Universitat Oberta de Catalunya

Presentació

Infraestructura hiperconvergent en la industria farmacèutica

13 de junio de 2023

Alumne: Adrian José Antón Gonzalvez

Tutor: Mireia Puig Verge

Universitat Oberta de Catalunya

Índex

Revisió abast del projecte

1. Anàlisi I estudi tecnològic
2. Estàndard de connectivitat de xarxa
3. Infraestructura hiperconvergent
4. Sistema de backup immutable

Arquitectura de xarxa i ciberseguretat

Objectiu i resultats esperats

1. Definir l'arquitectura de xarxa, seguint els estàndards i les bones pràctiques definides a l'IEC62443 i NIST800-82
2. Adaptació de l'arquitectura de control al paradigma de seguretat OT actual
3. Especificació de Zones i Conductes. Estratègia filtrat intrazona
4. Controls de seguretat de xarxa addicionals per a la detecció d'anomalies OT
5. Protegir l'entorn industrial contra accessos i comportaments indeguts. Millora en la resposta a incidents de seguretat
6. Restricció del trànsit entre cel·les/processos. Reducció del soroll de xarxa i trànsit broadcast.
7. Estandardització i definició de requisits d'accés a la xarxa OT des de xarxes externes (IT, VPN). Seguretat i robustesa

Nomenclatura dispositius de xarxa

Estàndard de noms

AABBBCDDEEFFFF

- AA País on s'ubica el dispositiu d'acord amb l'estàndard UN/LOCODE (la part del país coincideix amb la norma ISO 3166-1 alpha-2)
  - En cas que els servidors estiguin allotjats en un servei Cloud, s'utilitzaran les inicials següents: ME (Middle East), EU (Europe), US (EUA), AP (Àsia Pacific), segons ubicació.
- BBB Ciutat on s'ubica el dispositiu d'acord estàndard UN/LOCODE.
  - En cas que els servidors estiguin allotjats en un servei Cloud i donin servei a més d'una seu, es faran servir les inicials dels Headquarters
- C Identificador numèric de la seu dins la ciutat on hi ha l'equip. Aquest identificador s'inclou per si hi ha diverses ubicacions a la mateixa localitat, cosa que actualment no passa.
- DD Xarxa a què pertany el dispositiu. Al principi, ens podríem trobar amb les opcions IT, OT o IO (IT/OT).
- EE Tipus d'element davant del qual ens trobem. Exemples: SW (switch), FW (Firewall), SV (server), PP (patch panell), RK (rack), PL (PLC), HM (HMI), PF (Perifèria), AP (Punt d'accés), ST (Storage), VL (VLAN), etc
- FFFF Identificador alfanumèric del dispositiu dins de la seu. Aquest ha de ser utilitzat per poder ubicar unívocament l'equip, per exemple, numerant consecutivament aquells que estan en una mateixa ubicació.

Objectiu

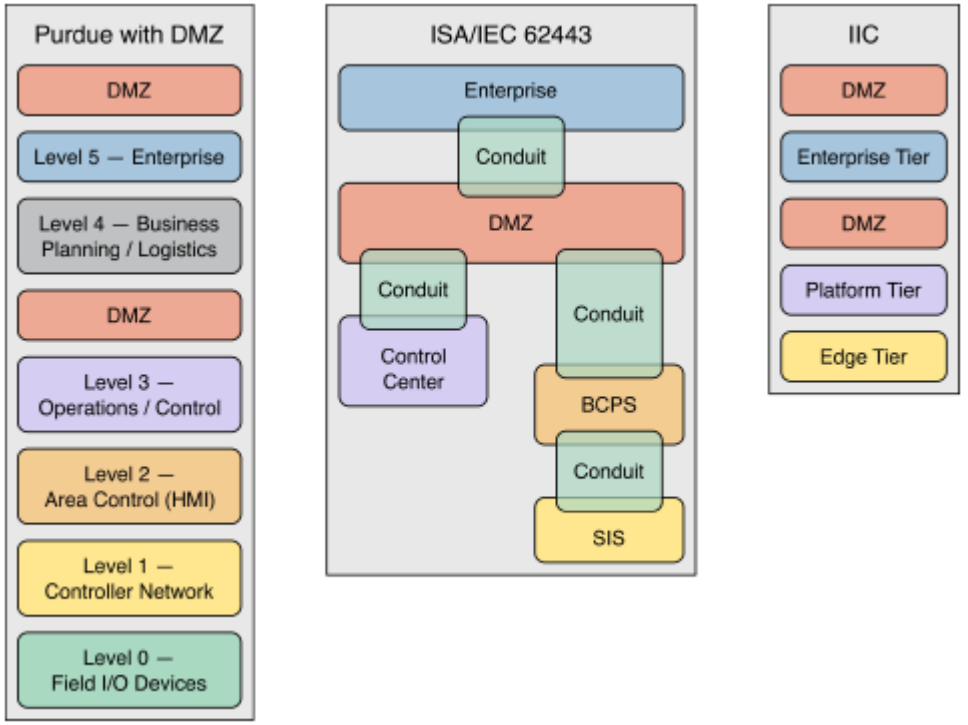
Estàndard de xarxa Industrial

INTRODUCCIÓ

Els sistemes industrials han passat de ser sistemes aïllats que executen protocols propietaris a utilitzar protocols de xarxa estàndard. Aquesta integració, permet noves capacitats per motius de productivitat o eficiència però proporciona un aïllament significativament menor de la xarxa industrial respecte a les xarxes de risc (IT), creant una major necessitat de protecció.

OBJECTIU

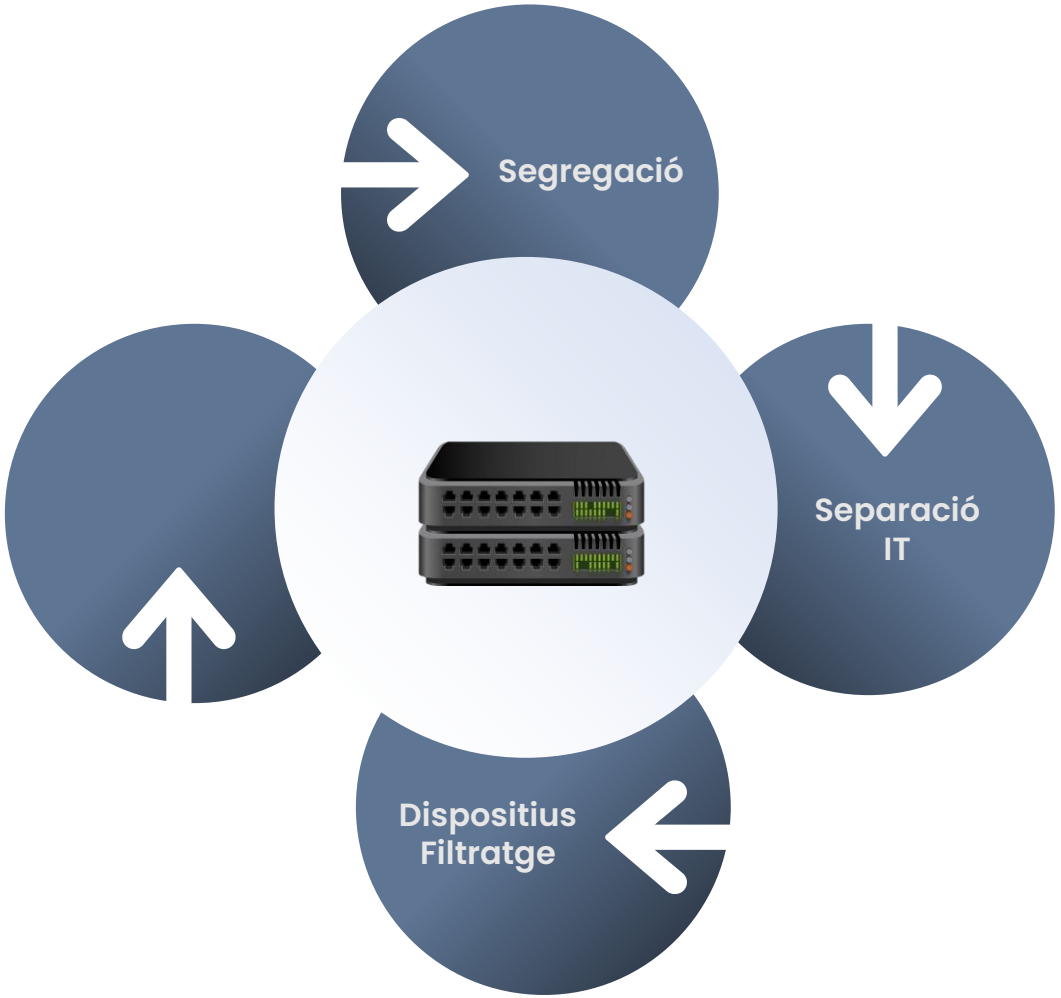
L'estàndard de xarxa presenta un model de referència per a l'entorn industrial, aplicant el concepte de defensa en profunditat per segmentar els dispositius més crítics i més vulnerables el més allunyat possible de les xarxes de risc, amb l'objectiu que un possible incident de seguretat hagi de creuar varies capes fins a arribar als sistemes objectiu.



La definició de l'arquitectura es basa en els conceptes definits en els models de referències del model Purdue, ISA/IEC62443 i IIC per adaptar-se en l'entorn industrial.

Segmentació xarxes OT. Arquitectura de referència

Principis de segmentació



Segregació

La segregació de la xarxa es basa a restringir a través de Firewalls tot el trànsit que no sigui estrictament necessari.

Separació amb IT

Es requereix una xarxa de producció amb un perímetre clarament definit i diferenciat. Aquest perímetre amb IT s' haurà de realitzar amb la inclusió d' un Firewall.

Dispositius de filtratge

Totes les zones de seguretat de l' entorn industrial han de ser gestionades pel clúster de firewalls OT, sempre que l' adreçament utilitzat sigui el descrit per l' arquitectura de referència.

Configuració del Firewall

Només es permetrà trànsit autoritzat. Al final de cada grup trobarem un DENY ALL.

Segmentació xarxes OT. Arquitectura de referència

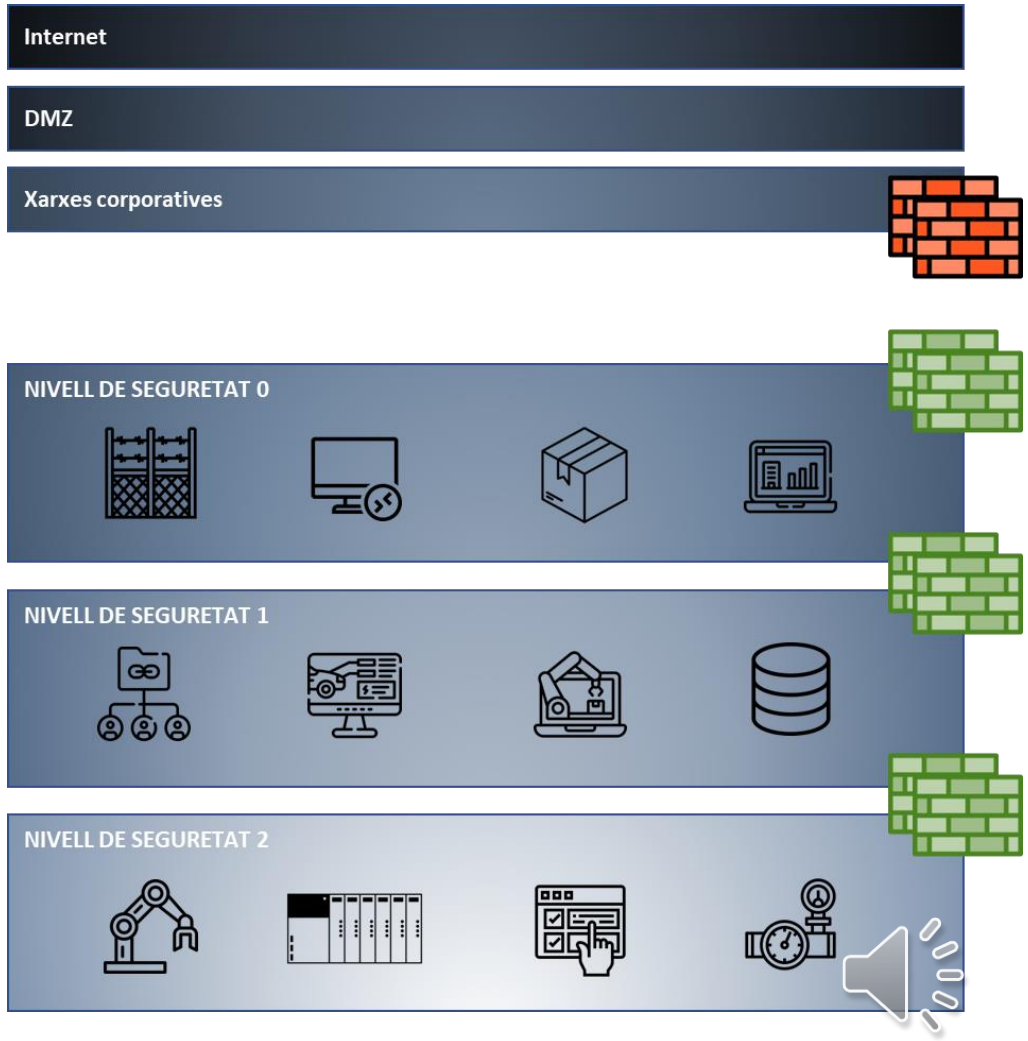
Nivells de seguretat

NIVELLS

- Nivell de seguretat 0
- Nivell de seguretat 1
- Nivell de seguretat 2
- Gestió
- VPN

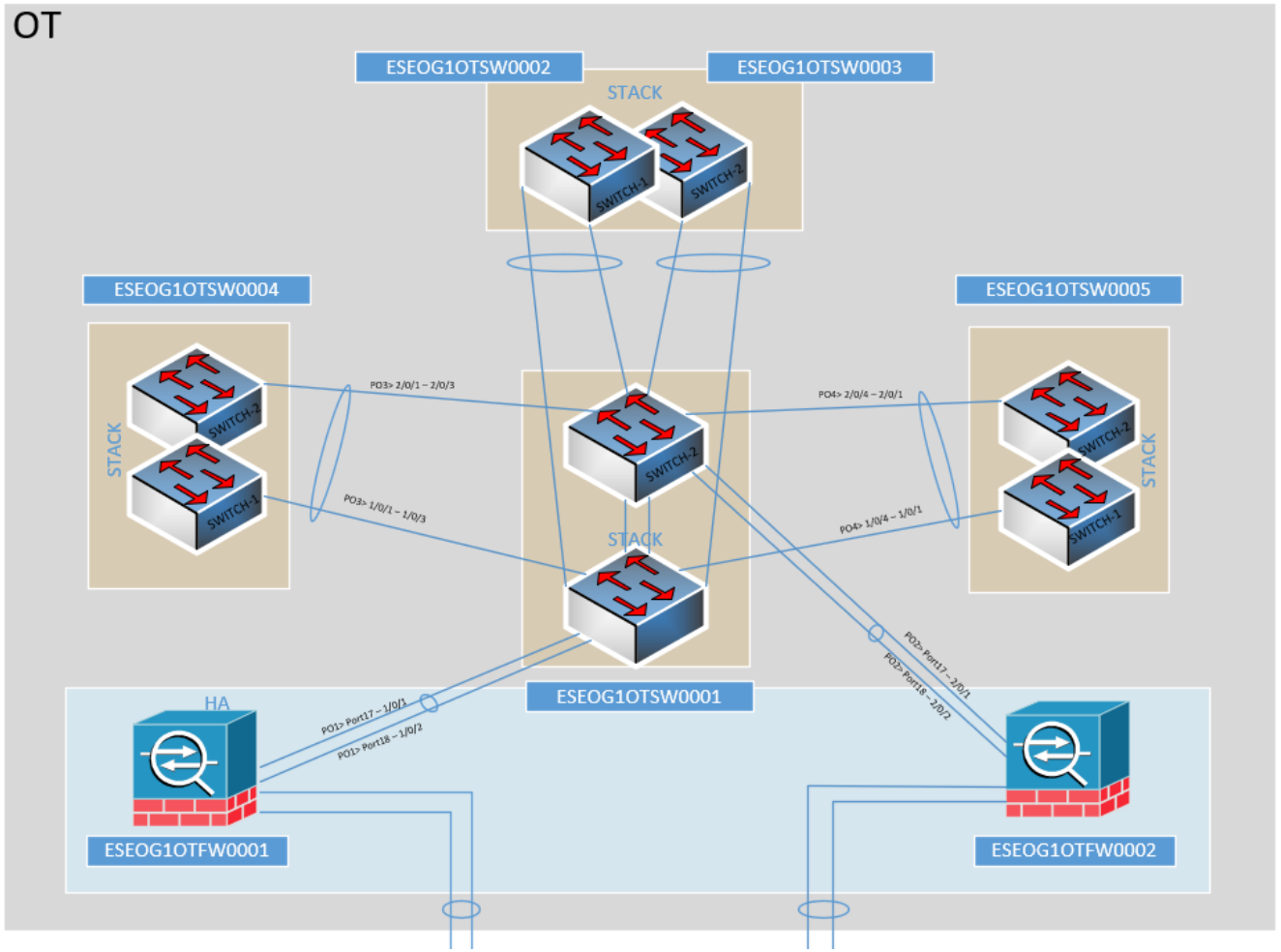
REQUISITS

- Antivirus/EDR
- Sistema operatiu/Firmware
- IPS
- Filtres d' aplicació
- Control de sessió
- Accessos remots
- Pla d'obsolescència



Arquitectura de xarxa i ciberseguretat

Disseny de xarxa



Arquitectura de xarxa i ciberseguretat

Materials

- **Firewalls**

Descripció	Quantitat
FortiGate-201F Hardware plus 3 Year 24x7 FortiCare and FortiGuard Enterprise Protection	2
10GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots	4
FortiGate-201F Hardware plus 3 Year 24x7 FortiCare and FortiGuard Enterprise Protection	2

- **Switches Core**

Descripció	Quantitat
Catalyst 9300X 24x25G Fiber Ports, modular uplink Switch	2
Catalyst Stack Power Cable 30 CM Spare	2
715W AC 80+ platinum Config 1 Power Supply Spare	2
DNA Essentials 5 Year License	2

- **Switches Acceso**

Descripció	Quantitat
Catalyst 9200L 48-port PoE+, 4 x 10G, Network Essentials	5
1KW AC Config 5 Power Supply	5
Cisco Catalyst 9200L Stack Module	5
C9200L Cisco DNA Essentials, 48-port, 5 Year Term license	5
10GBASE-SR SFP Module (Interconexió Acces, Core y Firewall)	20

Arquitectura de servidors(OT)

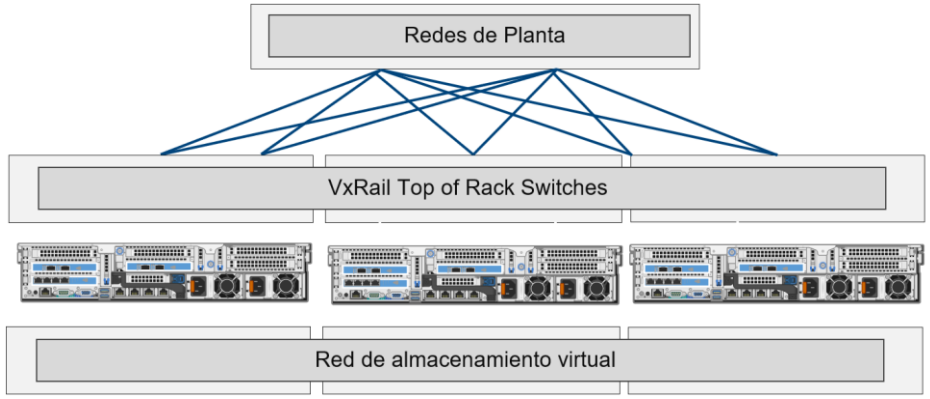
Objectiu i solució proposada

1 Objectiu

- Instal·lació i configuració d'una infraestructura de virtualització hiperconvergent, amb capacitat per allotjar el conjunt de servidors i estacions client que constitueixen el sistema de control i serialització.

2 Solució de virtualització proposada

- Solució hiperconvergent VxRAIL
- Switchs dedicats per independitzar el trànsit SAN de la xarxa industrial
- Actualitzacions certificades en conjunt. Menor complexitat i probabilitat de fallada per incompatibilitats.



Arquitectura de servidores (OT)

Materials

- **Nodos VxRail**

Descripción	Cantidad
VxRail E660F, ALL FLASH	3
16 GB de memoria RDIMM, 3200 MT/s, bloque doble	12
SSD SATA Read-Intensive de 1,92 TB a 6 Gb/s, unidad AG 512 de 2,5 conectable en caliente, 1 esc/día	12
VxRail VMware vSphere Standard para 1 procesador, 5 años	3
VxRail VMware, vSAN Standard, 5 años	3
5 Years, ProSupport with Mission Critical, Software Support	3

- **Switches TOR**

Descripción	Cantidad
Switch Dell EMC S4112F, 12 × 10 GbE SFP+, 3 × 100 GbE QSFP28	2
Cable Dell Networking, 100 GbE, de QSFP28 a QSFP28, cable de conexió directa de cobre pasivo, 0,5 metros	2
Dell Networking, de SFP+ a SFP+, 10 GbE, cable de conexión directa Twinax de cobre, 3 metros	2

- **Licencias**

Descripción	Cantidad
Windows Server 2019 Standard, ROK, 16 núcleos	3
MS2019 Standard, licencia adicional, 16 núcleos, sin medios/claves, kit para clientes	3

Solució de backups (OT)

Objectiu y solució proposada

Universitat Oberta de Catalunya

1 **Reduir el temps d'inactivitat i les interrupcions en producció**

- Rapidesa en l'accés a les còpies de seguretat per reduir el temps d'inactivitat de la producció, podent restaurar la darrera versió vàlida de tots els dispositius que donen suport als processos de fàbrica.

2 **Reducció tasques manuals equips baremetal**

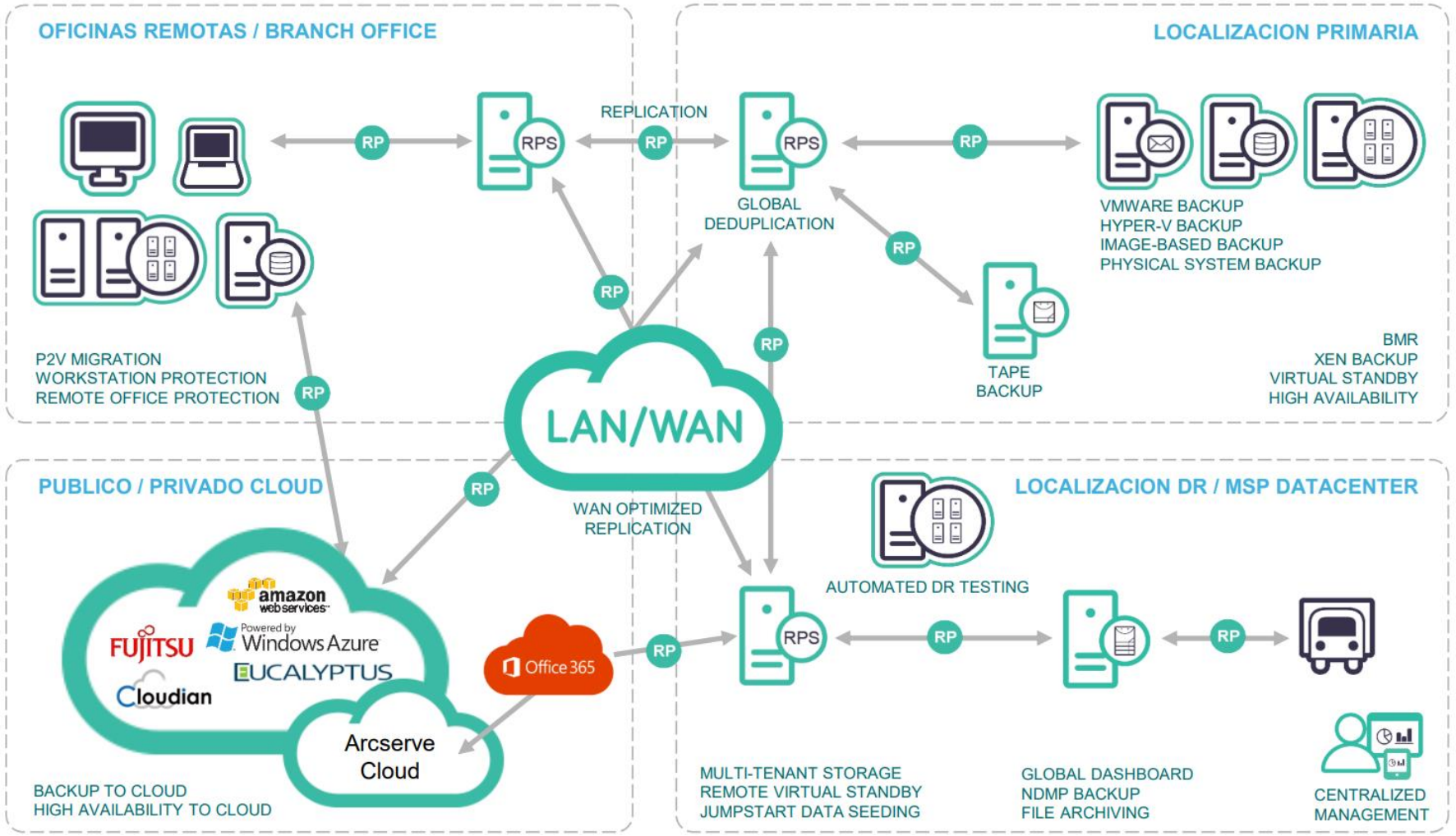
- Configuració automàtica de còpies i plans de backup, definint periodicitat, retenció i arxivat automàtic.

2 **Augmentar els nivells de compliment i seguretat**

- Emmagatzematge estructurat de totes les versions. Retencions de backups a appliance:
  - Backup diari: 7 dies
  - Backup setmanal: 5 setmanes
  - Backup mensual: 12 mesos
  - Backup manual: 1 còpia
- Per a l'arxivat a una segona unitat d'emmagatzematge, s'instal·larà una cabina amb 96TB d'emmagatzematge brut immutables, amb snapshots cada 90 segons. Aquesta cabina pot estar al mateix site que l'appliance o al site remot per fer còpies creuades. Retencions de backups a cabina d'arxivat:
  - Backup diari: 7 dies
  - Backup setmanal: 5 setmanes
  - Backup mensual: 84 mesos
  - Backup manual: 1 còpia

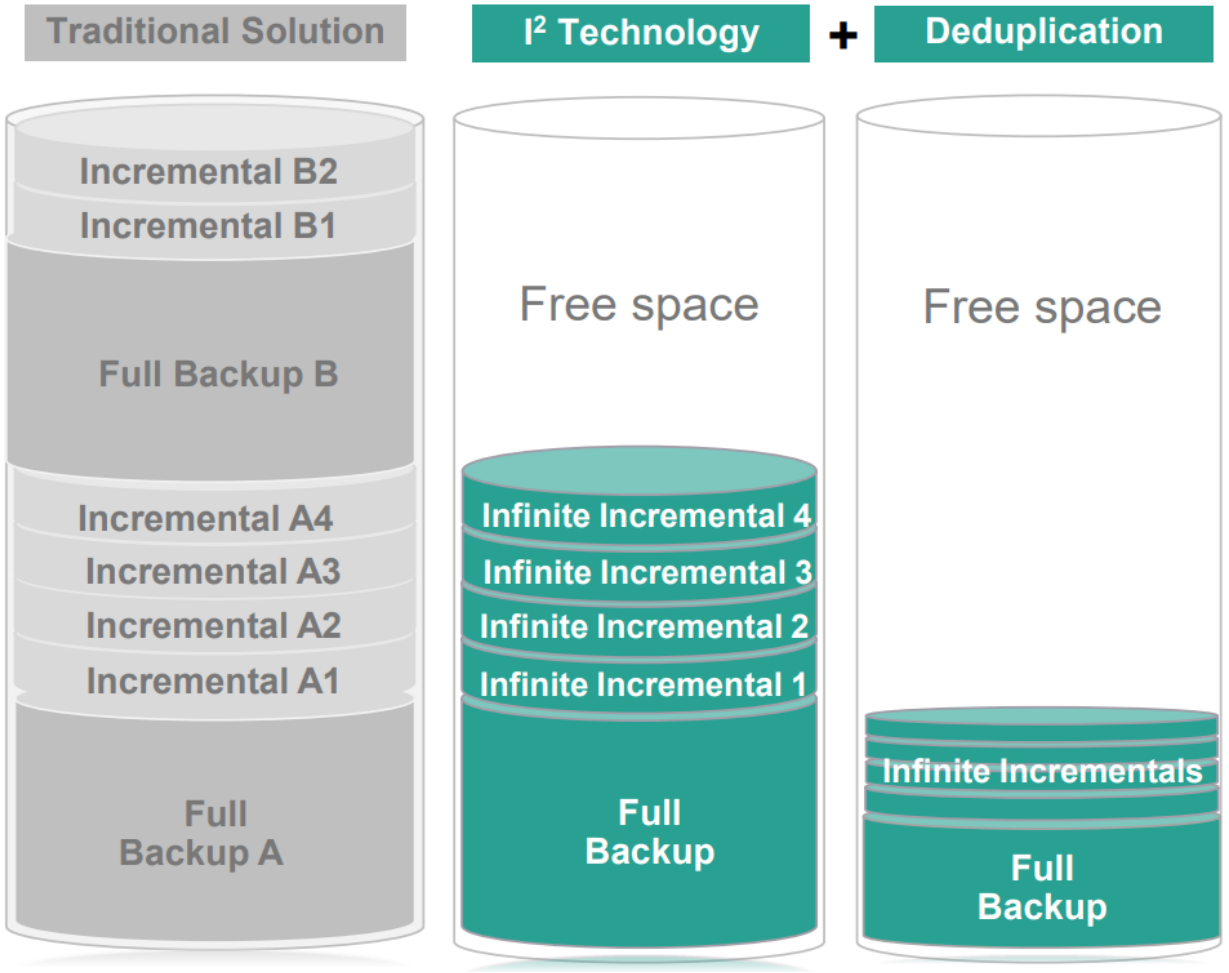
Solució de backups (OT)

Arcserve UDP



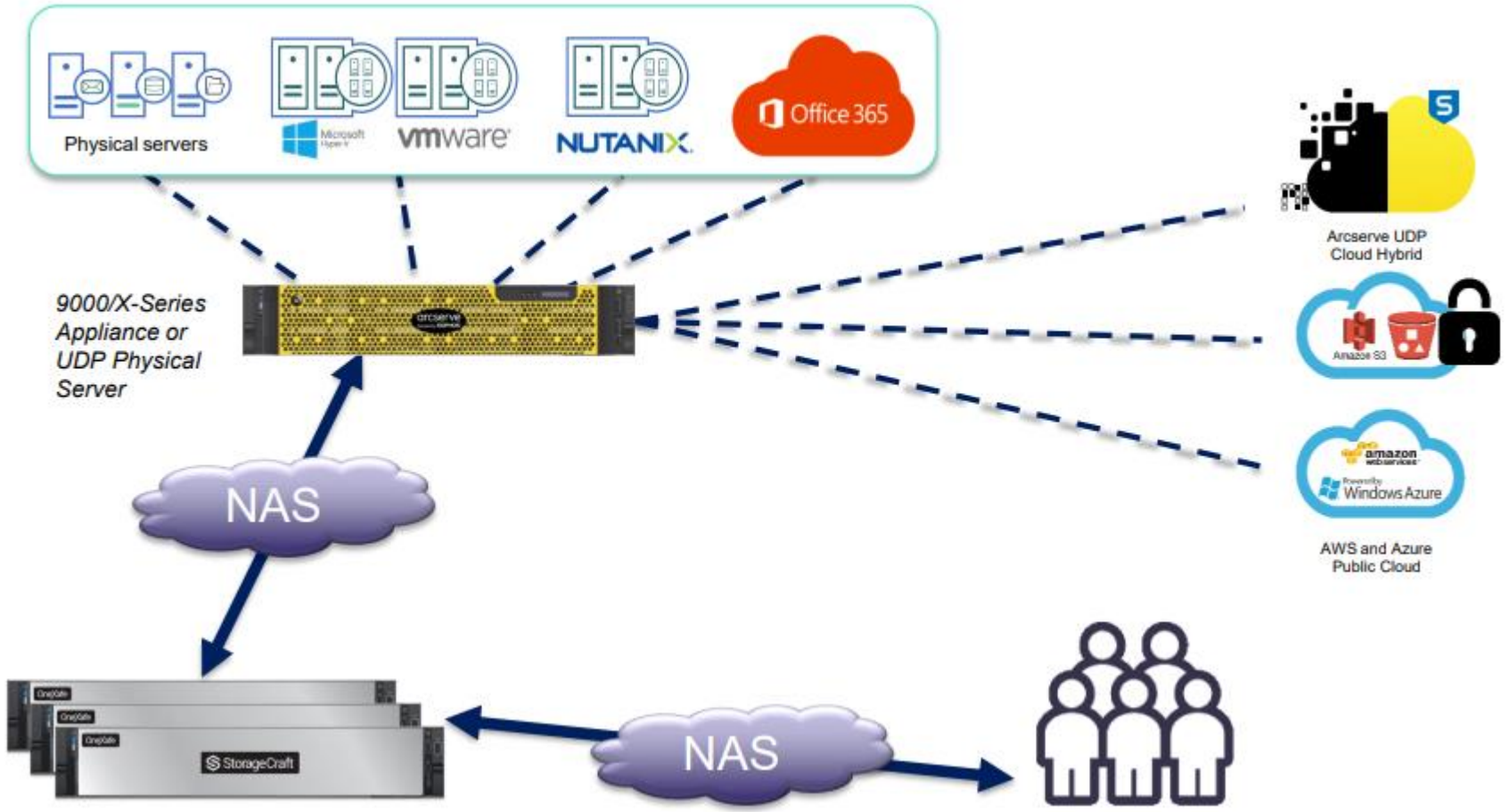
Solució de backups (OT)

Arcserve UDP



Solució de backups (OT)

Cabina immutable OneXafe



Solución de backups (OT)

Materiales

- **ArcServe**

Descripción	Cantidad
Arcserve Appliance 9048 - Product Only	1
Arcserve Appliance 9048 - Three Year Platinum Maintenance - New	1
Arcserve Appliance 9000 series - SFP+, SR, Optical Transceiver, Intel, 10Gb-1Gb, Customer Installation	6
Arcserve Appliance 9000 series - Intel X710 Dual Port 10Gb Direct Attach, SFP+, Converged Network Adapter, Customer Kit	1

- **Cabina inmutable**

Descripción	Cantidad
OneXafe 4412 96TB 10GbE SFP+	1

Conclusions