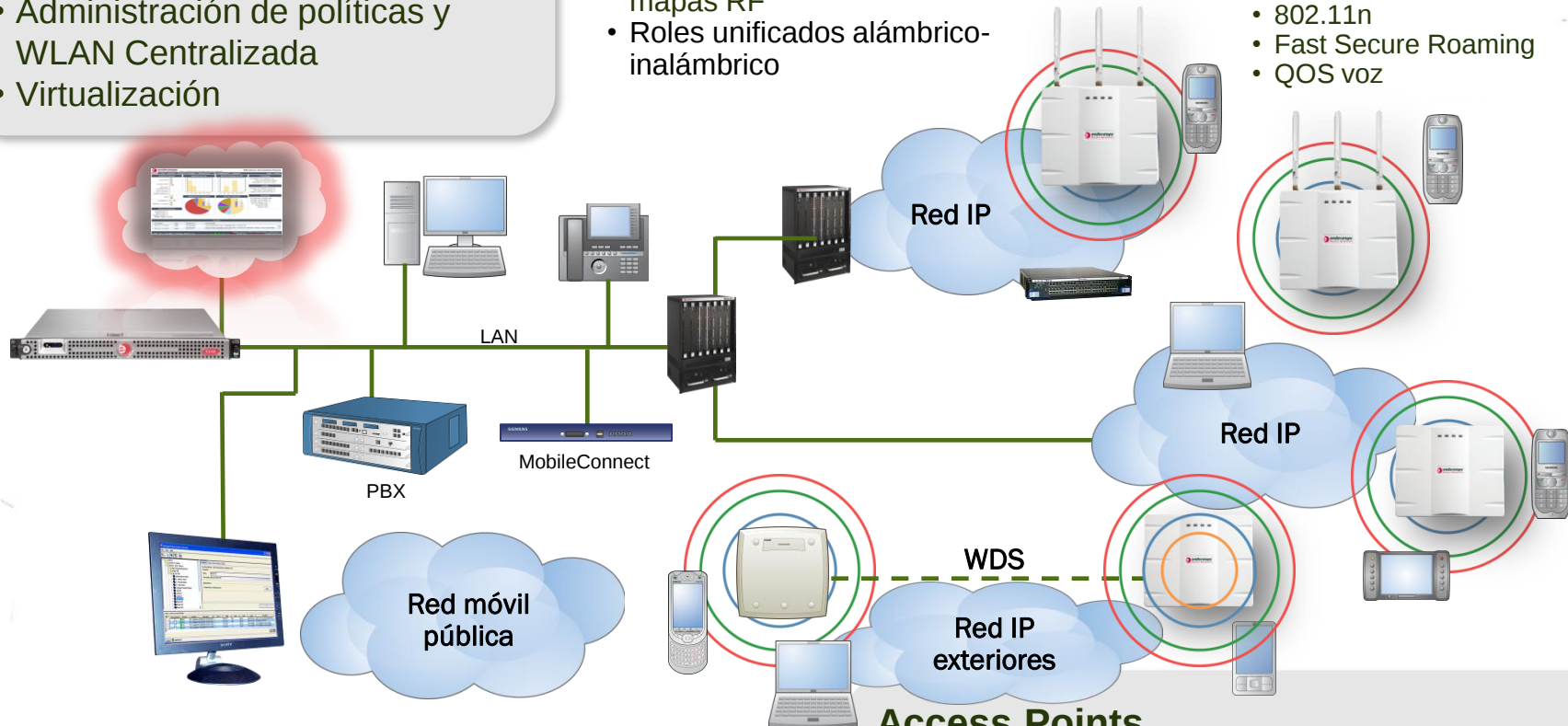
- HA/Redundancia
- Administración de políticas y WLAN Centralizada
- Virtualización

Administración Unificada

- Administración Multi-controladora
- Wireless IPS, "Location services", mapas RF
- Roles unificados alámbrico-inalámbrico

Clientes Móviles

- 802.11n
- Fast Secure Roaming
- QoS voz



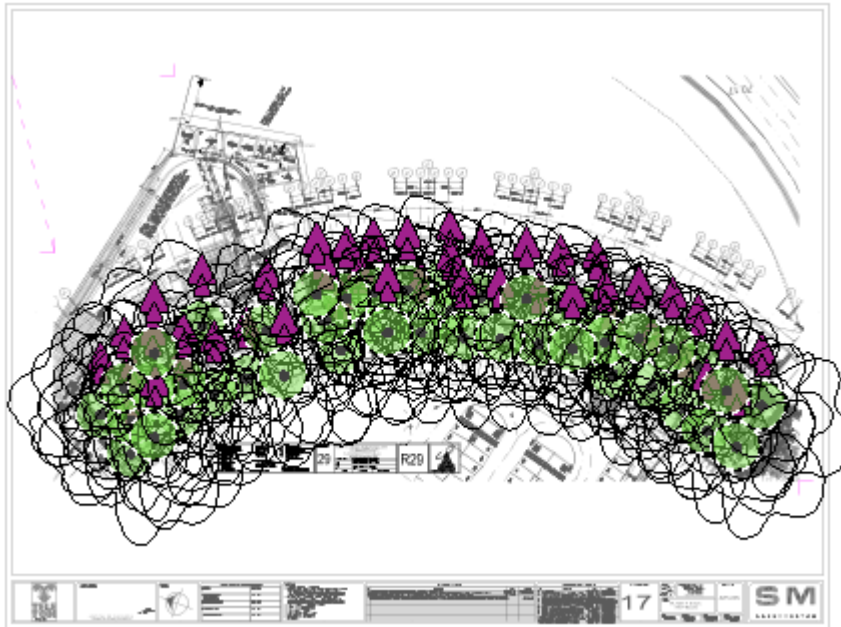
Capacidades "Enterprise-class"

- 802.11n , 3X3 MIMO ,802.3af PoE
- Políticas locales en AP's y rate limiting
- 802.11an: 228 Mbps (channel bonded)
- 802.11bgn: 190 Mbps (channel bonded)

Access Points

- Multi-SSID
- WPA, WPA2, WEP + encriptación/authenticación
- Balanceo de cargas y auto-failover
- Dynamic Frequency Selection, Radio Management, Airtime Fairness
- FCC and ETSI Dynamic Frequency Selection (permite uso completo 5 GHz)

- Mismo edificio, dos diseños



Diseñando por desempeño

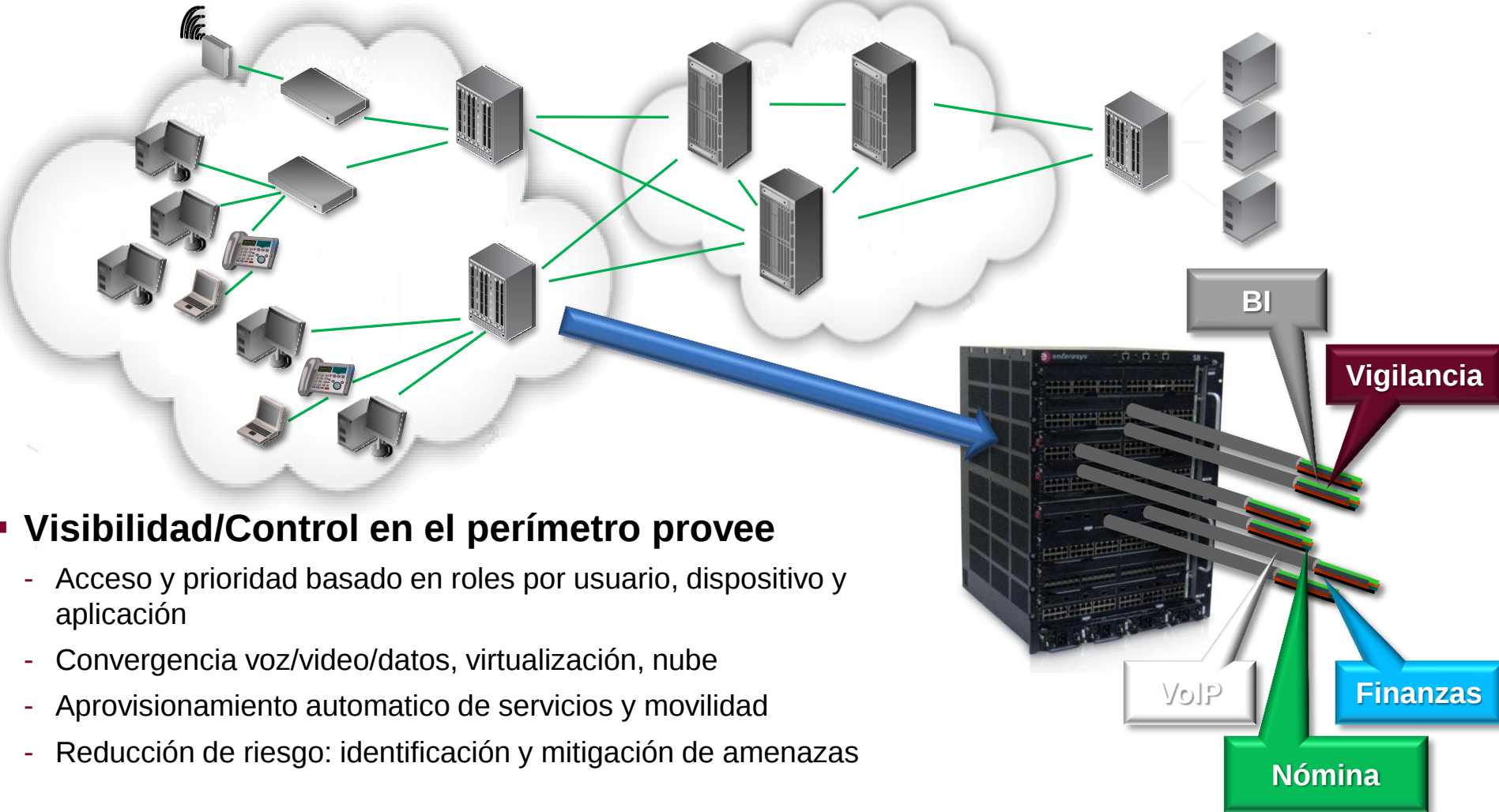


Diseñando por cobertura

Acceso

Distribución/Core

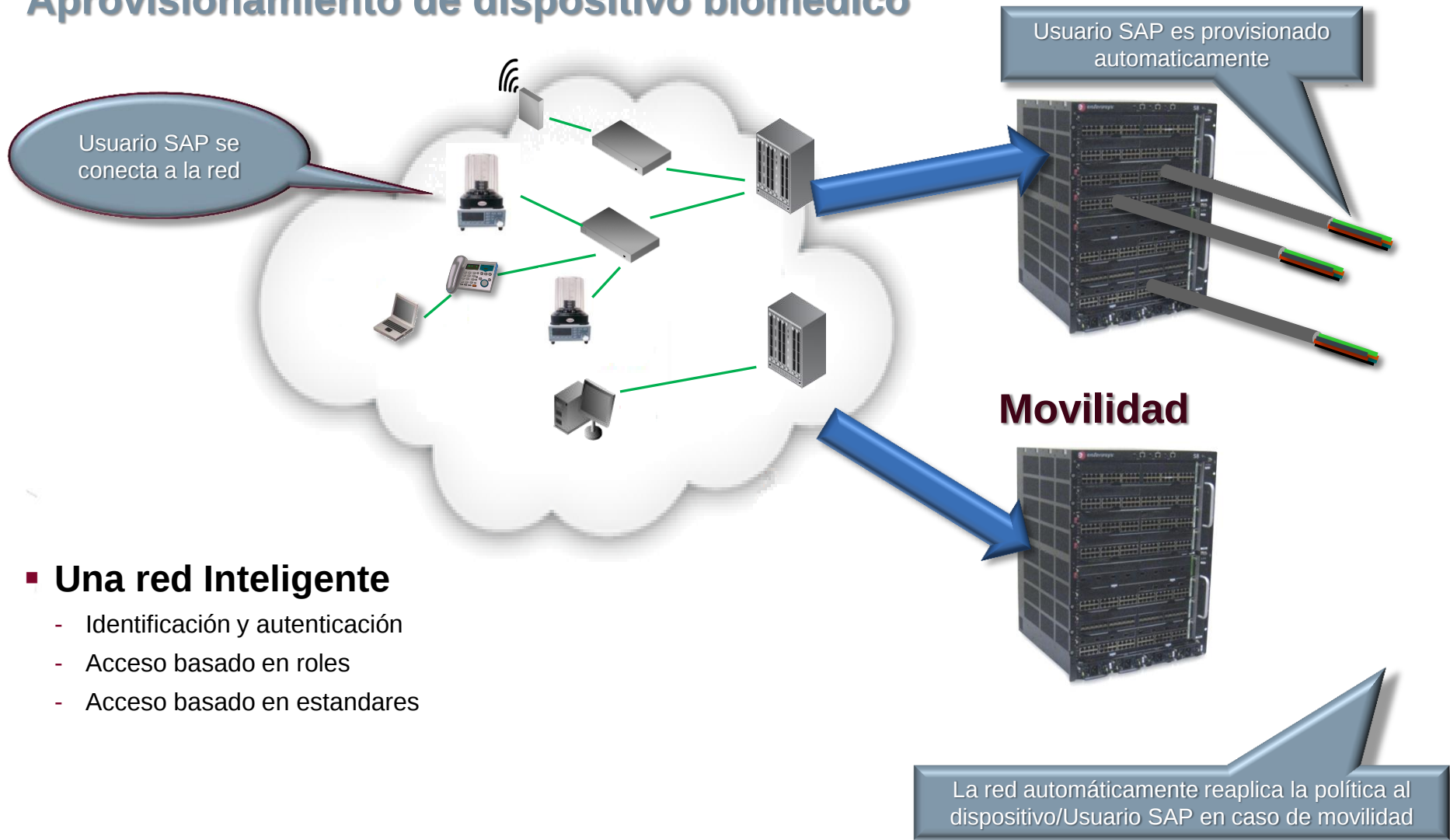
Data Center



■ Visibilidad/Control en el perímetro provee

- Acceso y prioridad basado en roles por usuario, dispositivo y aplicación
- Convergencia voz/video/datos, virtualización, nube
- Aprovisionamiento automático de servicios y movilidad
- Reducción de riesgo: identificación y mitigación de amenazas

Aprovisionamiento de dispositivo biomédico



■ Una red Inteligente

- Identificación y autenticación
- Acceso basado en roles
- Acceso basado en estándares

Política BYOD

- **Responsabilidades del usuario**
- **Responsabilidades de soporte de TI**
- **Política de configuración segura**
 - Controles de acceso
 - Acceso WiFi
 - Acceso a información personal
 - Detección y prevención de fugas de información
 - Respaldo y recuperación



BYOD otros requerimientos

■ Registro de acceso

- Portal de auto servicio con acceso a herramientas, formas de servicio y aceptación de política de uso de la red

■ Regulación de acceso a WiFi

- Reglas y políticas en torno a los recursos permitidos y el acceso a internet

■ Política Técnica

- Segregación de datos y tecnología aprobada



Controles de Seguridad

- **Control de Acceso básico**
 - Passwords fuertes y “security type”
 - Encripción & autenticación
 - Políticas en el acceso
- **Controles de acceso a aplicaciones Web, e-mail**
- **Acceso a recursos internos por WiFi**
 - Basados en localización, dispositivos, usuarios



Segmentación de información

- **Proveer políticas explícitas en relación al acceso de información personal**
 - Monitorear aplicaciones instaladas
 - Distribución de aplicaciones
 - Valuación de postura de seguridad



Cumplimiento y reporte

- Estado de dispositivos y que controles de seguridad han sido aplicados
- Intentos de acceso despues que a un dispositivo le ha sido negado el acceso a la red
- Detección de fugas de información
 - Malware
 - Correo electrónico
- Administración de parches
- Dispositivos no soportados





“There is nothing more important than our customers”

! Gracias !