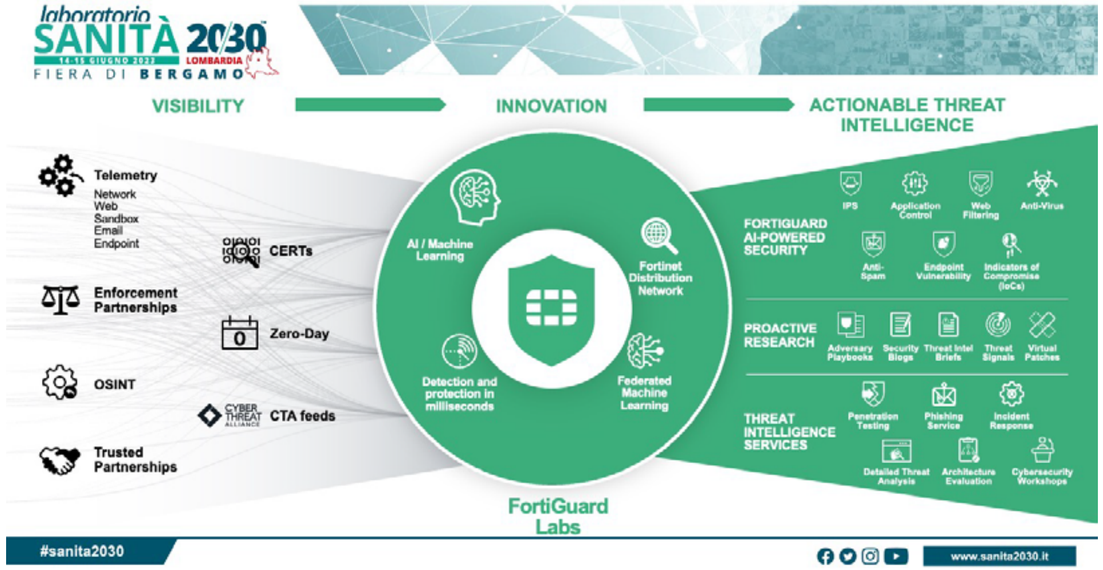
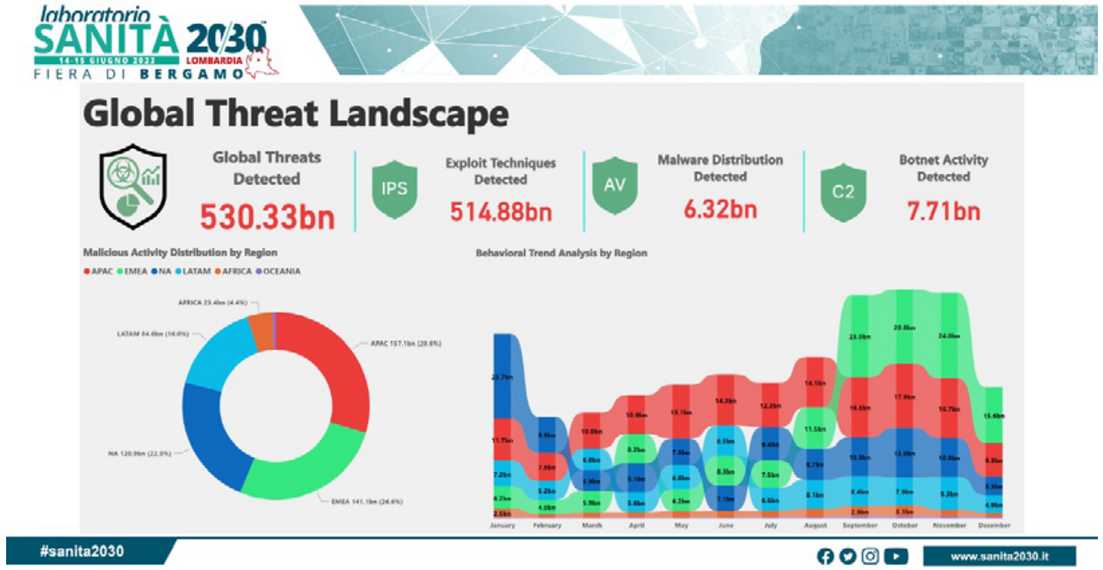
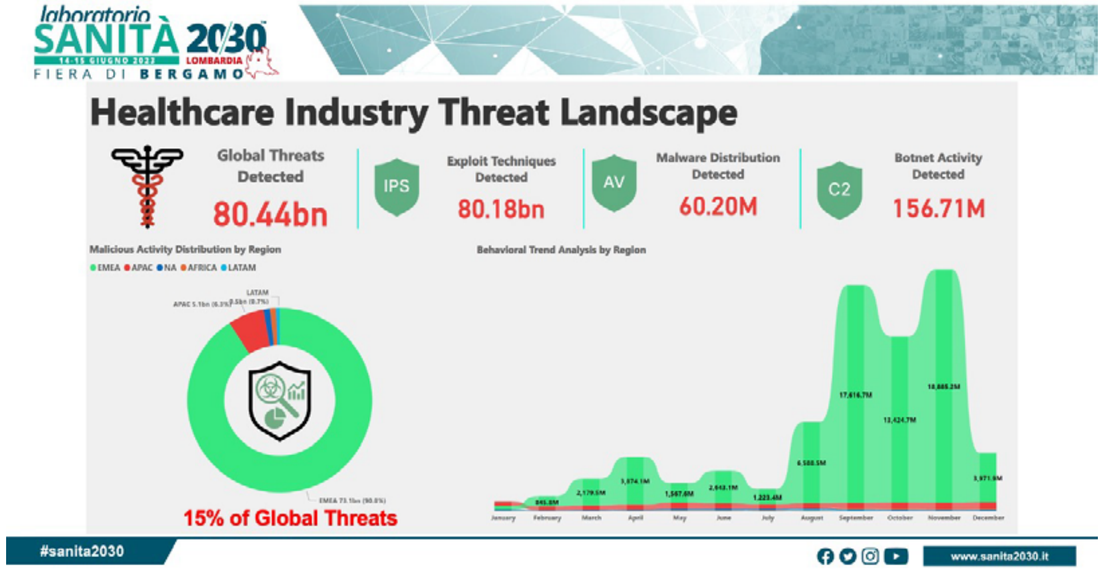
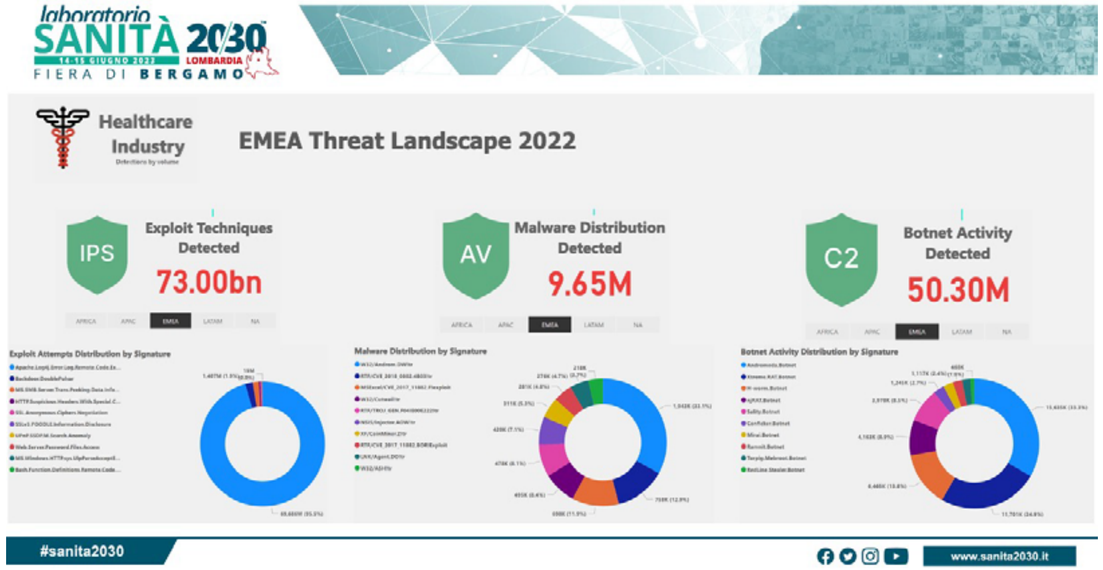
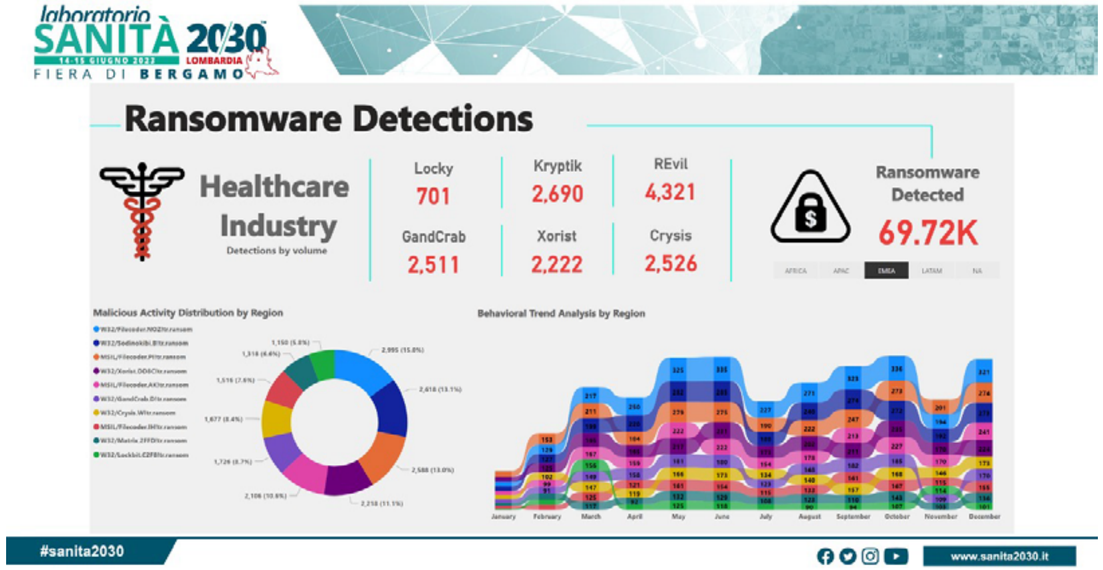


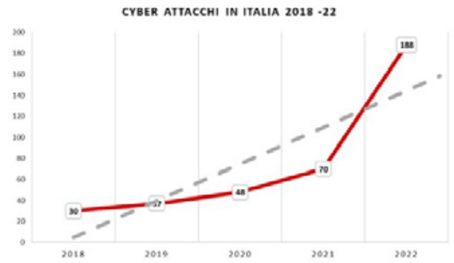


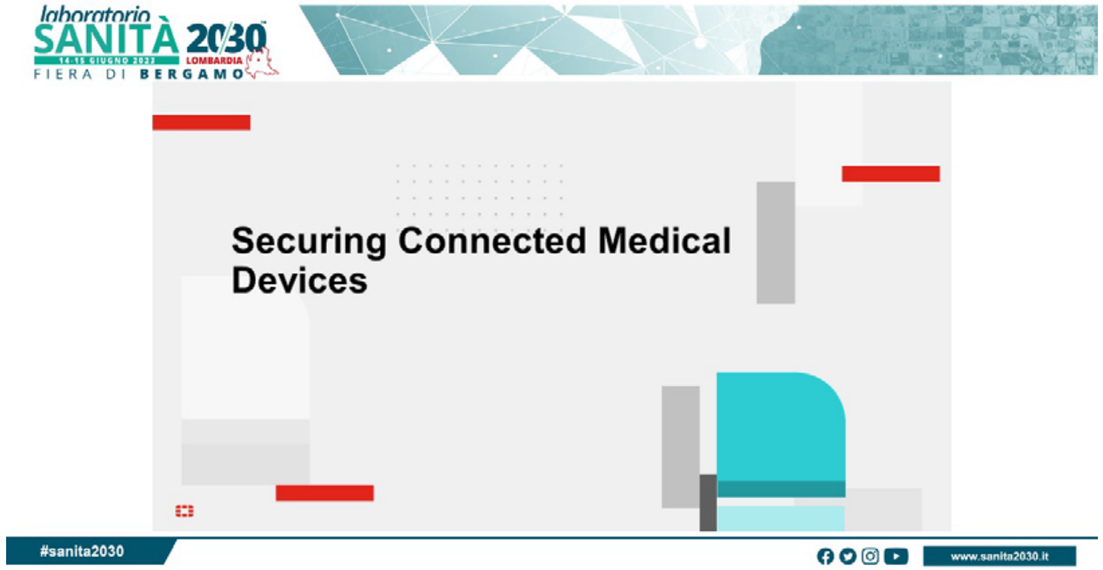






Rapporto Clusit 2023





Infusion Pumps

PCA Pumps
(Patient Controlled Anesthesia)

Medication Dispensers

Glucometers

Lab Analysis Devices

Nurse Call Systems

Challenges Specific to Medical Devices

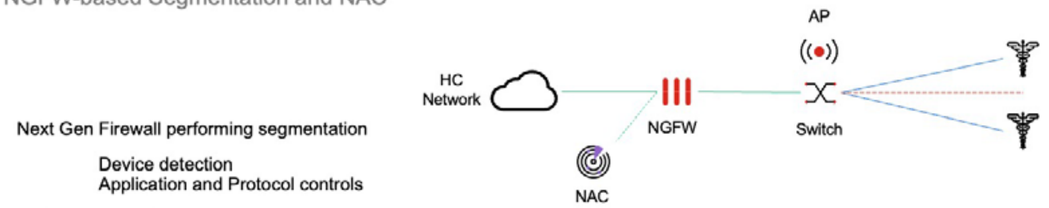
- Most devices are “black boxes”
- Operating systems are often embedded versions
  - Custom tiny Linux build, Vanilla Windows, WinCE, XP (!!)
  - Most devices do not support any sort of standard update system (Windows Update, yum/apt, etc.)
    - Updates will come in the form of some sort of maintenance update from the vendor
  - Can not join Active Directory, MDM, or apply any corporate policies
  - These vanilla OS installs may have unnecessary services enabled
- Limited or non-existent 802.1X capabilities
  - Big issue for Wi-Fi clients (PSK only?)

Risks posed by Medical Devices

- These are often truly critical devices
  - Medication administration
  - Patient telemetry can't be recreated if lost or missed
- Can't be added to a standard IT patching and update program
- Are absolutely targets for bad actors
  - If compromised, can be leveraged for lateral movements
- Aren't necessarily monitored for bad behavior, anomalies

Securing Medical Devices

NGFW-based Segmentation and NAC



Next Gen Firewall performing segmentation

- Device detection
- Application and Protocol controls

Network Access Control

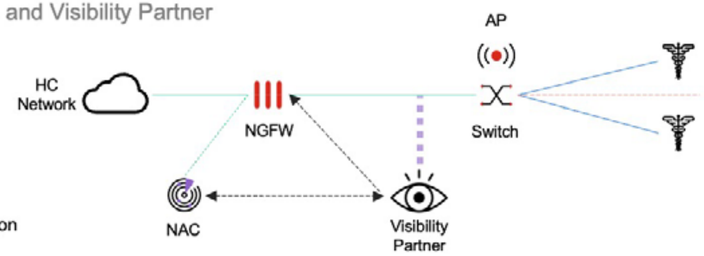
- Microsegmentation based on device role

IoT detection service

- Subscription service that allows NGFW to detect specific IoT-type devices
- Continually updated to enable detection of new devices

Securing Medical Devices

NGFW-based Segmentation, NAC and Visibility Partner



Next Gen Firewall performing segmentation

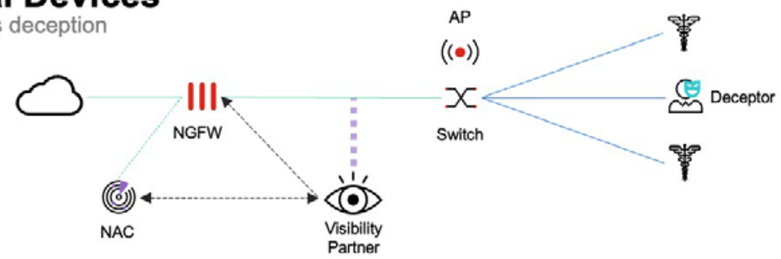
Visibility partner solutions

Examine traffic from devices and can identify devices down to the firmware revision

This granular, medical-device specific identification helps further place and segment devices, and apply proper policies via NAC integration or direct adjustment of policies in NGFW

Securing Medical Devices

Intelligent segmentation plus deception



Deceptor hides among the end device population and mimics common devices

Acts as a tripwire and provides an early warning of malicious activity

Can interact with other security device, automating countermeasures adoption

Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

Torna all'inizio