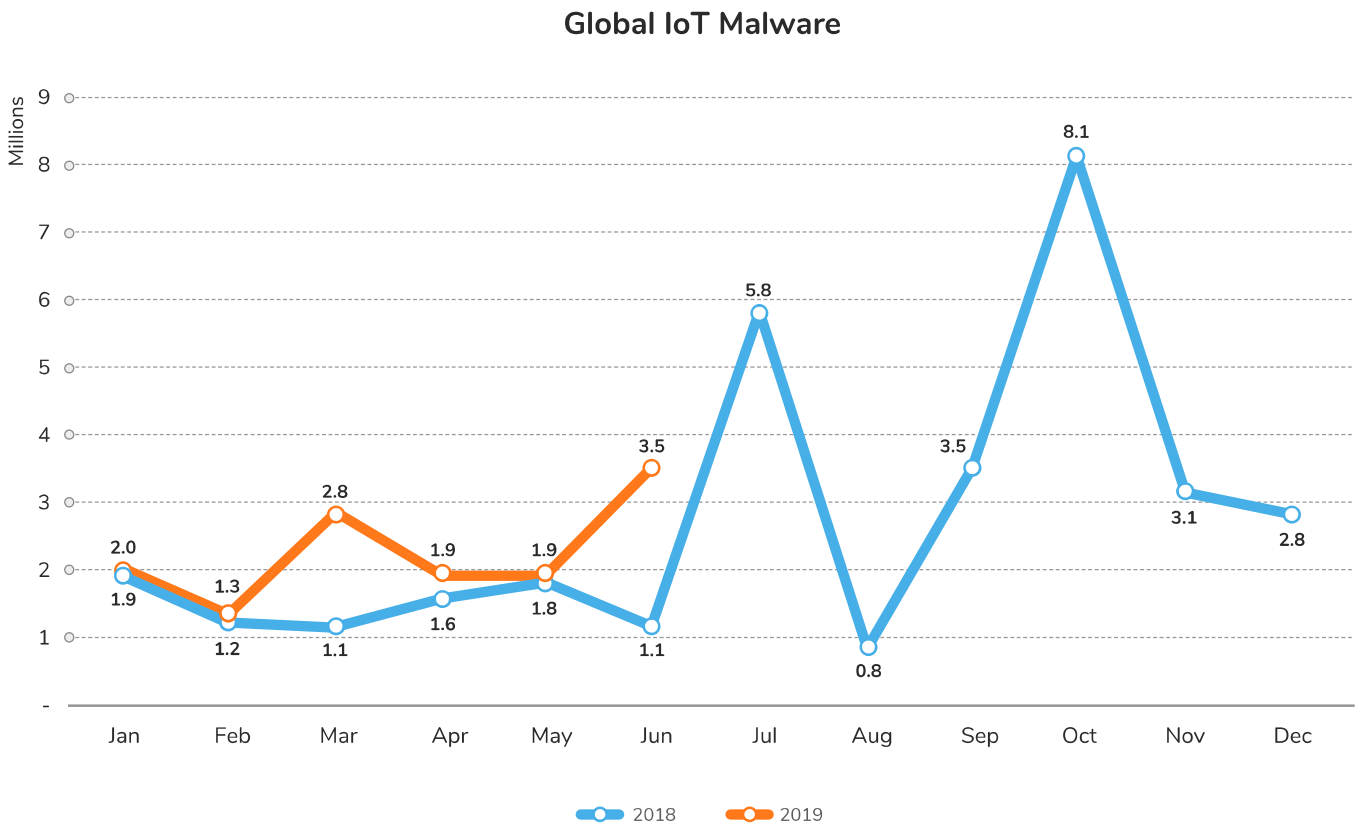
Cybersicurezza e sanità: sfide e opportunità per l'industria 4.0

Claudio Dell'Ali

SE Italia Extreme Networks

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

I MALWARE PROLIFERANO NEL MONDO IOT



Solo considerando la prima metà del 2019, gli addetti ai lavori hanno già registrato ben 13,5 milioni di attacchi verso le Device IoT, che superano i primi due trimestri del 2018 ben del 54,6%

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

ZERO TRUST PER IOT DEVICE

Le device IoT sono direttamente collegate all'interno della rete e per loro natura tendono a dialogare con server remoti posizionati nel Cloud senza un approccio robusto di sicurezze.

ZERO TRUST è il concetto alla base di un architettura incentrata sulla sicurezza che deve coniugare l'utilizzo delle device IoT mitigando i rischi

MINACCE ALL'EDGE DELLA RETE

25B
IoT Devices

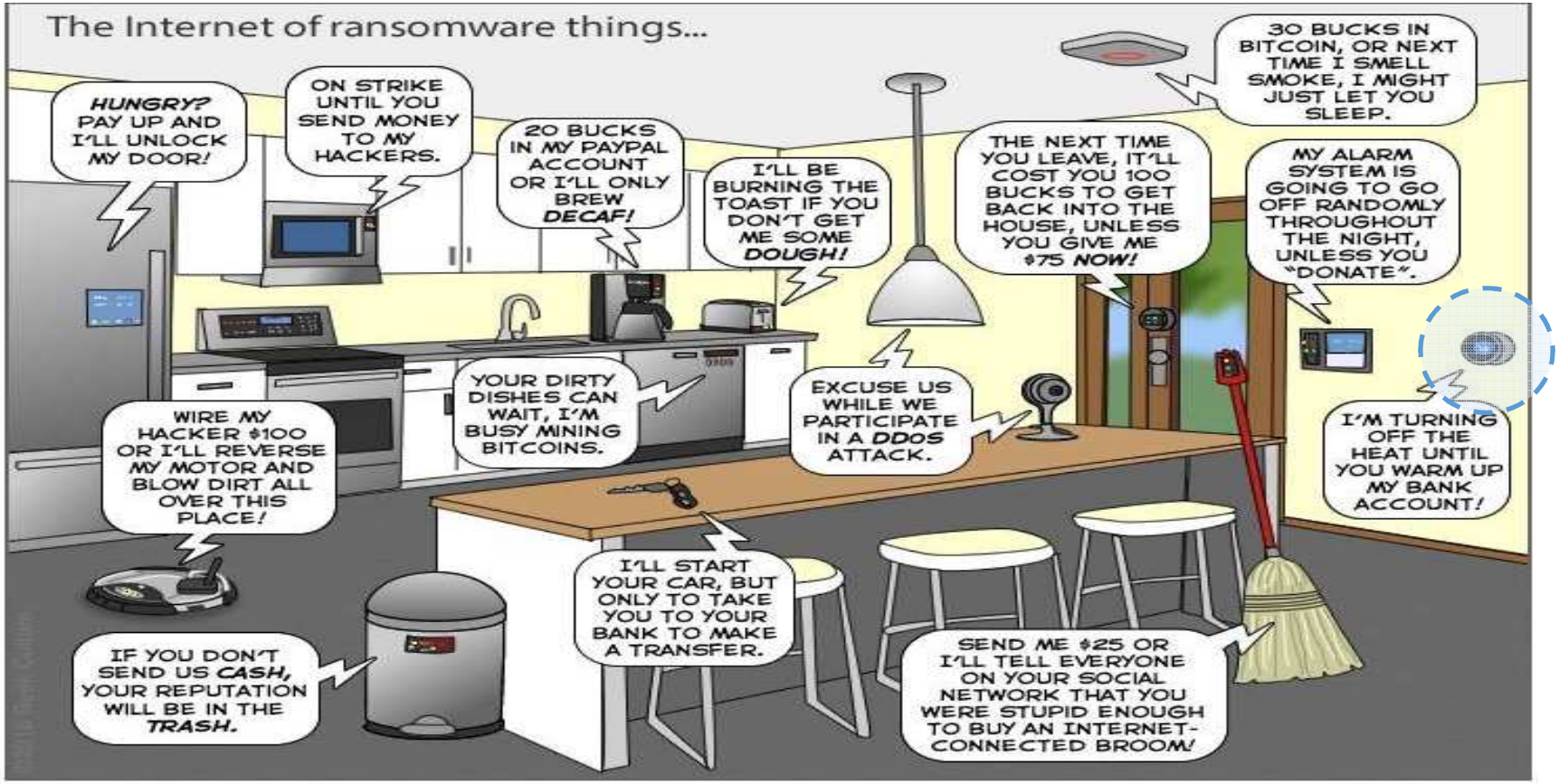
33%
Bluetooth (BLE) Beacon
Growth Rate

600%
Increase in IoT attacks
between 2016-2017

75%
Connected to
WLAN

25+%
Enterprise
Attacks will be IoT

IOT E RANSOMWARE: COLLISIONE!!



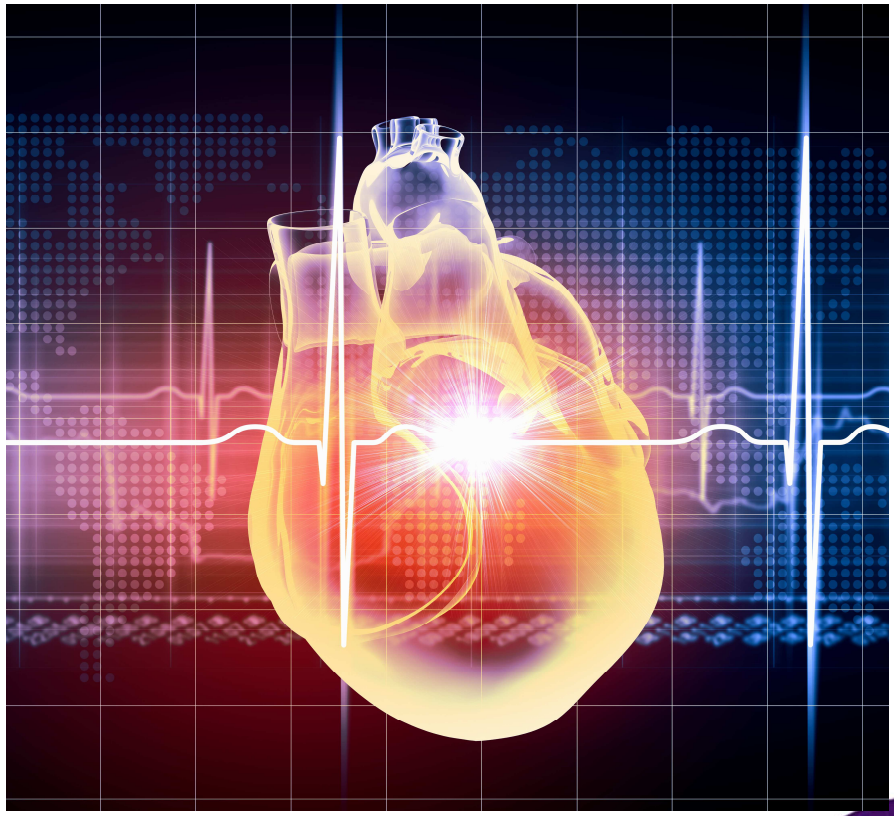
COSA SIGNIFICA IOT”

IoT=Internet of Things? NO IoT=Internet of Threats?

IOT

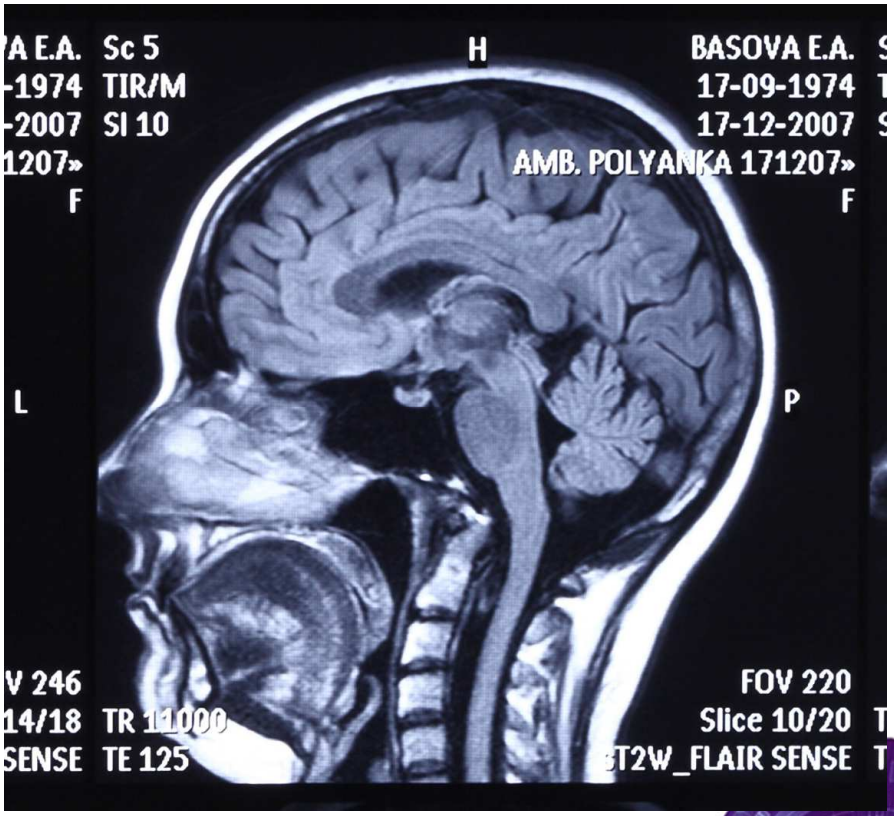
IMPATTO SIGNIFICATIVO

- Ottobre 2016: Johnson & Johnson avvisò che una delle sue pompe di insulina per diabetici era soggetta ad un attacco Hacker che causava un sovradosaggio letale
- Agosto 2017 (USA): ben 465,000 americani ricevettero una nota che li avvisava di aggiornare il firmware che gestiva il loro pacemaker Abbott (ex St. Jude Medical) poiché esisteva il rischio concreto di attacchi Hacker potenzialmente fatali



MRI: VULNERABILITA' LETALE

- Dei ricercatori Israeliani hanno scoperto che attraverso una vulnerabilità presente su Magnetic Resonance Imaging (MRI) i tumori cancerosi possono essere rimossi o inseriti da o nelle immagini del paziente
- L'infezione avviene sia tramite la rete PAC sia mediante iniezione diretta tramite chiavetta USB
- Se il Malware attecchisce possono essere modificale le immagini di tutti i pazienti, di alcuni specifici pazienti sia nuove che archiviate
- Gli studi effettuati riportano che le alterazioni alle immagini arrivano fino al 90% complessivo



Fonti: https://www.google.es/amp/s/www.washingtonpost.com/amphtml/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/; - https://arxiv.org/pdf/1901.03597.pdf

LE SPECIFICHE SFIDE DELLE DEVICE IOT

Specifiche generali alla maggior parte dei Dispositivi IoT

- Plug & Play senza sicurezza integrata
- Sistema operativo obsoleto, password non codificate, backdoor disponibili
- Difficile da ‘’patchare’’ contro le vulnerabilità
- Molti IoT device richiedono un collegamento mandatario ai PC legacy
- L'aggiornamento di tali dispositivi può presupporre la ricertificazione
- I dispositivi IoT potrebbero essere al di fuori del controllo degli Operatori IT: vengono collegati senza preavviso
- Mobilità del dispositivo
- Complessità dell'implementazione della sicurezza

> *"I dispositivi medici meno recenti nell'ambiente degli operatori sanitari pongono minacce specifiche che creano sfide uniche per il mondo della Sanità"*
>
> – Gartner 2017

SFIDE IOT: METTERE IN SICUREZZA L'EDGE

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA
A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

SICUREZZA SUL PUNTO RETE

Bring Security directly to the IOT Device

Add a Smart Security Physical Layer into your Network

Nel 2018 Extreme Network ha messo sul mercato il prodotto ''Defender for IoT'', pensato per portare un livello di sicurezza trasparente, implementabile su tutte le reti, direttamente al punto di connessione della Device IoT.

Funziona per accessi Cablati e Wireless.

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

COSA FA DEFENDER FOR IOT

Sicurezza, trasmissioni Cifrate e non solo…

Sicurezza a 360°

- Controlla la Device IoT dal punto di accesso alla rete
- Effettua un monitoraggio del traffic al fine di creare Policy Specifiche
- Isola fisicamente le Device tra di loro e nella rete
- IPSEC: trasmissioni cifrate attraverso rete interna e/o esterna

Visibilità Applicativa

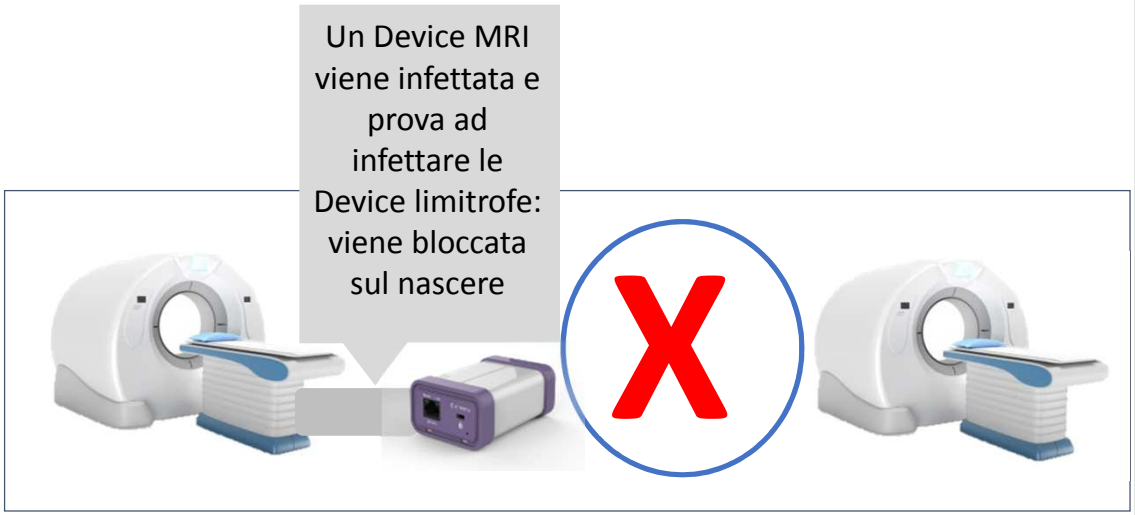
- IoT device traffic (utilizzo e throughput)
- Visibilità applicati fino a L7

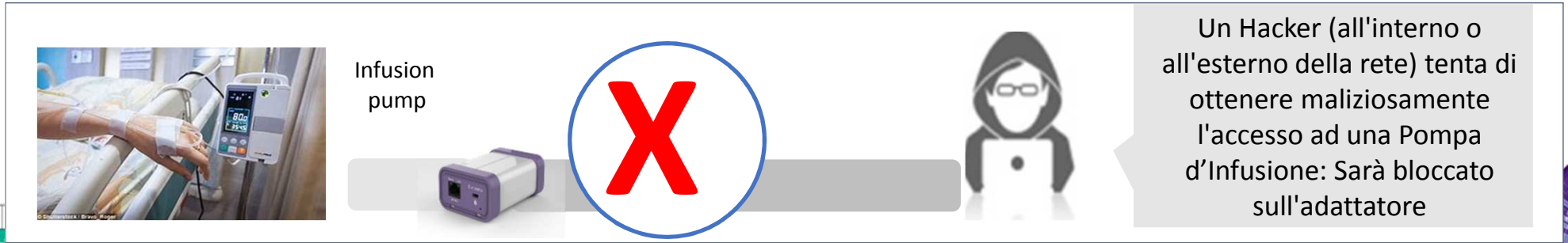
Inventario

- Pannello di controllo WEB-Based
- Inventario centralizzato per le Device attive e per quelle non attive
- Mostra e traccia la localizzazione della Device (ASSET)

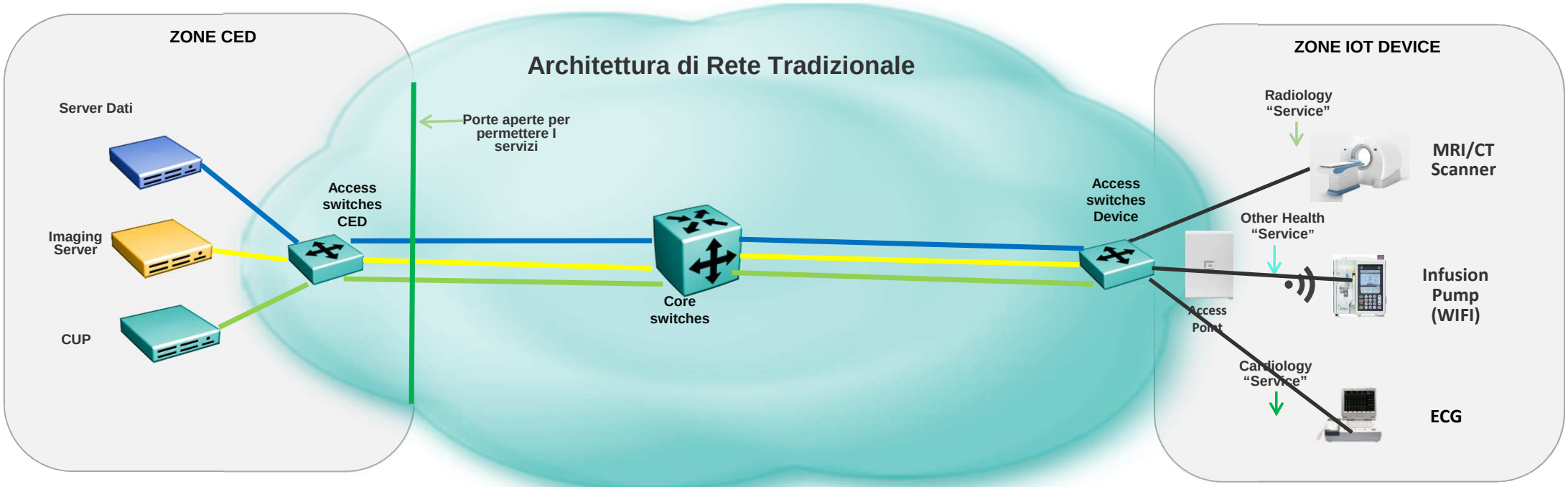
Easy Security for All Network Topology

SICUREZZA SUL PUNTOM RETE



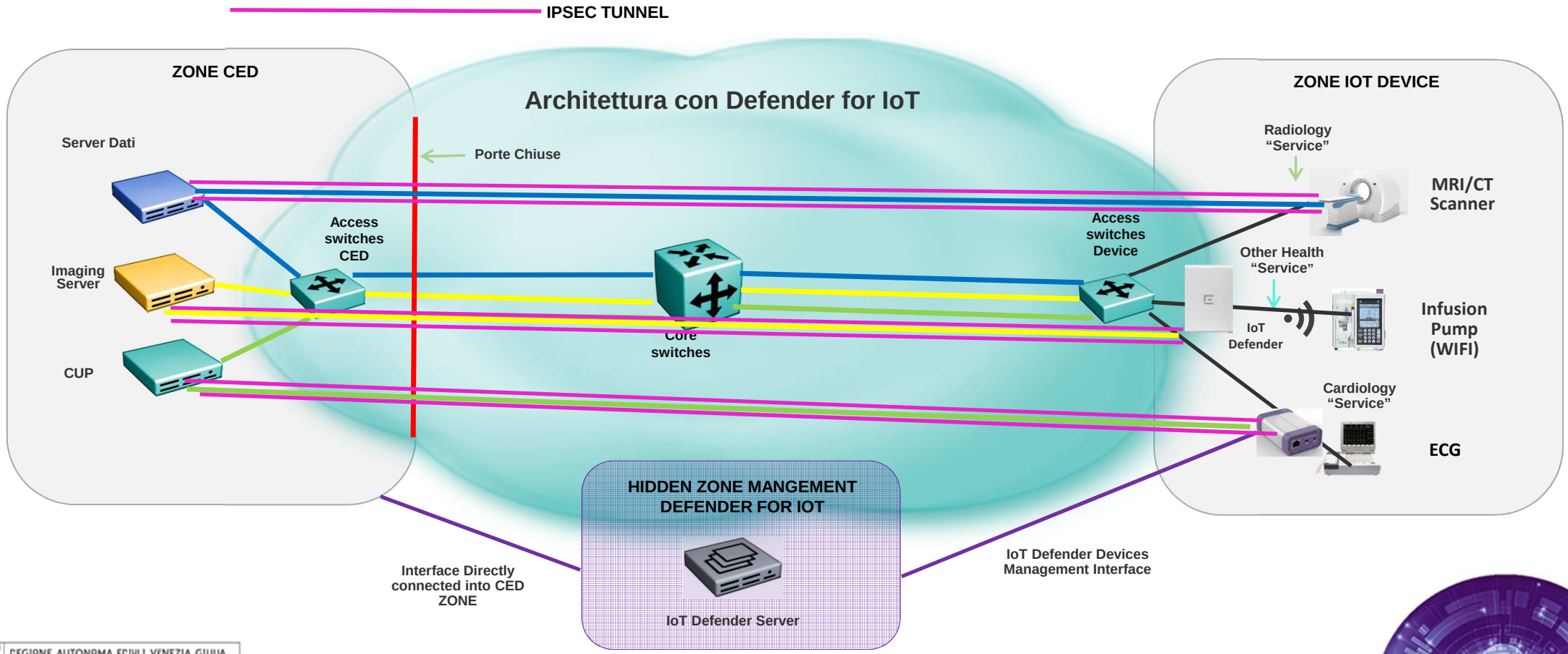


ARCHITETTURA TRADIZIONALE



Benefit: Ability to deploy a secure IoT solution without significant network changes

ARCHITETTURA TRADIZIONALE



Benefit: Ability to deploy a secure IoT solution without significant network changes

COMPLIANT

IPSEC

G.D.P.R.

NORMA IEC 80001

Fintanto che i dispositivi medici non prevedevano la connessione ad una rete internet, l'unico responsabile per i rischi associati alla loro progettazione, produzione e funzionamento era solo ed esclusivamente il fabbricante.
Oggi, considerato che moltissimi di essi sono dotati di interfaccia di rete, l'attore coinvolto in materia di gestione del rischio non può più essere soltanto il fabbricante: il buon senso, infatti, suggerisce che il fabbricante non può effettuare una gestione del rischio completa e corretta se non conosce preventivamente la tipologia e le caratteristiche dell'infrastruttura IT su cui il dispositivo verrà inserito.

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

GRAZIE

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA
A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO