Dispostivi elettromedicali e cybersecurity, stato del rischio e best practice

17 Maggio 2024
Antonio Scarfò Local Public Administration Italia

AIIC 2024 ROMA

Securing People, Devices, and Data Everywhere

Founded: **October 2000**

Founded by: **Ken Xie and Michael Xie**

Headquarters: **Sunnyvale, CA**

Fortinet IPO (FTNT): **November 2009**

Listed in both: **NASDAQ 100 and S&P 500**

Member of: **2022 Dow Jones Sustainability World and North America Indices**

Security Investment Grade Rating: **BBB+ Baa1**

For over 20 years, Fortinet has been a driving force in the evolution of cybersecurity and the convergence of networking and security. Our security solutions are among the most deployed, most patented, and most validated in the industry.

Antonio Scarfò Local Public Administration Italia

Global Customer Base

705k+

Customers

Broad, Integrated Portfolio of

50+

Enterprise Cybersecurity Products

2022 Billings

$5.59B+

(as of Dec 31, 2022)

Strong Analyst Validation

70+

Enterprise Analyst Report Inclusions

Market Capitalization

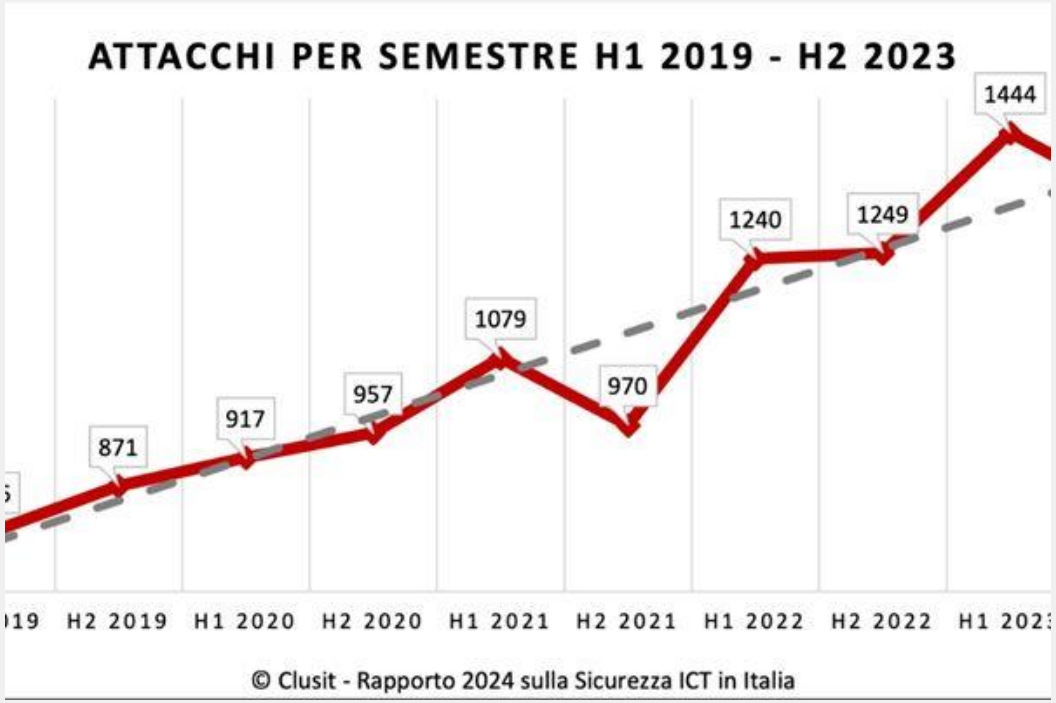
$45.5B

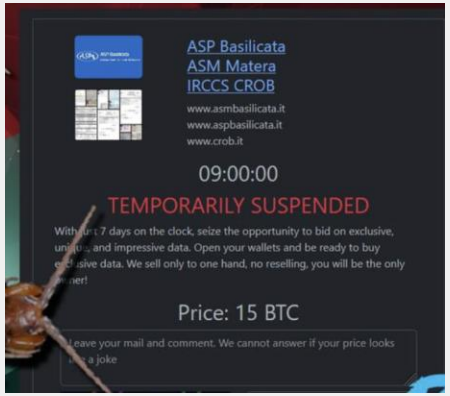
(as of March 31, 2023)

Vertical Integration

$1B+

Investment in ASIC Design & Development

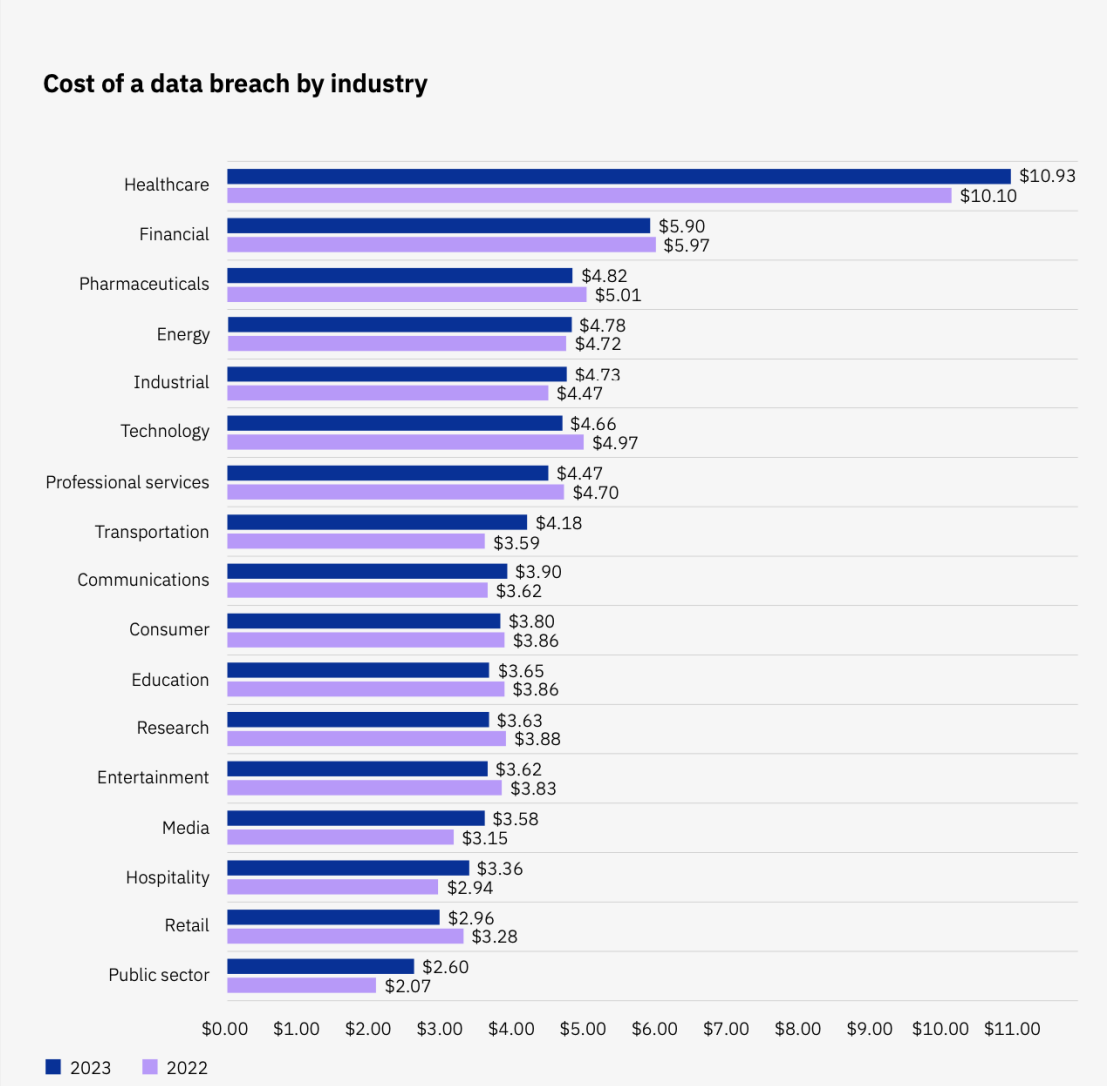




Cost of a data breach by industry

	2023	2022
1 ↑	**Healthcare** USD 10.93 million	**Healthcare** USD 10.10 million
2 ↓	**Financial** USD 5.90 million	**Financial** USD 5.97 million
3 ↓	**Pharmaceuticals** USD 4.82 million	**Pharmaceuticals** USD 5.01 million
4 ↑	**Energy** USD 4.78 million	**Technology** USD 4.97 million
5 ↑	**Industrial** USD 4.73 million	**Energy** USD 4.72 million

Cost of data breaches report 2023, IBM



Why Healthcare

Private patient information is worth a lot of money to attackers

Medical devices are an easy entry point for attackers

Staff need to access data remotely, opening up more opportunities for attack

Workers don't want to disrupt convenient working practices with the introduction of new technology

Healthcare staff aren't educated on online risks

The number of devices used in hospitals makes it hard to stay on top of security

Healthcare information needs to be open and shareable

SYSTEM FAILURE

SYSTEM FAILURE

In September 2022, the FBI reported that **53%** of hospital digital medical devices and other internet-connected products had known **critical vulnerabilities.**

IV pumps are the most commonly used healthcare IoT device, making up around 38% of a hospital's IoT footprint. It is these devices that were found to be the most vulnerable to attack, with **73% having a vulnerability that could threaten patient safety, service availability,**

There are more than **15 million medical devices in US hospitals** with an average of 10 to 15 connected devices per patient bed. The global number of connected medical devices is on track to exceed **50 billion in the next decade.**

THE HIPAA JOURNAL

Cynerio

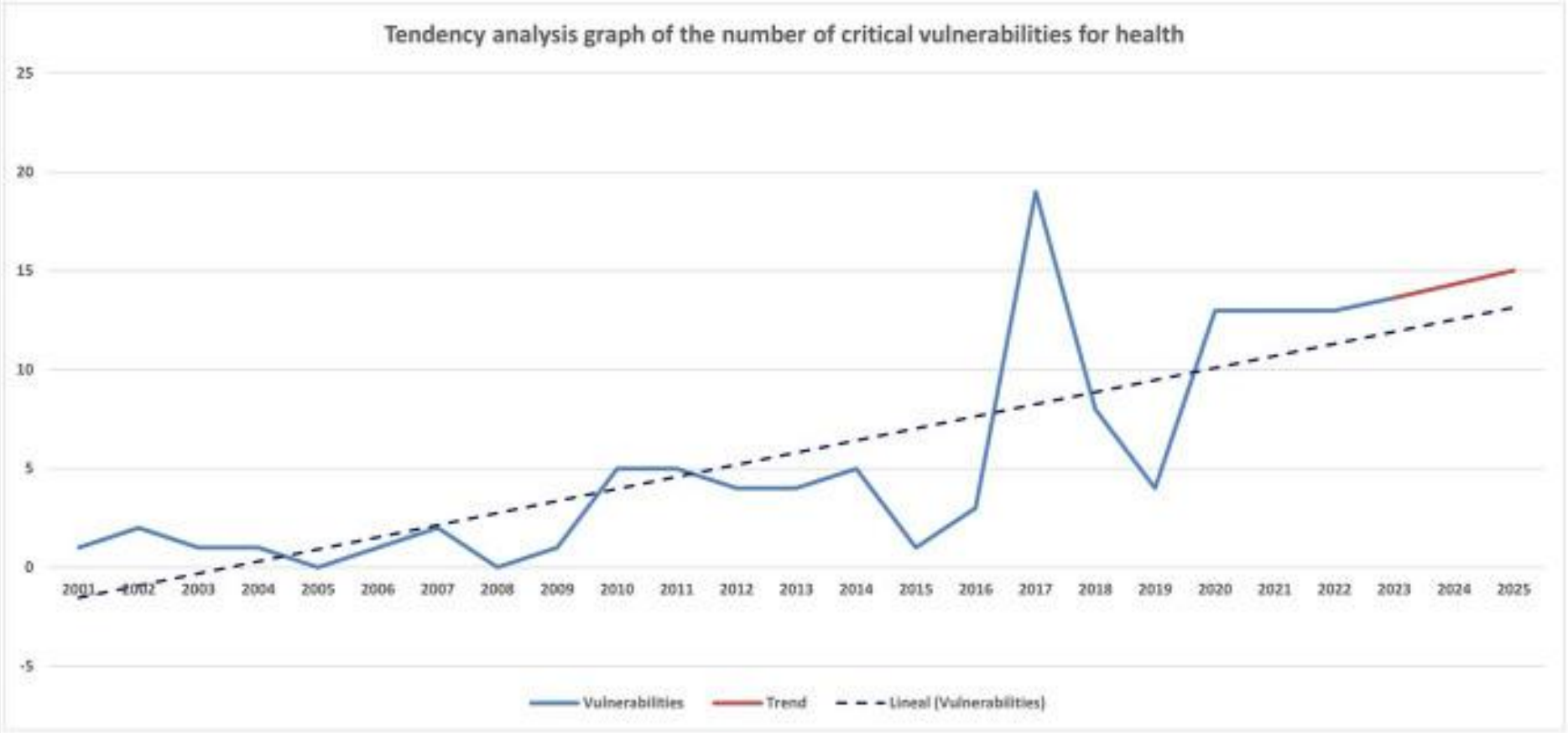
Medical Devices

- August 2017, the FDA recalled approximately **465,000 implantable cardiac devices** due to vulnerabilities that could cause serious issues for patient safety.
- In June 2019, the Food and Drug Administration recalled a kind of **insulin pump** with more than **4.000** implants that allowed a change set by an unauthorized person connecting via wireless.
- In November 2019, more than **1.000 insulin pump** remote controllers were recalled

Forbes

May 2017, Medical Devices Hit By Ransomware For The First Time In US Hospitals

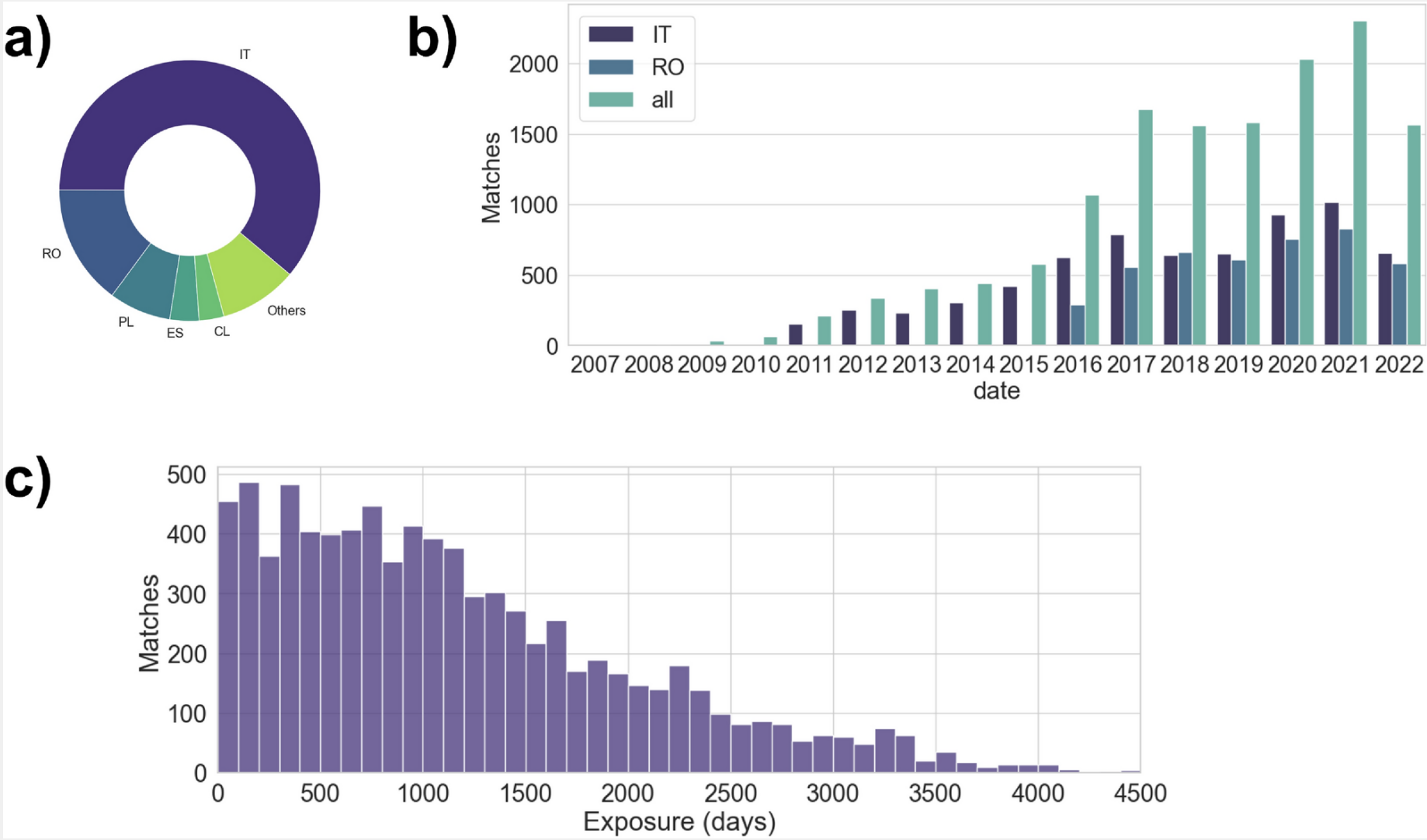
Vulnerabilities Analysis



Granada et al 2024 NIH

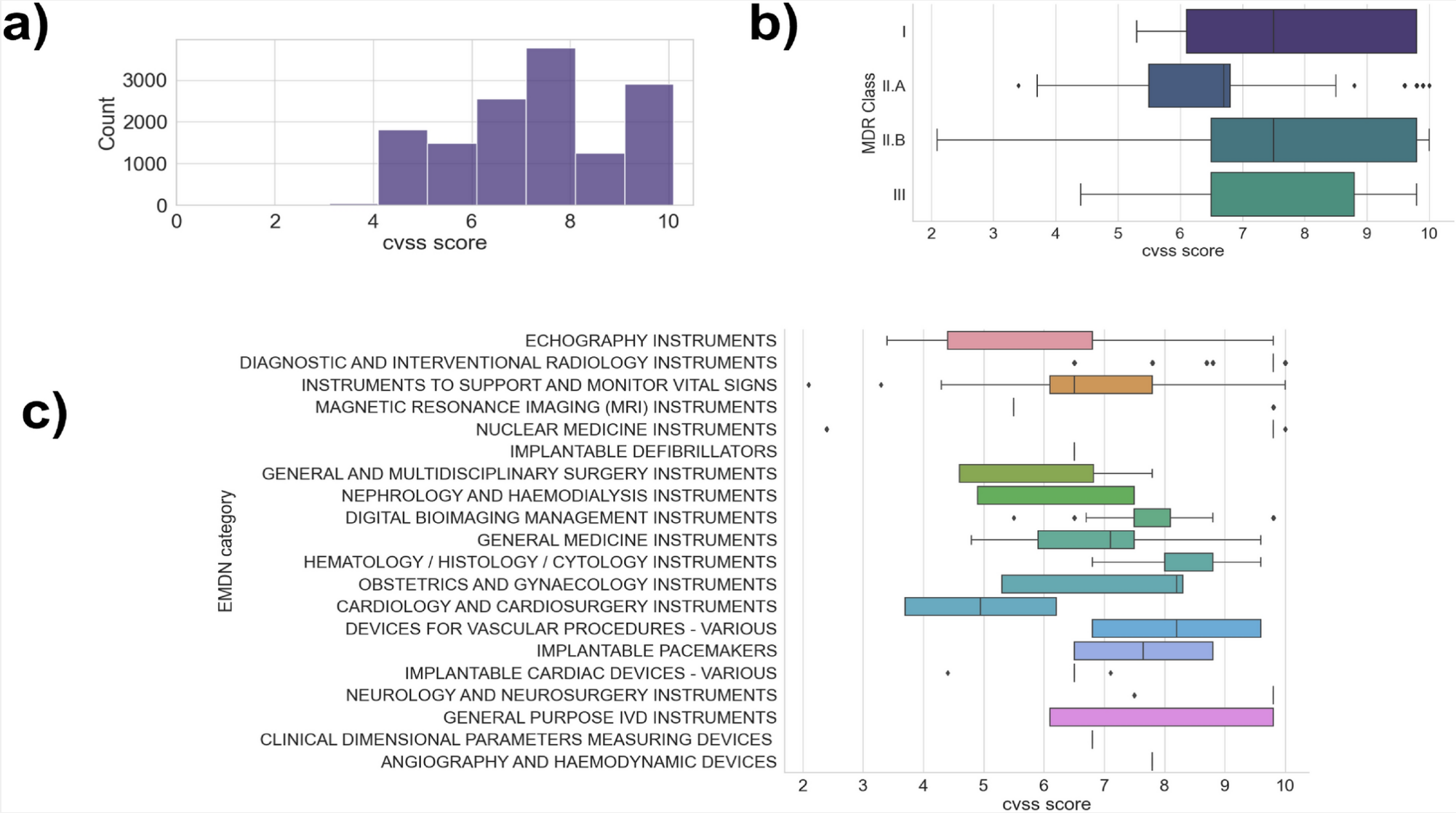
Vulnerabilities Analysis

- 1241 healthcare facilities
- 92 million public administration purchases
- 36 countries over a decade
- Open Contracting Data Standard (OCDS)



Bracciale, L., Loreti, et al. Nature 2023

Vulnerabilities Analysis



Bracciale, L., Loreti, et al. Nature 2023

NIS2 fundamental news

New Organizational Requirements

- Risk Management
- Corporate Accountability
- Reporting Obligations
- Business Continuity

SHARED RESPOSABILITY MODEL (Supply Chain) – CLOUD/IOT/IOMT SECURITY

Minimum Measures

- Risk Assessment
- Cryptography and encryption
- Vulnerability Management
- Data/Access Control
- Multi-Factor Authentication
- Evaluating the Security Measures
- Incident handling
- Cybersecurity Training
- Business Operation plan during/after incident
- Security around supply chains

Risks (Probability/Severity of harms), IT Security (protection of IT infrastructures), Information Security (CIA), Operational Security (protection of procedures and workflows) and the basic principle of **Safety** and **Effectiveness**.

2017

25 May 2017:
The MDR comes into force.

2019-2022

2019 – 2022:
Medline starts preparing by:
- Uniquely identifying devices
- Updating labelling
- Updating our quality management system
- Updating all of our technical files (class I, IIa and IIb, sterile and non-sterile)
- Working with our SPT component producers to ensure they receive their certificates.

2021

26 May 2021:
New devices and existing devices without an MDD/ AIMDD certificate must meet MDR requirements.

2022

July 2022:
Medline successfully completes its BSI audit to verify MDR compliance.

2023

2023:
Medline anticipates receiving all MDR certificates (1 year ahead of schedule).

2024

27 May 2024:
Devices may only be marketed under MDR certificates.

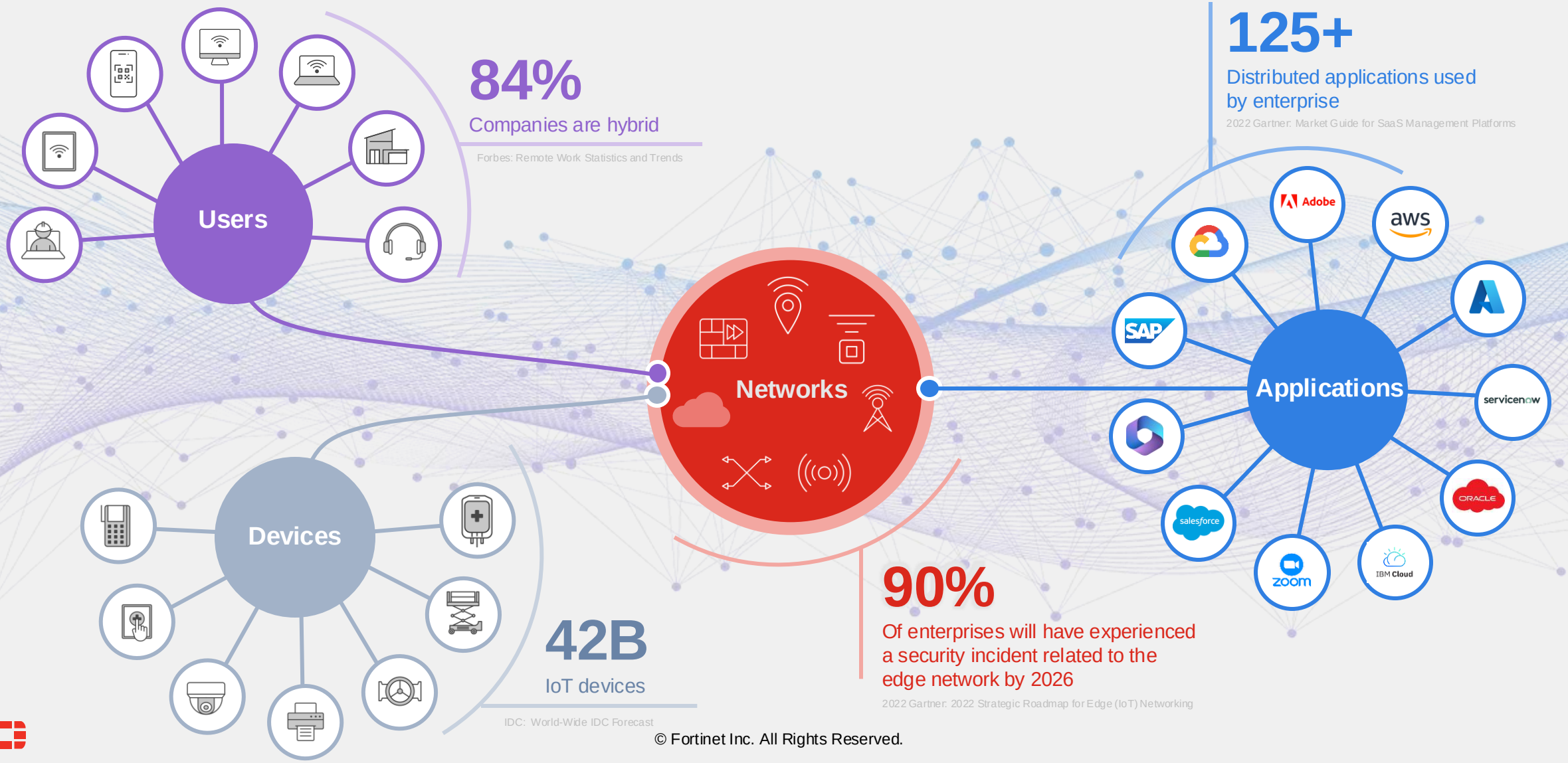
2025

27 May 2025:
Devices with an MDD certificate may no longer be sold.

SHARED RESPOSABILITY MODEL – IOT/IOMT SECURITY

Part 2 – Protection			
2.1	**IT Security Architecture**	Systems configuration	• **Operating environment must not hinder the application of security measures on the medical device or force the device to operate in lower security settings.** • **Session management measures (e.g. session timeouts).** • **Operating system hardening and application whitelisting** • **Antivirus / anti-malware software** • **Use of strong passwords** • Appropriate security measures for mobile devices and teleworking
		System segregation	• **Firewall** • **Network segmentation** • **Partitioning mechanisms and traffic segmentation**
		Traffic filtering	• **Use of traffic filtering software and hardware**
		Cryptography	• **Encryption when storing sensitive personal data** • **Encryption of data in transit**
2.3	**Identity and access management**	Authentication and identification	• **User access management (credentials for accessing software applications or devices, user access policy etc.)**
		Access rights	• Apply principle of least privilege to user workstations and connected devices. • Least privileges must take into account data minimisation per role
2.4	**IT security maintenance**	IT security maintenance	• **Provisions regarding patch management** • **Support patching without compromising interoperability/compatibility**

Infrastructure Has Become More Complex and More Vulnerable to Attack



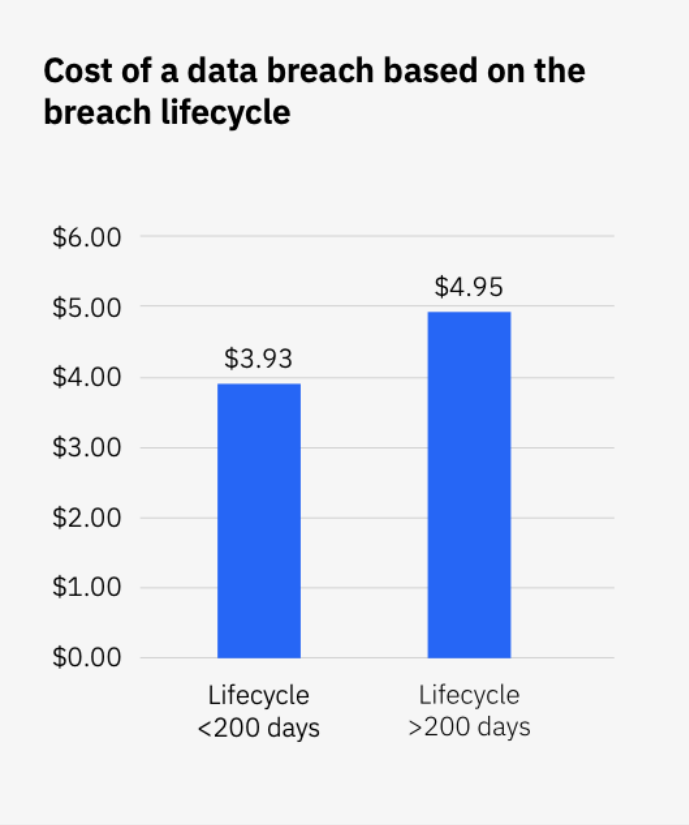
84%
Companies are hybrid
Forbes: Remote Work Statistics and Trends

125+
Distributed applications used by enterprise
2022 Gartner: Market Guide for SaaS Management Platforms

90%
Of enterprises will have experienced a security incident related to the edge network by 2026
2022 Gartner: 2022 Strategic Roadmap for Edge (IoT) Networking

42B
IoT devices
IDC: World-Wide IDC Forecast

When Attackers Get In, They Stay Longer and Cost You More



Cost of data breaches report 2023, IBM

+ Automation (AI)
+ IR
+ Training

- Complexity
- Skill shortage
- Noncompliance

Tech Strategy – Medical Devices Security Architecture

Operation Center

AI

SIEM

CSIRT SOC Regionale ACN Cyclone

Alerts

Business Services Dashboard

Analisi Traffico

Servizi Cloud

Servizi Locali

Segmenti di rete

SdWan

Deceptor

Log

Retroazione

NGFW

Monitoraggio Remoto

Rete Locale

Network Access Control

Tag servizio

IAM-PAM

MDR

Segregazione della rete

Gestione delle identità

Early Detection

Database elettromedicali

Automazione

Rete Locale