



LANDSCAPE DELLE MINACCE IN AMBITO SANITA'

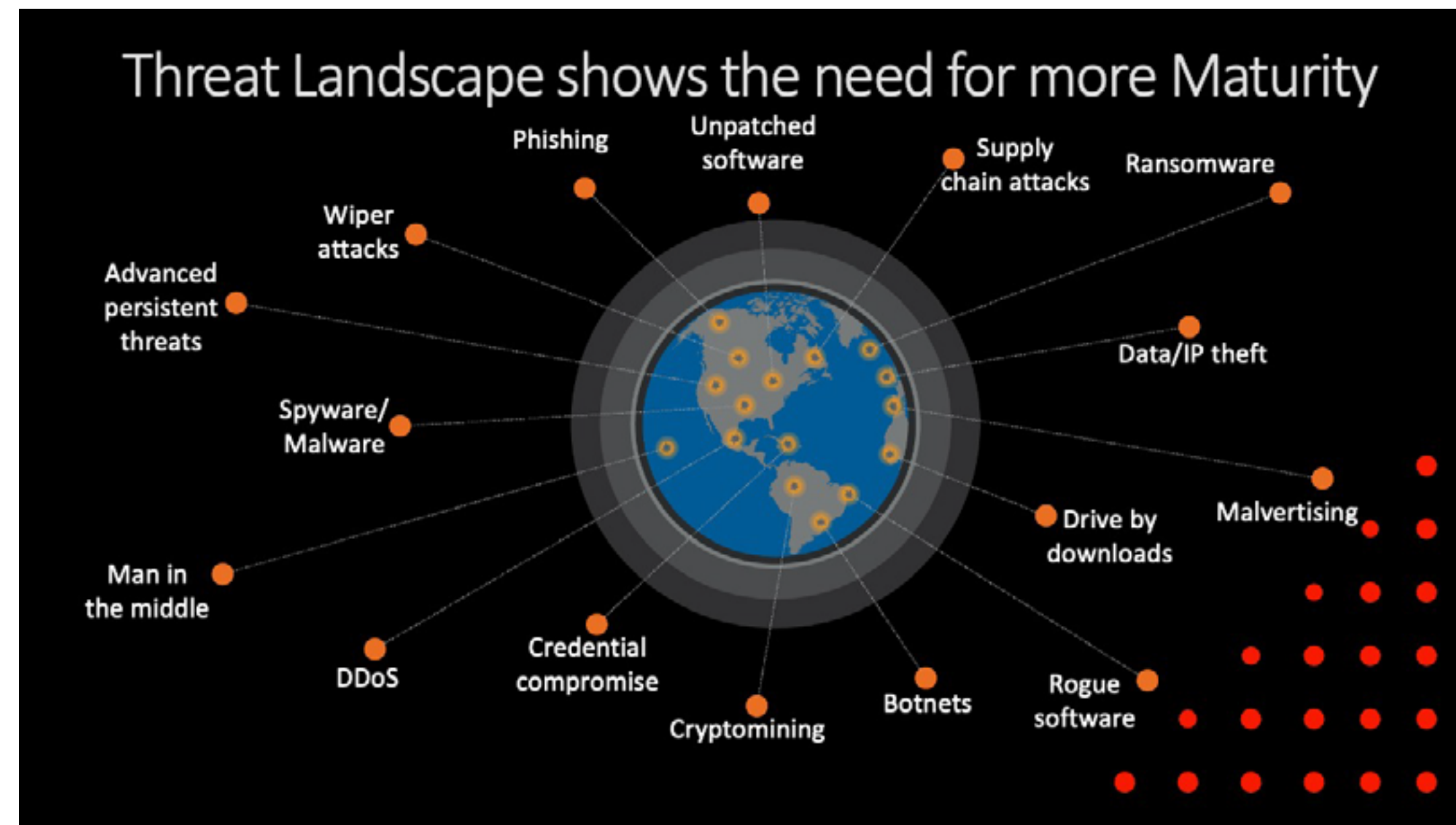
Andrea Castellano CYBERSECURITY LEADER CISCO ITALIA

#sanita2030



www.sanita2030.it

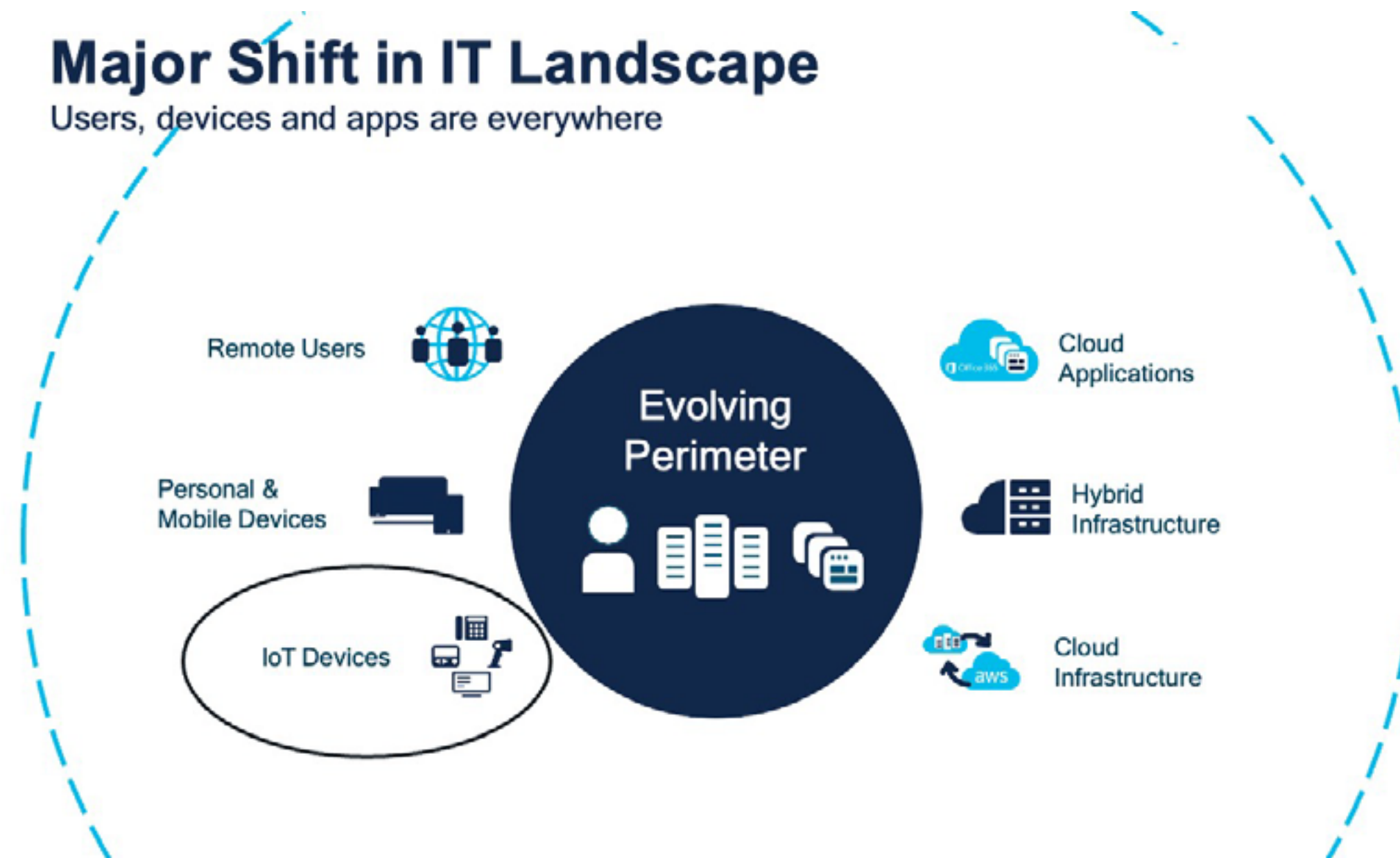


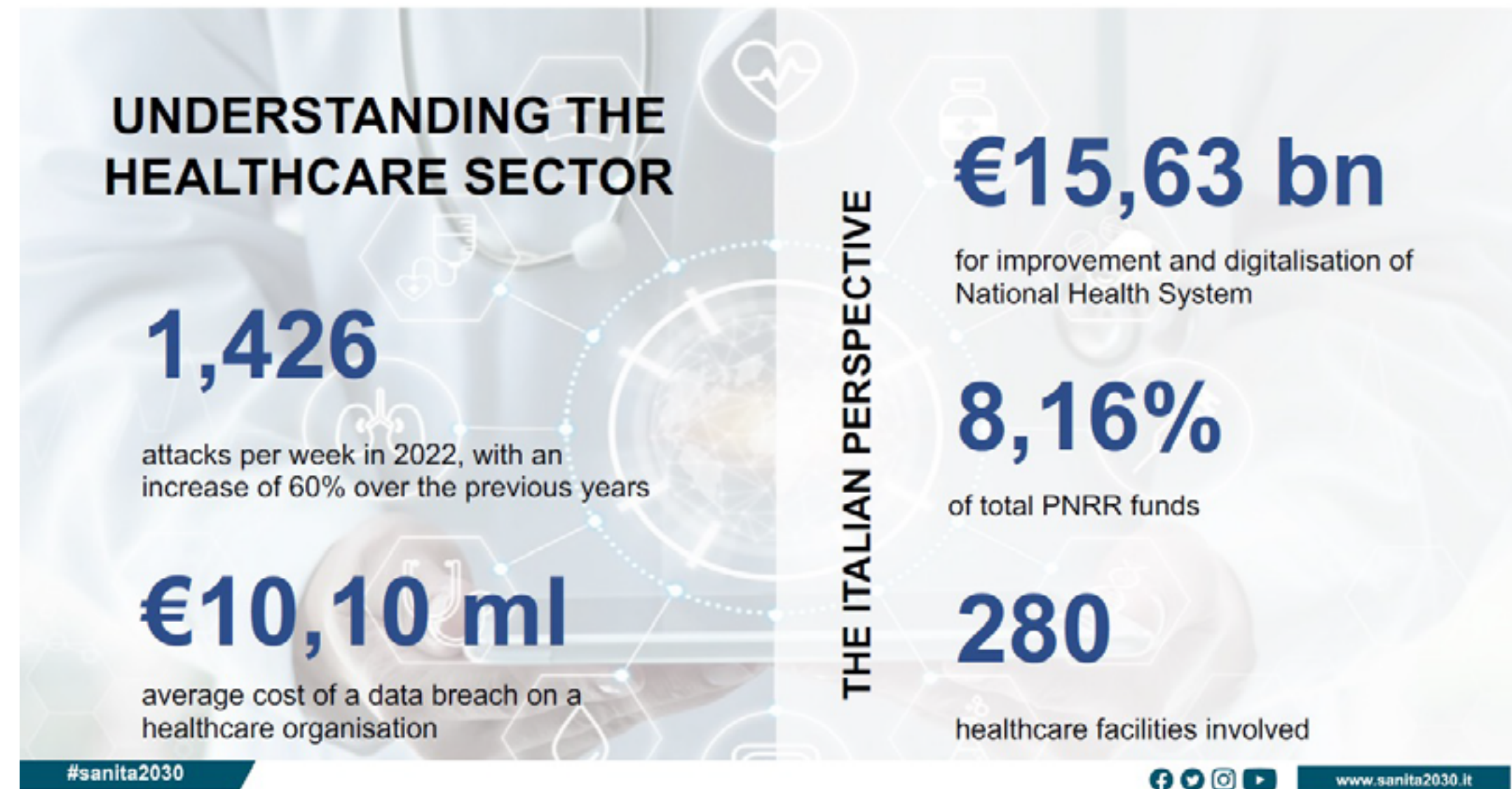




Major Shift in IT Landscape

Users, devices and apps are everywhere







ASSETS AND VALUES AT RISK

PATIENTS



DATA AND EHR

Patients' data are the most valuable assets in healthcare with an estimated value of **300-1000€/record**. Their protection is essential for ensuring **privacy** and **complying** with healthcare regulations. In addition, data are used to improve patient care and outcomes, as well as support medical research.

CITIZENS' HEALTH

The **health** of citizens is the primary focus of healthcare providers. Also, providing high-quality healthcare services can enhance the **reputation** of the healthcare provider and increase patients' loyalty and trust.

CONTINUITY OF HEALTH SERVICE (BCP)

The continuity of health services is critical for ensuring that patients receive consistent care, even in the event of a crisis or disaster.

ORGANIZATION



REPUTATION AND PATIENTS' TRUST

The reputation of a healthcare provider is critical for **attracting** and retaining patients, as well as maintaining relationships with stakeholders such as insurers and regulators.

FINANCIAL STABILITY

Healthcare providers must maintain financial stability to continue providing high-quality care and **investing** in **new technologies** and **treatments**.

KNOW HOW



INTELLECTUAL PROPERTY AND MEDICAL RESEARCH

Healthcare providers support **innovation** and the development of new treatments and therapies.

FACILITIES, EQUIPMENT, AND MEDICAL SUPPLIES

Critical for providing high-quality healthcare services. Also, their **increasing** level of **connectedness** broadens the surface of cyber attacks.

RELATIONSHIPS

Healthcare providers must maintain a network of relationships with their stakeholders (providers, insurers, regulators) to ensure patients receive coordinated care.

IT SYSTEMS

IT systems are critical for managing patient data, facilitating communication between providers, and supporting medical research.

#sanita2030



www.sanita2030.it



RELEVANT THREATS AND CYBER RISKS

1 THE DATA

Data breaches and data leaks compromising the **Confidentiality, Integrity and Availability** of the data stored could result in **identity theft** and significant delays in provision of medical services to patients. This is even riskier if data is stored on Cloud.

4 TELEMEDICINE AND IOT

Increasingly connected technologies while providing efficient ways to take care of patients, also broaden the surface for cyber attacks. Single devices may be exploited as entry points to access larger networks and directly threaten patients' health.

2 SYSTEM VULNERABILITIES

The majority of healthcare providers rely on legacy systems with **known vulnerabilities** that can easily be exploited by a malware or ransomware attack, threatening business continuity. Updating them may be problematic when the system is widely used also in equipment.

5 THIRD PARTY RISK

Healthcare providers have large networks of third parties. If not properly managed on a least-privilege access basis single partners could compromise the overall security of IT systems, resulting in a **cascading effect**.

3 THE HUMAN FACTOR

Due to a **shortage of information security professionals**, the human factor is the weakest link of the chain, vulnerable to social engineering and phishing. In healthcare, end-user security is also an issue.

6 COMPLIANCE

Healthcare is a **highly regulated sector**, subject to GDPR, NIS 1 (as Operator of Essential Service) and to the upcoming NIS 2. Hence, cyber security requirements apply, along with notification issues in case of incidents.

#sanita2030



www.sanita2030.it



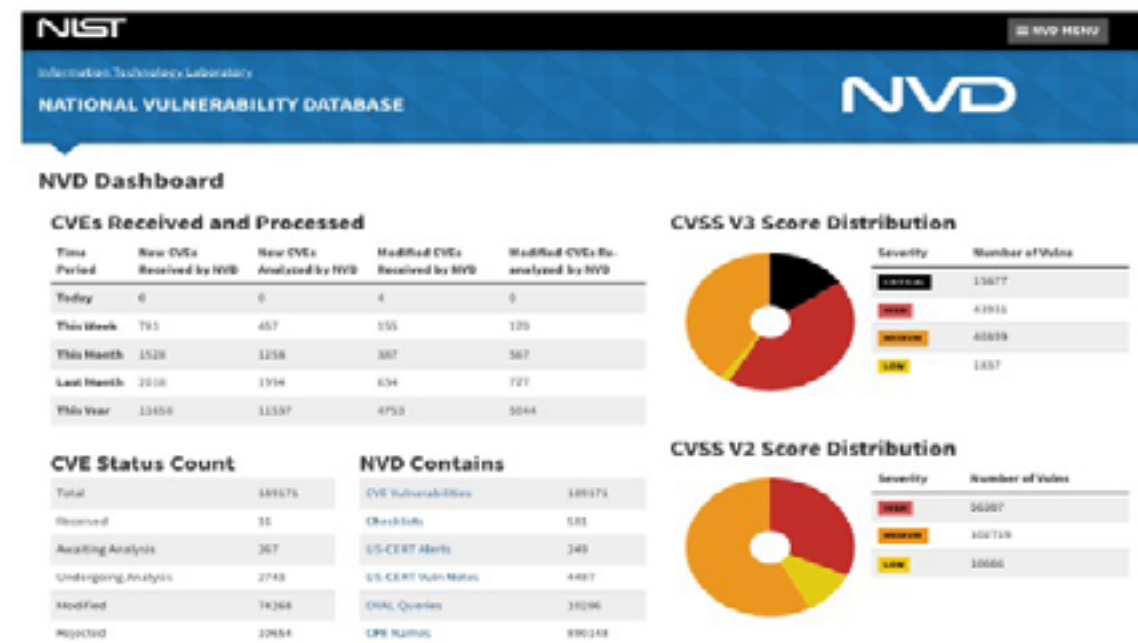
National Vulnerability Database (NVD)

<https://nvd.nist.gov/general/nvd-dashboard>

TOTAL CVE #214187 → Updated!

CVE Status Count

Total	214187
Received	5
Awaiting Analysis	258
Undergoing Analysis	359
Modified	72126
Deferred	115
Rejected	12437



#sanita2030

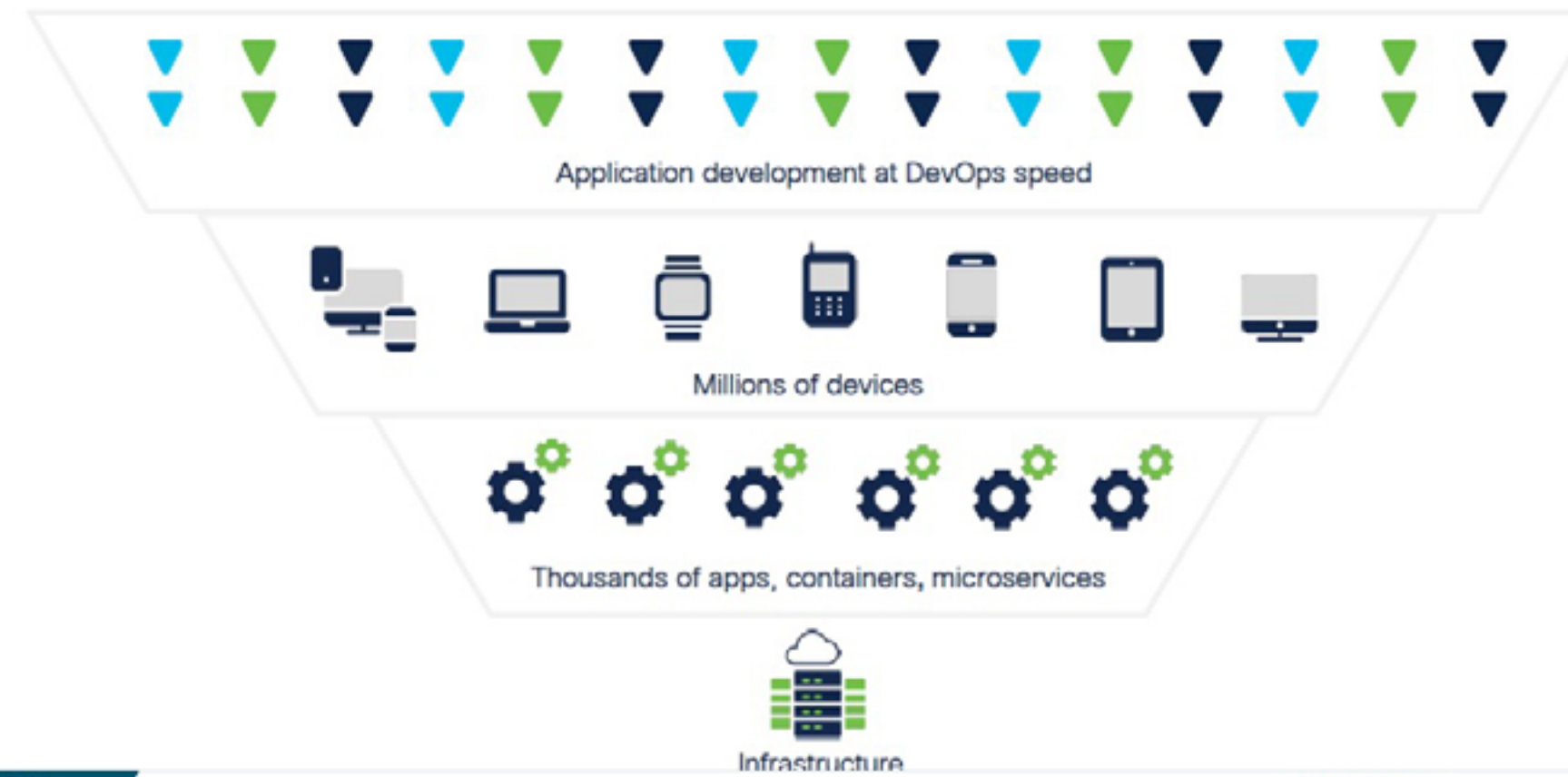


www.sanita2030.it





And it's going to get worse...5G, OT, IoT, IoE...



#sanita2030






www.sanita2030.it







CYBER SECURITY PRIORITIES

- #1**

IMPROVE PATIENTS CARE
Leveraging technologies as Telemedicine to improve home assistance and patients' care while ensuring privacy and data protection.
- #2**

INVEST IN WORKFORCE FORMATION
Addressing the workforce shortage providing by means of region-sponsored security training and partnerships with local universities and vocational school.
- #3**

ENSURE THIRD PARTY SECURITY
Addressing third party risks, especially IoT providers, by identifying trustworthy vendors approved at regional level and defining minimum requirements they should meet.

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](#)