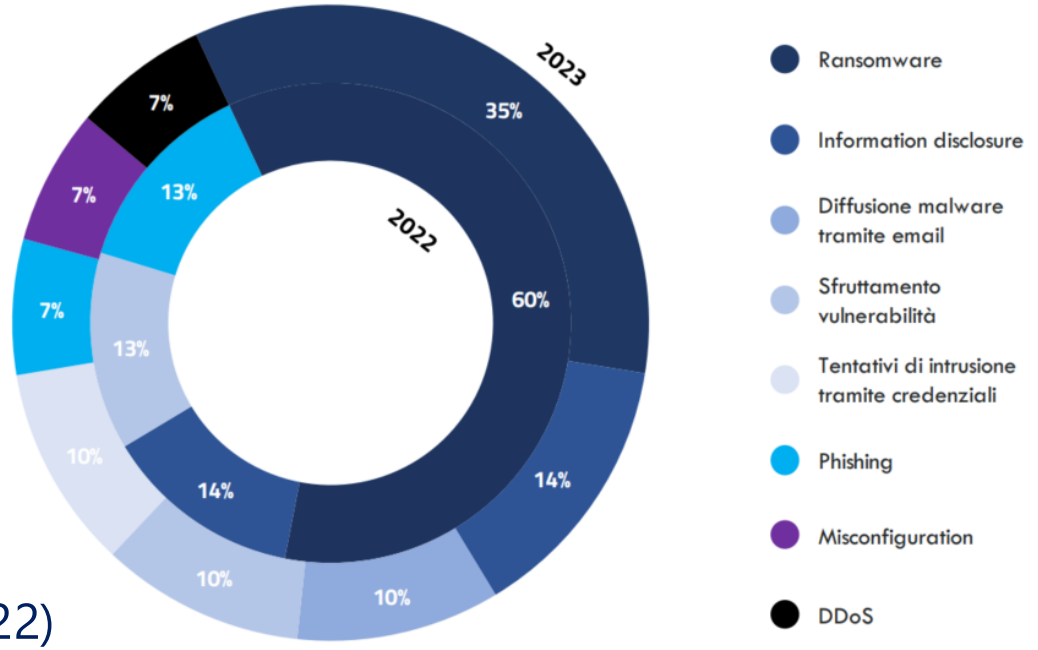
Sanità e Cybersecurity: strategia Zero Trust per un futuro sicuro

Giuseppe Di Pasquale
Senior Sales Engineer - Fortinet

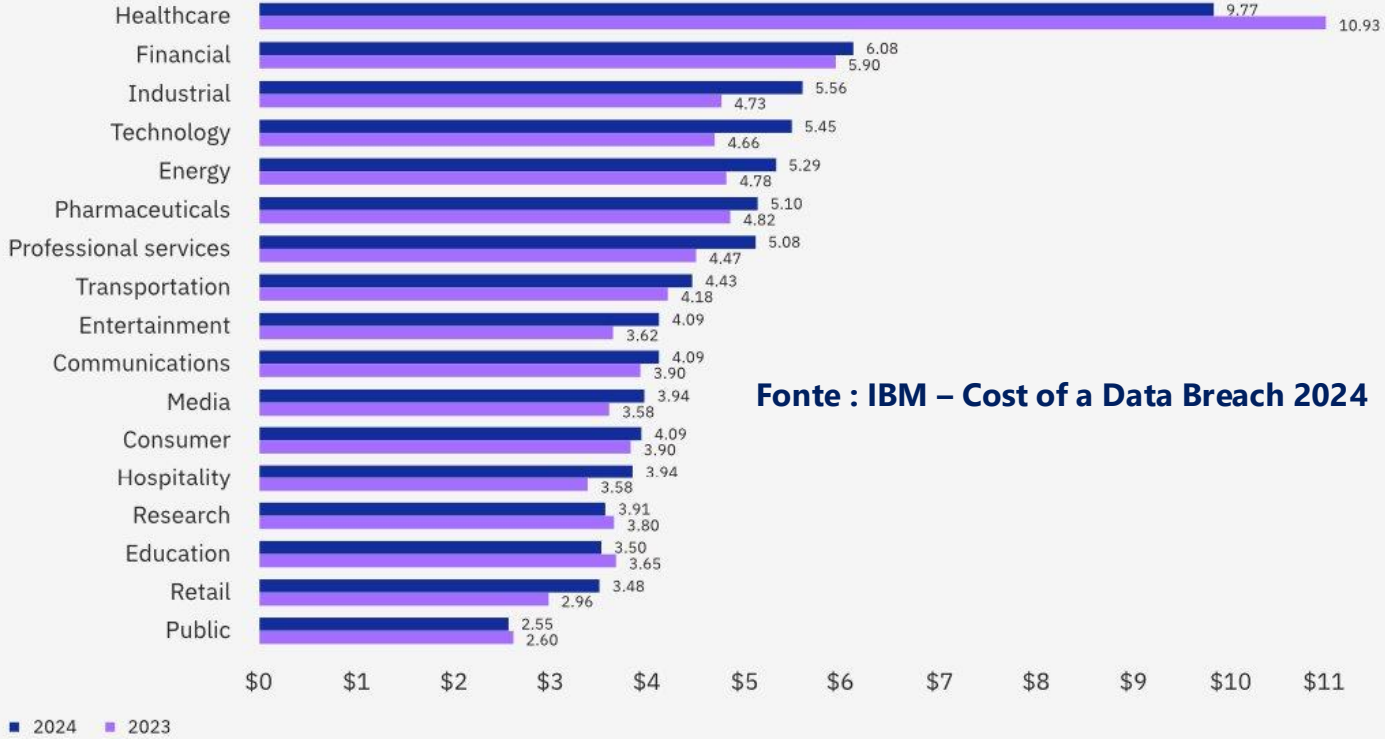
Qualche numero in Italia...

- almeno 2 eventi/mesi (2022-2023)
- totale di 45 eventi (50% aumento dal 2022 al 2023)
- percentuale eventi cyber confermati : 47% (21 incidenti)
- incidenti causati da ransomware : 35% (2023) – 60% (2022)
- 2.178 IP esposti



Fonte : ACN – La minaccia cibernetica al settore sanitario – Settembre 2024

E nel mondo...



Fonte : IBM – Cost of a Data Breach 2024

Cost of a data breach by country or region

#	Country	2024	2023
1	United States	$9.36	$9.48
2	Middle East	$8.75	$8.07
3	Benelux	$5.90	–
4	Germany	$5.31	$4.67
5	Italy	$4.73	$3.86
6	Canada	$4.66	$5.13
7	United Kingdom	$4.53	$4.21
8	Japan	$4.19	$4.52
9	France	$4.17	$4.08
10	Latin America	$4.16	$3.69
11	South Korea	$3.62	$3.48
12	ASEAN	$3.23	$3.05
13	Australia	$2.78	$2.70
14	South Africa	$2.78	$2.79
15	India	$2.35	$2.18
16	Brazil	$1.36	$1.22

Figure 2A. Measured in USD millions

La sanità, un'azienda «speciale»...

- Dati sensibili e critici per la salute
- Target preferito per attacchi mirati e ransomware
- Dipendenza da dispositivi connessi (IoMT)
- Regolamentazioni più stringenti e obblighi di conformità
- Personale con diversi livelli di consapevolezza e formazione

Benefici VS Rischi

Benefici dell'IT nella sanità	Rischi e Minacce Cyber Associati
Continuità e qualità delle cure	Interruzione operativa (Ransomware)
Accesso rapido ai dati dei pazienti	Violazioni dei dati
Diagnosi e trattamenti più efficienti	Manomissione dei dispositivi IoMT
Facilità di collaborazione tra medici	Condivisione insicura dei dati
Telemedicina e accesso remoto alle cure	Aumento della superficie di attacco

Zero Trust Access

Verifica per sessione

Controlli identità utente

- MFA / Passwordless
- Single Sign-on
- Luogo
- Orario
- Ruolo

Controlli device

- Identità
- Versione OS
- A/V status
- Vulnerability assessment

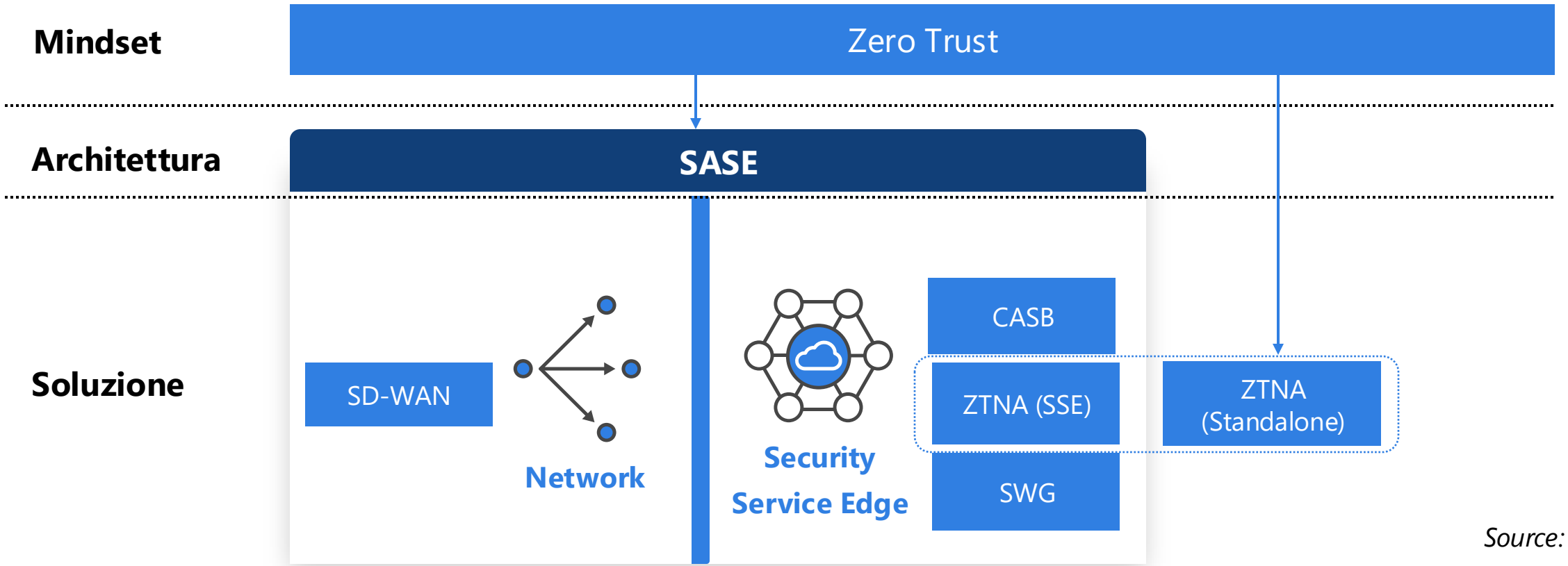
Verifica continua

- Postura Device
- Comportamento utente
- Risk Scoring

Controllo granulare

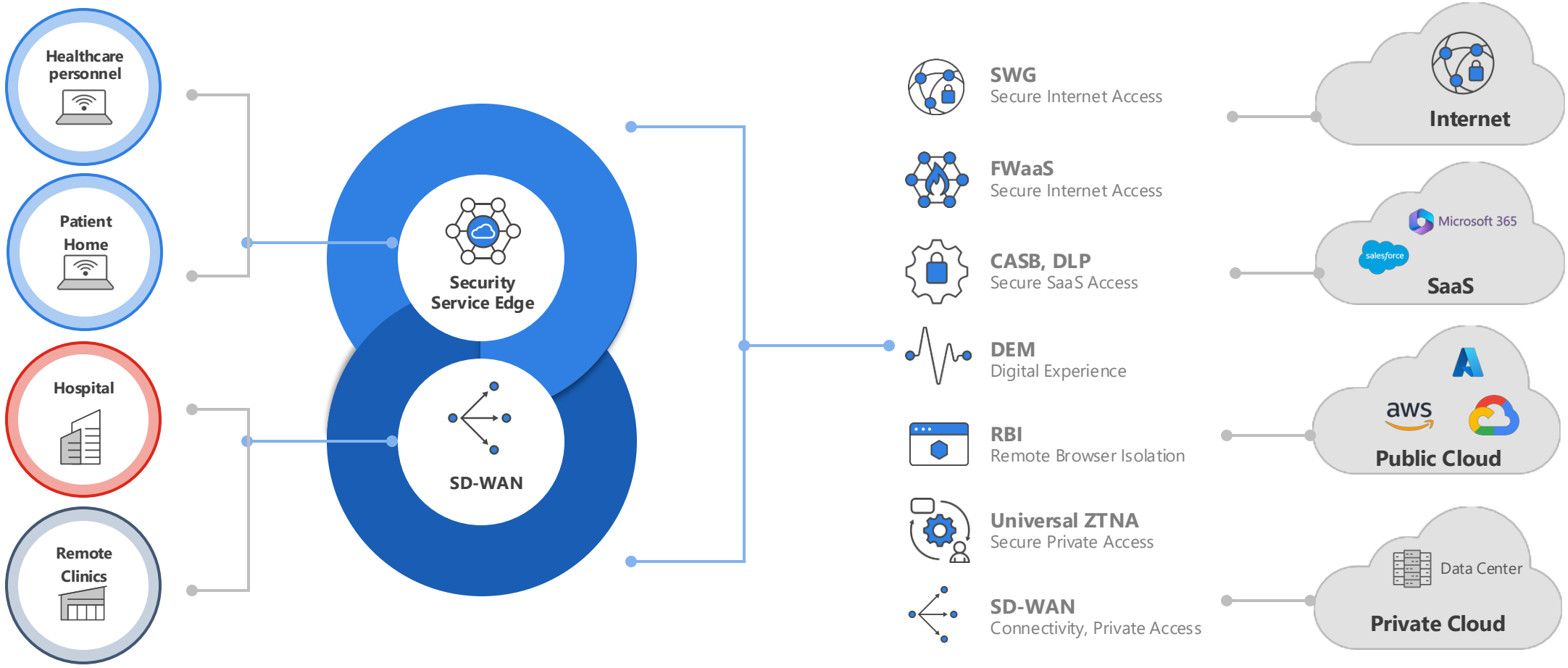
- Accesso autorizzato solo a determinate applicazioni
- Accesso autorizzato solo a determinate porzioni di rete

SASE & Zero Trust



Source: Gartner

SASE & Zero Trust



2025 e considerazioni finali

- Crescita della specializzazione nella catena di attacco
- Automazione nel crimine informatico
- Combinazione di minacce digitali e fisiche
- AI per migliorare la risposta alle minacce

- Effettuare una valutazione del rischio
  - Proteggere supply chain sanitaria
- Implementare un approccio Zero Trust
- Sfruttare il modello SASE per unire sicurezza e accesso remoto
- Formare il personale e promuovi la cyber hygiene

Fonte : Fortiguard Labs - Cyberthreat Predictions for 2025

https://www.fortinet.com/blog/threat-research/threat-predictions-for-2025-get-ready-for-bigger-bolder-attacks

Immaginate un futuro sicuro ?