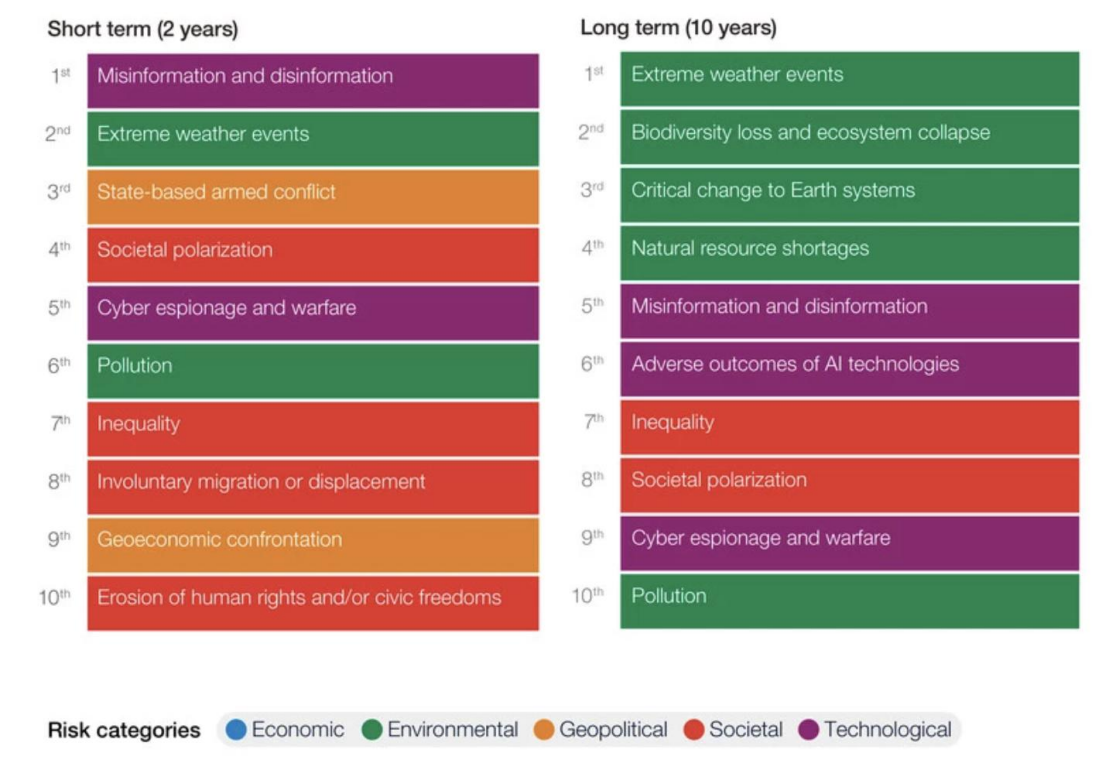
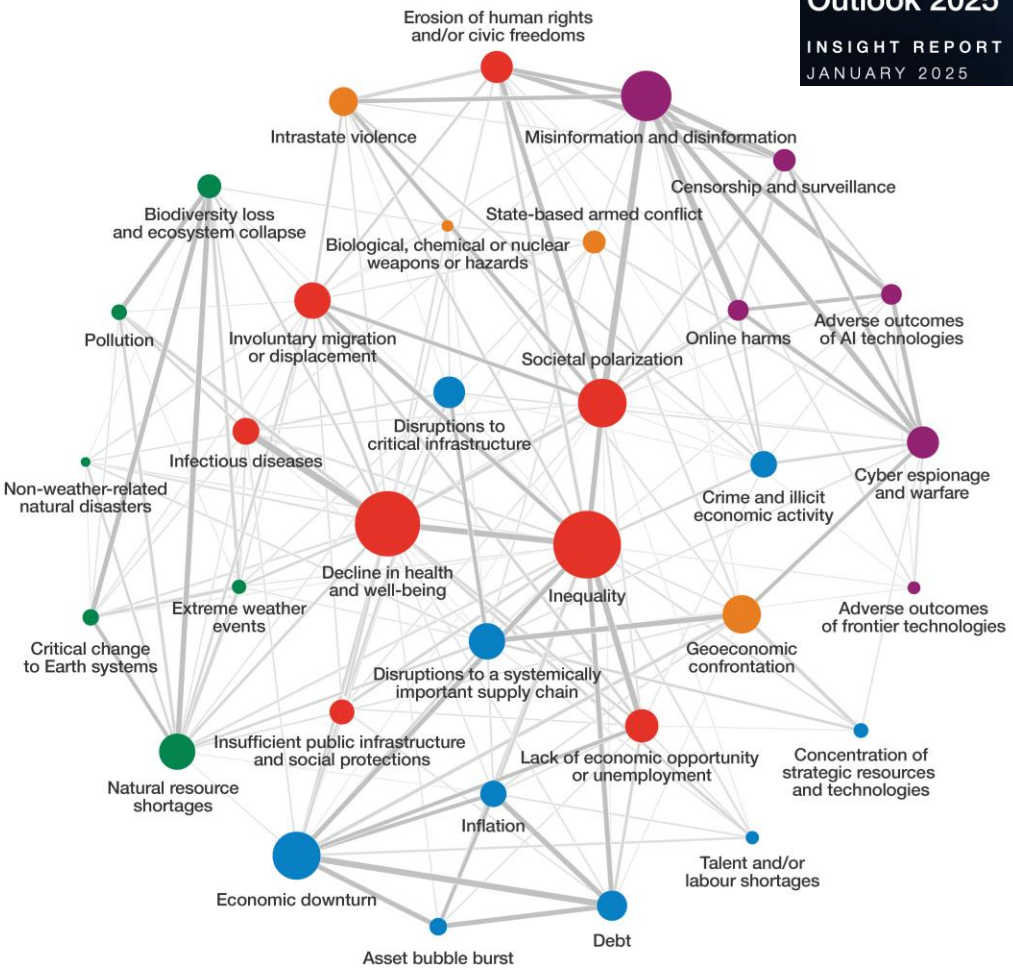
Sicurezza cibernetica e aerospaziale

Antonio Scarfò
Resposabile mercati Local Government, Healthcare and Education

Minacce e dipendenze WEF 2025

Diversi fenomeni, tra cui le tensioni politiche e l'avvento massivo dell'AI stanno complicando notevolmente lo scenario del cyberspace



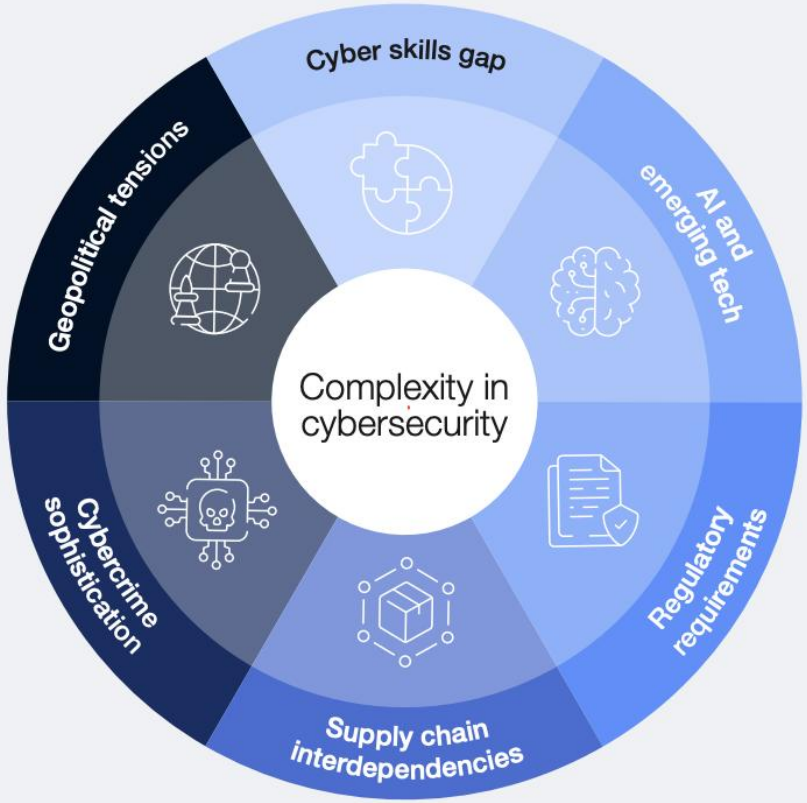


World Economic Forum

Global Cybersecurity Outlook 2025
INSIGHT REPORT
JANUARY 2025

Il 63% delle organizzazioni ha citato il panorama delle minacce complesso e in continua evoluzione come la sfida più grande per diventare resilienti dal punto di vista informatico. Complessità all'intersezione tra IT e OT

Factors compounding the complex nature of cybersecurity



Geopolitical tensions

Geopolitical tensions are an influence on cyber strategy in nearly 60% of organizations, with one in three CEOs citing cyber espionage and loss of sensitive information/IP as top concerns.

Cybercrime sophistication

72% of respondents say cyber risks have risen in the past year, with cyber-enabled fraud on the rise, an increase in phishing and social engineering attacks and identify theft becoming the top personal cyber risks.

Supply chain interdependencies

With 54% of large organizations citing third-party risk management as a major challenge, supply chain challenges remain a top concern for achieving cyber resilience.

Regulatory requirements

78% of leaders from private organizations feel that cyber and privacy regulations effectively reduce risk in their organization's ecosystems. However, two-thirds of respondents cited the complexity and proliferation of regulatory requirements as a challenge.

AI and emerging tech

66% of respondents believe that AI will affect cybersecurity in the next 12 months, but only 37% have processes in place for safe AI deployment.

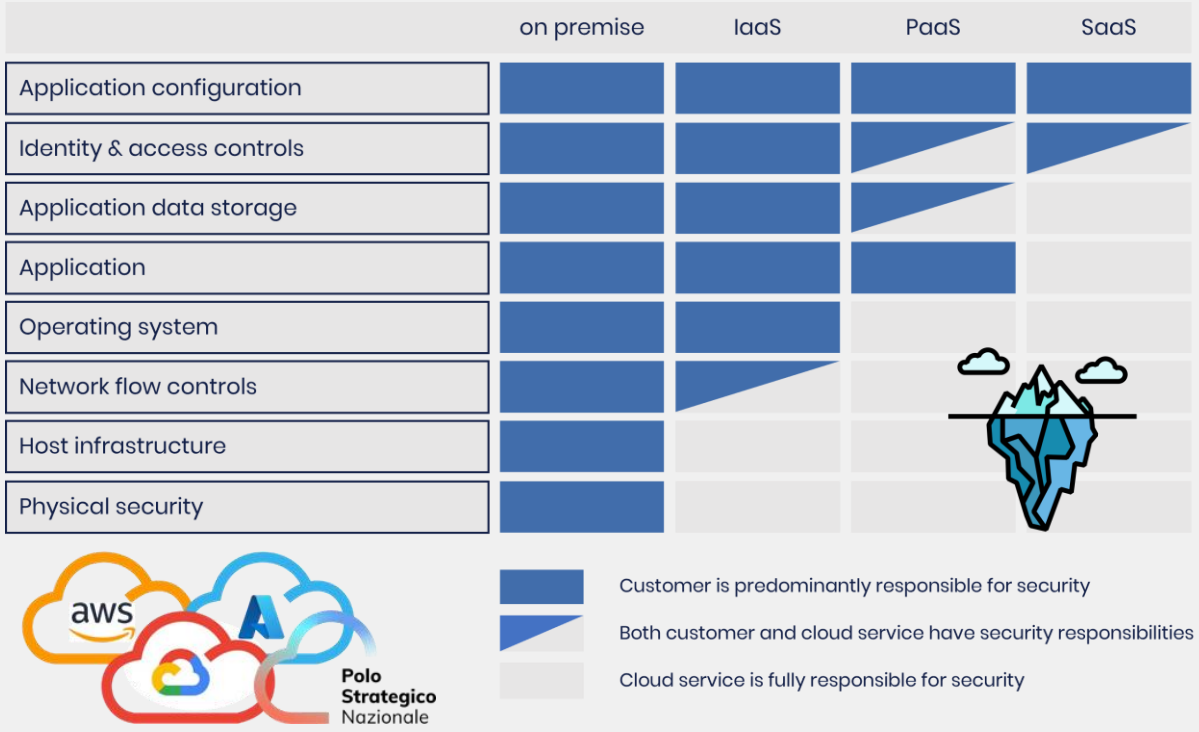
Cyber skills gap

The cyber skills gap has widened since 2024, with two in three organizations reporting moderate-to-critical skills gaps. Only 14% of organizations are confident that they have the people and skills required.

Non solo la rete

L'hacker collegato all'intrusione in Oracle Cloud minaccia di vendere dati rubati- Cybersecurity dive
Westpole-PA Digitale – digital360

ENISA prevede che la **prima** minaccia nel 2030 proverrà dal codice sviluppato dai fornitori e dalla sue dipendenze



Polo Strategico Nazionale

IoT

IoMT

Cloud Native AI Code

Supporto e Manutenzione

MSSP

La Minaccia dalla Supply Chain

- +30% YoY attacchi via Supply Chain
- 66% degli attacchi avviene attraverso il codice sviluppato dai fornitori
- 62 % degli attacchi via Supply Chain si basa sulla fiducia verso i fornitori
- 66% dei casi le aziende vettore dell'attacco non sono consapevoli o non dichiarano la compromissione

NIS2-Dl/138

Evoluzione della resilienza cyber

Gartner

Gartner Research

SD-WAN Is Killing MPLS, So Prepare to Replace It Now

Published: 26 September 2018

ID: G00368838

Analyst(s): Danellie Young , Neil Rickard , Mike Toussaint , Andrew Lerner

Summary

MPLS is still the leading WAN transport; however, software-defined WAN is moving users away from MPLS to hybrid and internet-only WANs. Infrastructure and operations leaders responsible for WAN design should leverage SD-WAN to improve availability and save costs, without sacrificing performance.

AgID

AGID

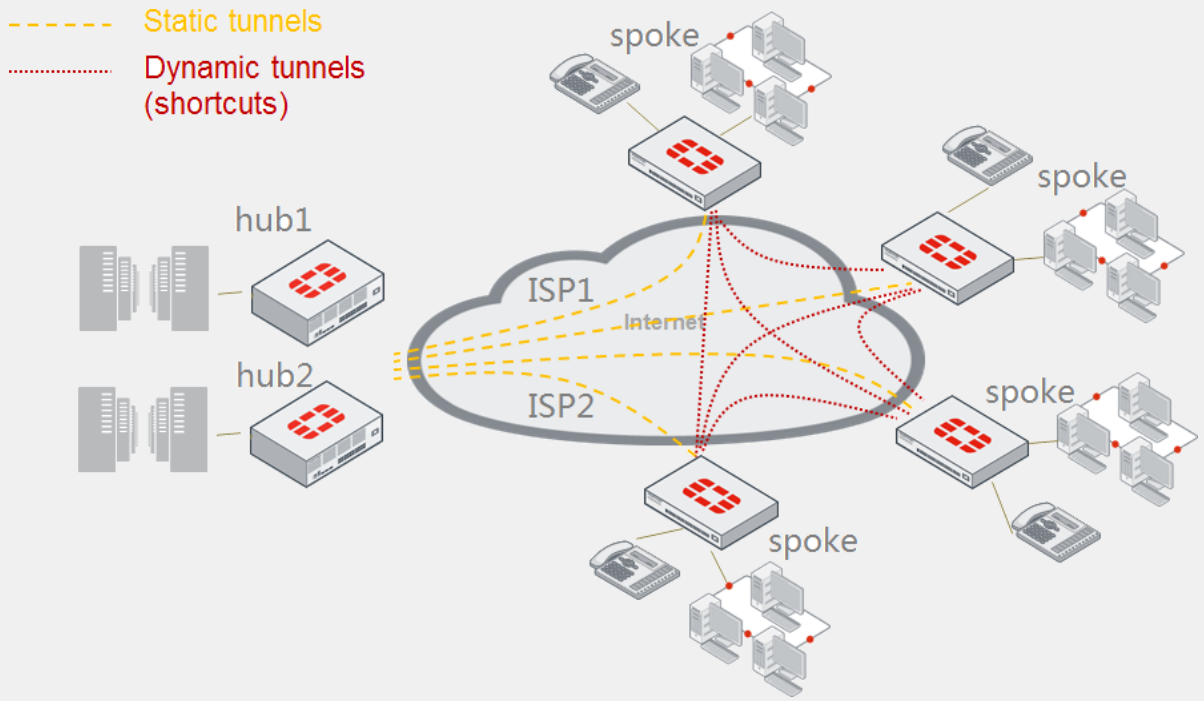
Le reti della PA (SPC) sono inadeguate, ecco come evolveranno 2017

…**La connettività pubblica è quindi ancorata ad un passato tecnologico** … Intorno al 2011-2012 si cominciò a dibattere su un nuovo paradigma a fondamento del networking, a partire da alcune ipotesi avanzate dalla Stanford University, chiamato **Software Defined Network o SDN**. Acronimo da tenere bene a mente perché probabilmente diventerà molto famoso nel giro di pochi anni

Evoluzione della resilienza cyber

Software Defined Network

1. **disaccoppia il data plane dal control plane,** e permette di astrarre il livello logico dall'hardware, rende disponibili API per programmare le funzioni di rete.
2. **l'istradamento avviene in base al tipo di flusso dati e non solo all'indirizzo di destinazione.. unifica il comportamento del device ad ogni livello a cui opera**
3. **tutta la rete è programmabile interamente e in modo estremamente flessibile** attraverso Network Application quali Firewalling, Load Balancing, Consumo energetico, QoS end to end, MPLS, virtualizzazione della rete, traffic engineering, IDS, Mobile etc. In realtà non c'è limite alle Net App



SC-6: Resource AvailabilitySC-7(20): Dynamic Isolation and Segregation

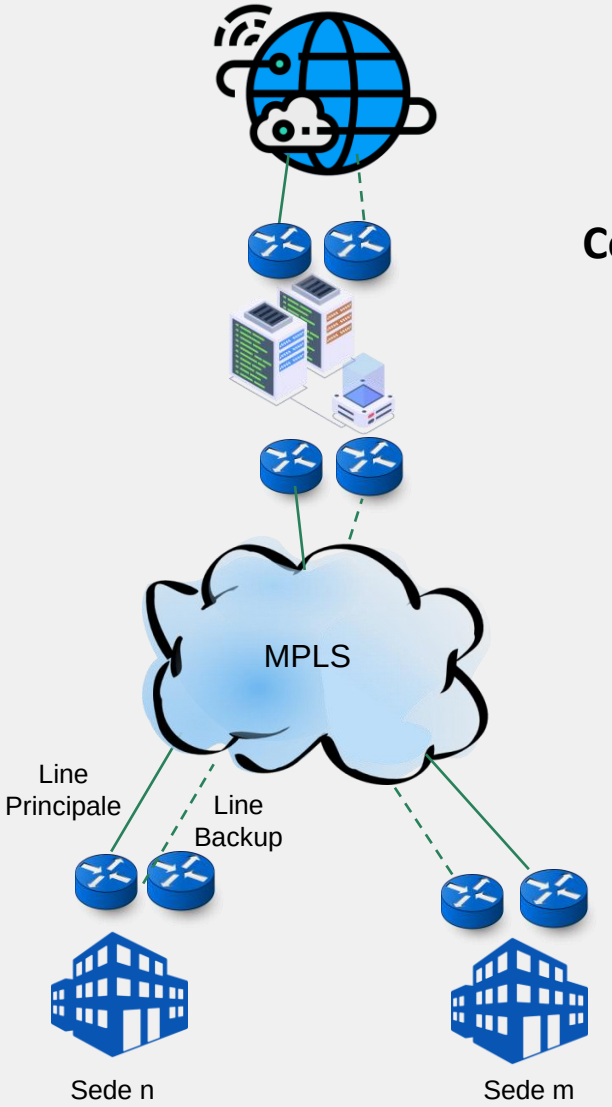
SC-7(20): Dynamic Isolation and Segregation

SC-8: Transmission Confidentiality and Integrity

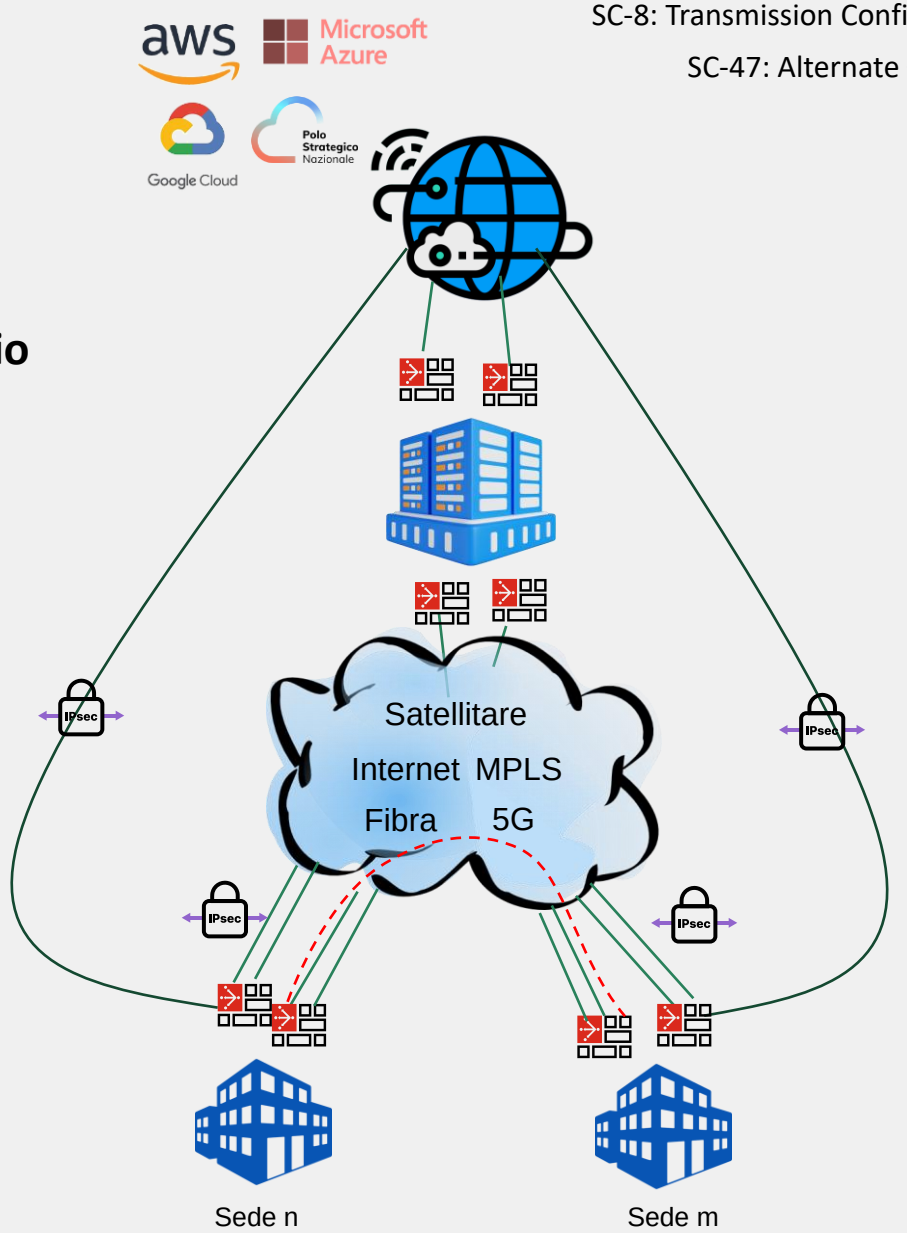
SC-47: Alternate Communications Paths

Evoluzione della resilienza cyber

Software Defined Network



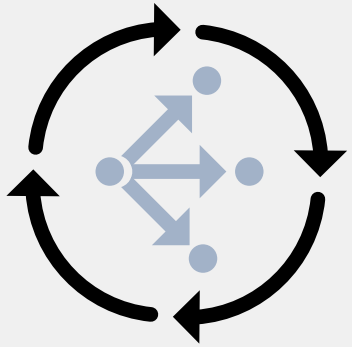
Come controllo il mio servizio di connettività?

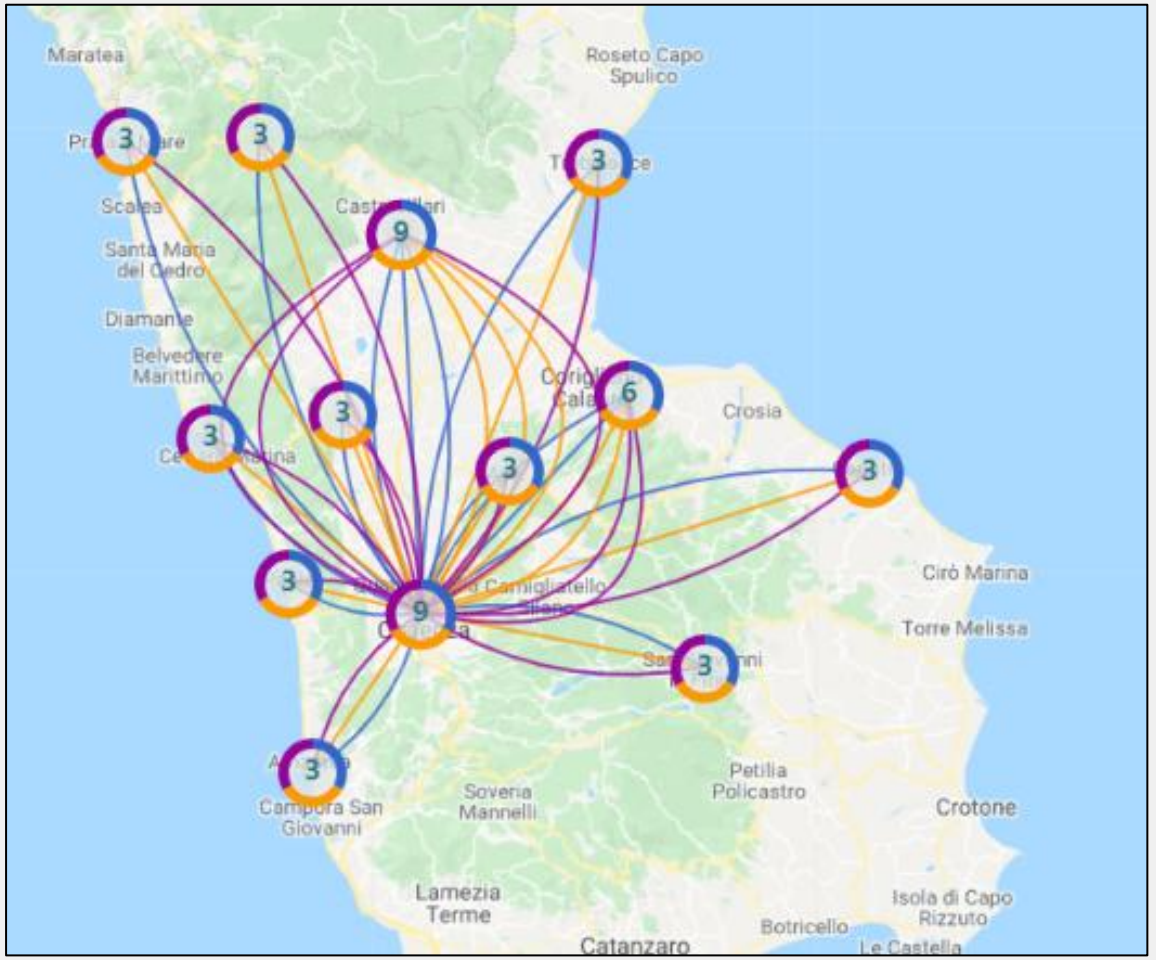


Evoluzione delle soluzioni

Software Defined Network

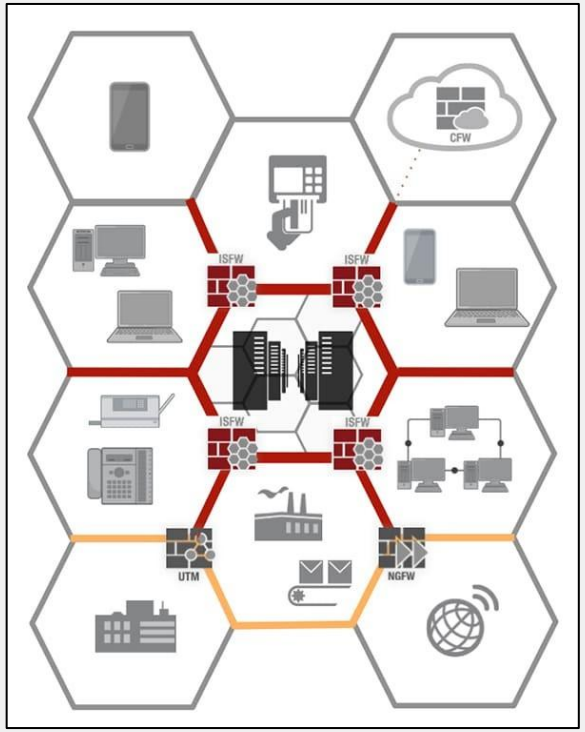
Il primo caso

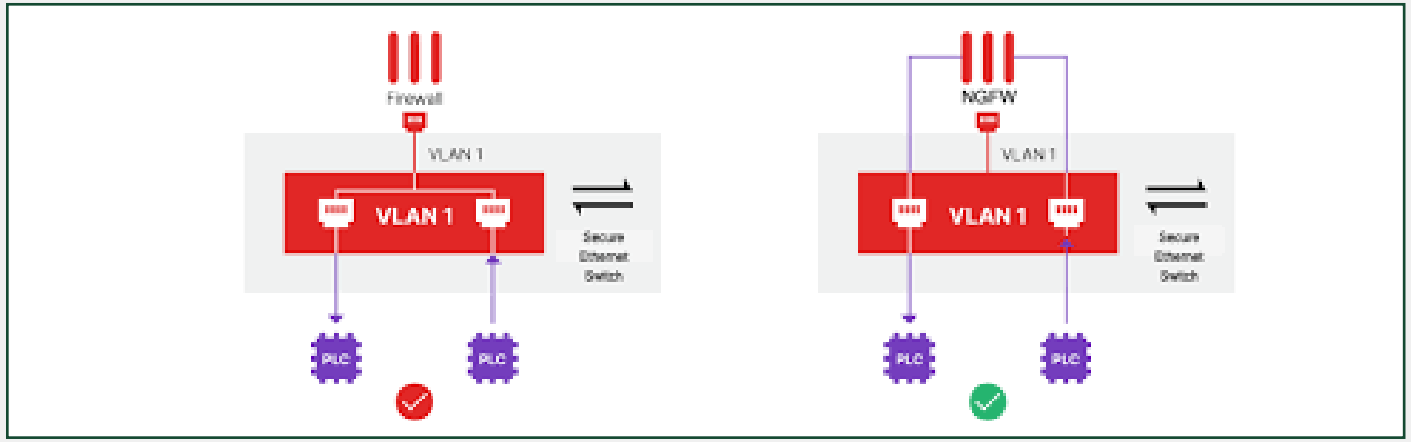


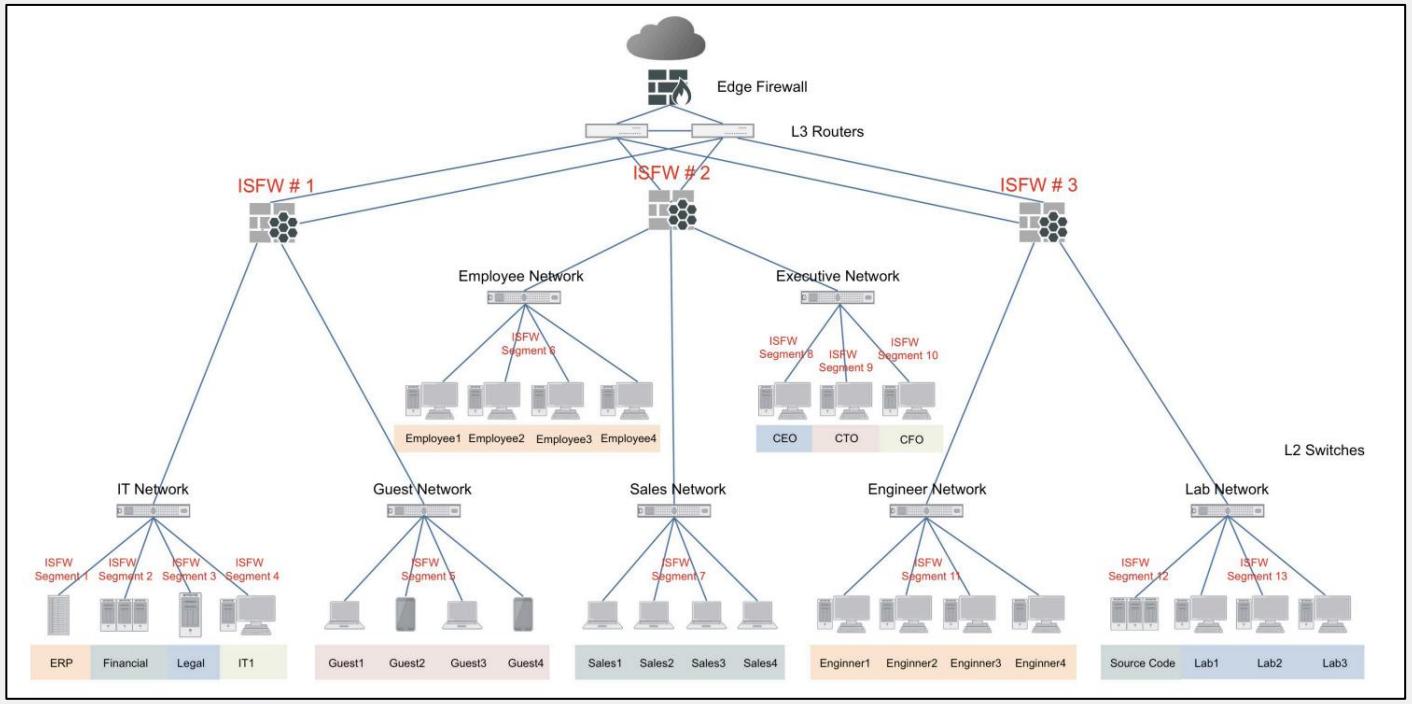


Evoluzione della resilienza cyber

Segregazione, compartimentazione

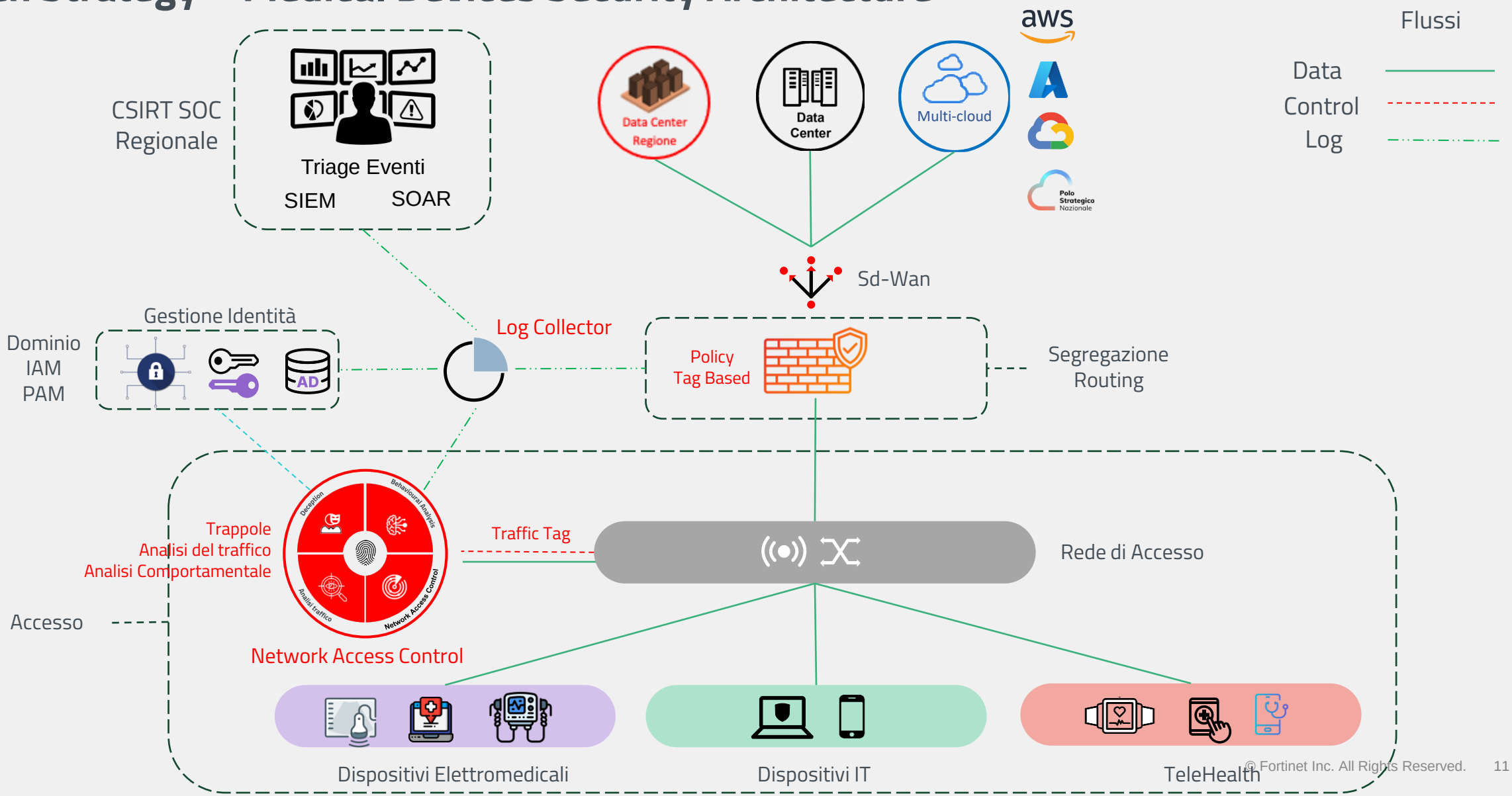






Evoluzione della resilienza cyber

Tech Strategy – Medical Devices Security Architecture



Evoluzione della resilienza cyber

Benefici dell’adozione di Sd-Wan

1. **Controllo delle prestazioni della rete in tempo reale**
2. **Sensibile aumento della qualità del servizio, della continuità del servizio e della sicurezza.**
3. **Agilità**
    a) Variazione delle politiche di sicurezza, routing e dei livelli di servizio applicazione/utenti
    b) Attivazioni e disattivazioni sedi
    c) Attivazioni/disattivazioni applicazioni
    d) Attivazioni e disattivazioni linee
4. **Risparmio sui costi delle linee**
5. **Supporto all’adozione di architetture cloud – multicloud**
6. **Abilita all’implementazione della segregazione del traffico**
7. **Completa indipendenza dall’operatore**

Resilienza – NIS2

NIS Objectives

Objective A	Objective B	Objective C	Objective D
managing security risk	Protecting against cyber attack	Detecting cyber security events enter	Minimizing the impact of cyber security incidents

NIS Principles

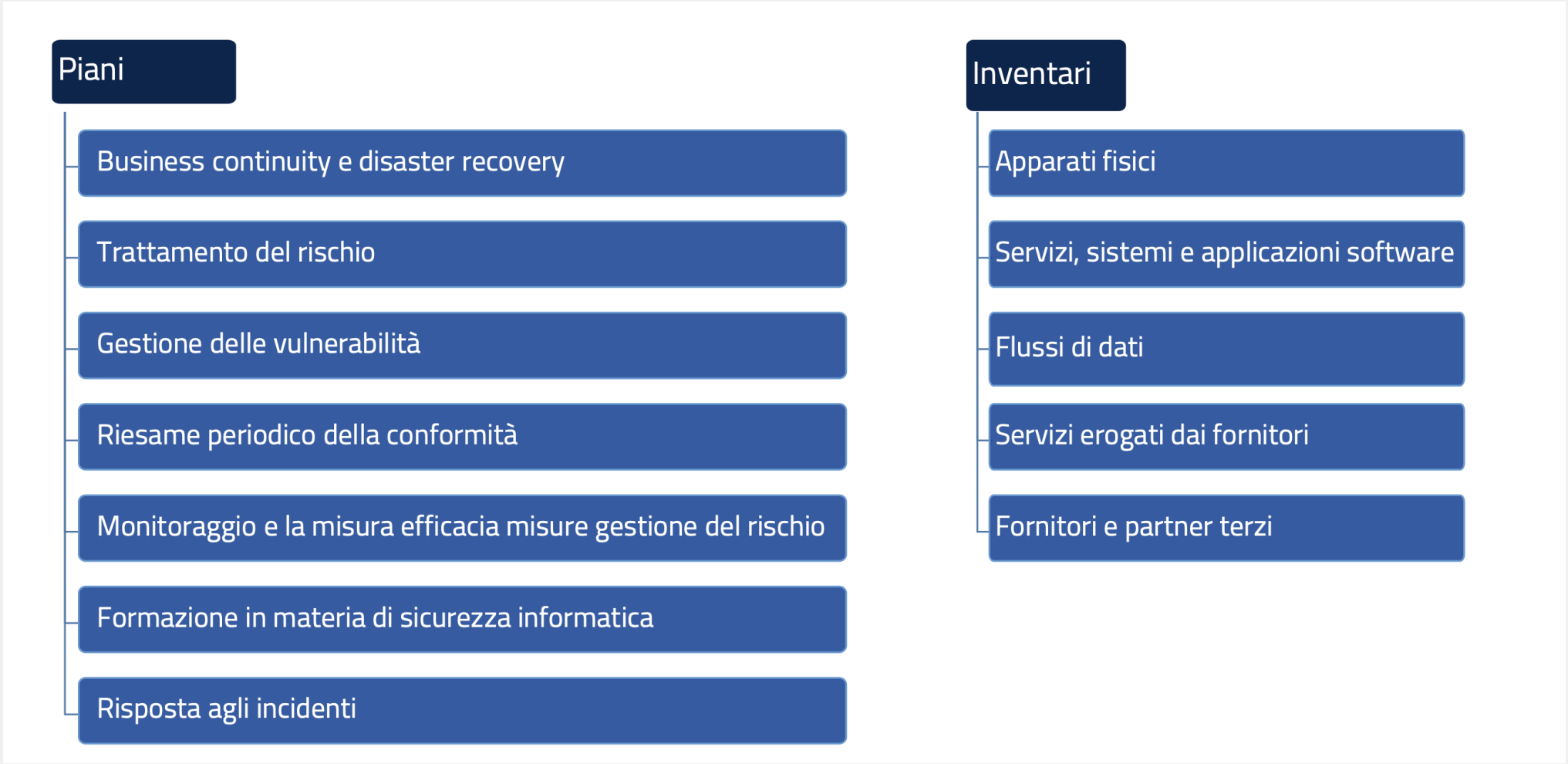
A1 Governance	**A2** Risk Management	**B1** Service Protection Policies and Processes	**B2** Identity and access control	**C1** Security Monitoring	**C2** Proactive Security event Discovery	**D1** Response and Recovery Planning	**D2** Lessons Learned
A3 Common Asset Management	**A4** Colin Supply Chain	**B3** Data Security	**B4** System Security				
		B5 Resilient Netwerk and Systems	B6 Stuff Awareness and Training Governance				

Resilienza – ACN 138/24

Ambiti di applicazione delle misure di sicurezza

Politiche di analisi dei rischi e di sicurezza dei sistemi informativi	Gestione degli incidenti	Continuità operativa, inclusa la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi	Sicurezza catena di approvvigionamento, compresi aspetti relativi sicurezza rapporti con diretti fornitori o fornitori di servizi
Sicurezza acquisizione, sviluppo e manutenzione dei sistemi informativi e di rete, ivi compresa gestione e divulgazione vulnerabilità	Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza	Pratiche di igiene informatica di base e formazione in materia di cybersicurezza	Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura
	Sicurezza risorse umane, strategie di controllo dell'accesso e gestione degli assetti	Uso di soluzioni di autenticazione a più fattori o di autenticazione continua e di sistemi di comunicazione protetti	

Resilienza – ACN 138/24



Digital Networking & Infrastructure Evolution Accelerating

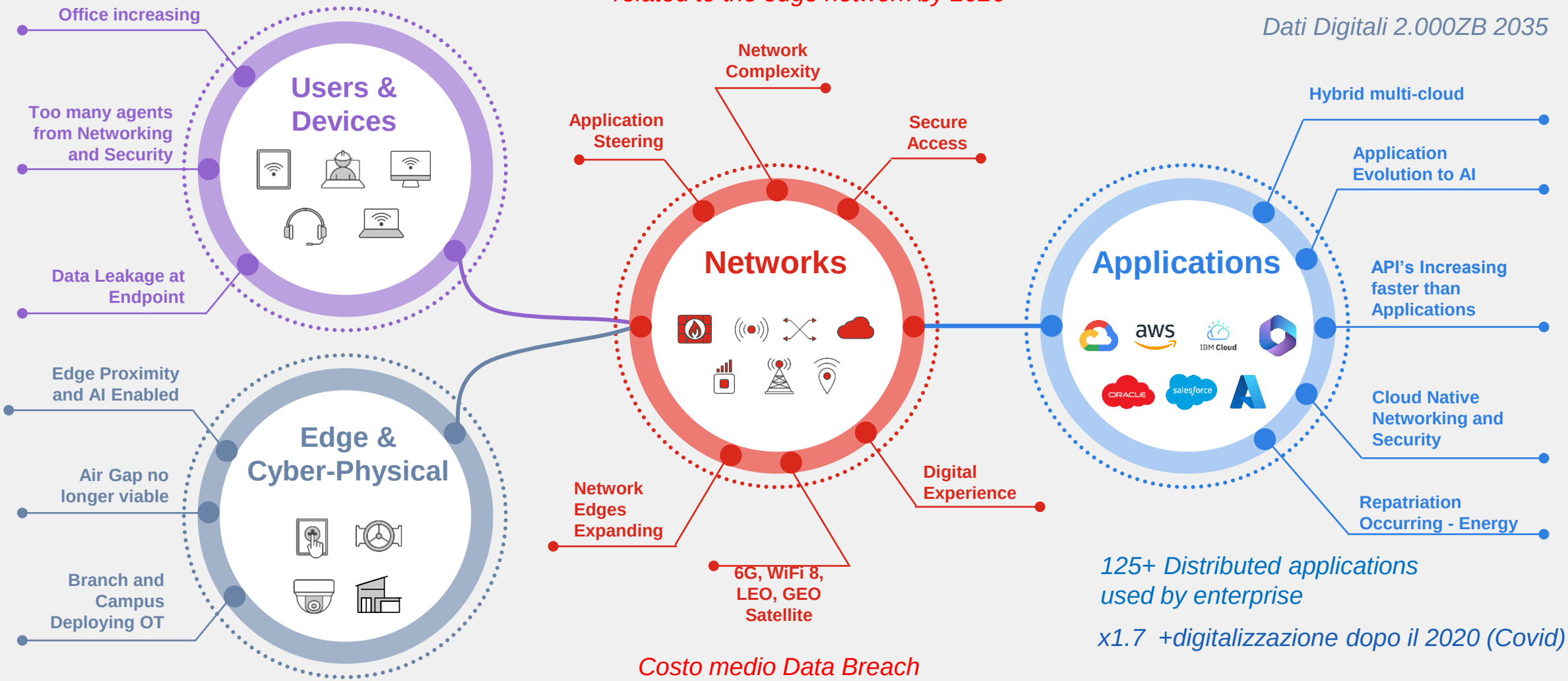
The attack surface continues to expand

84% Companies are hybrid

90% Of enterprises will have experienced a security incident related to the edge network by 2026

«Data Singularity» Ray Kurzweil, 2001

Dati Digitali 2.000ZB 2035



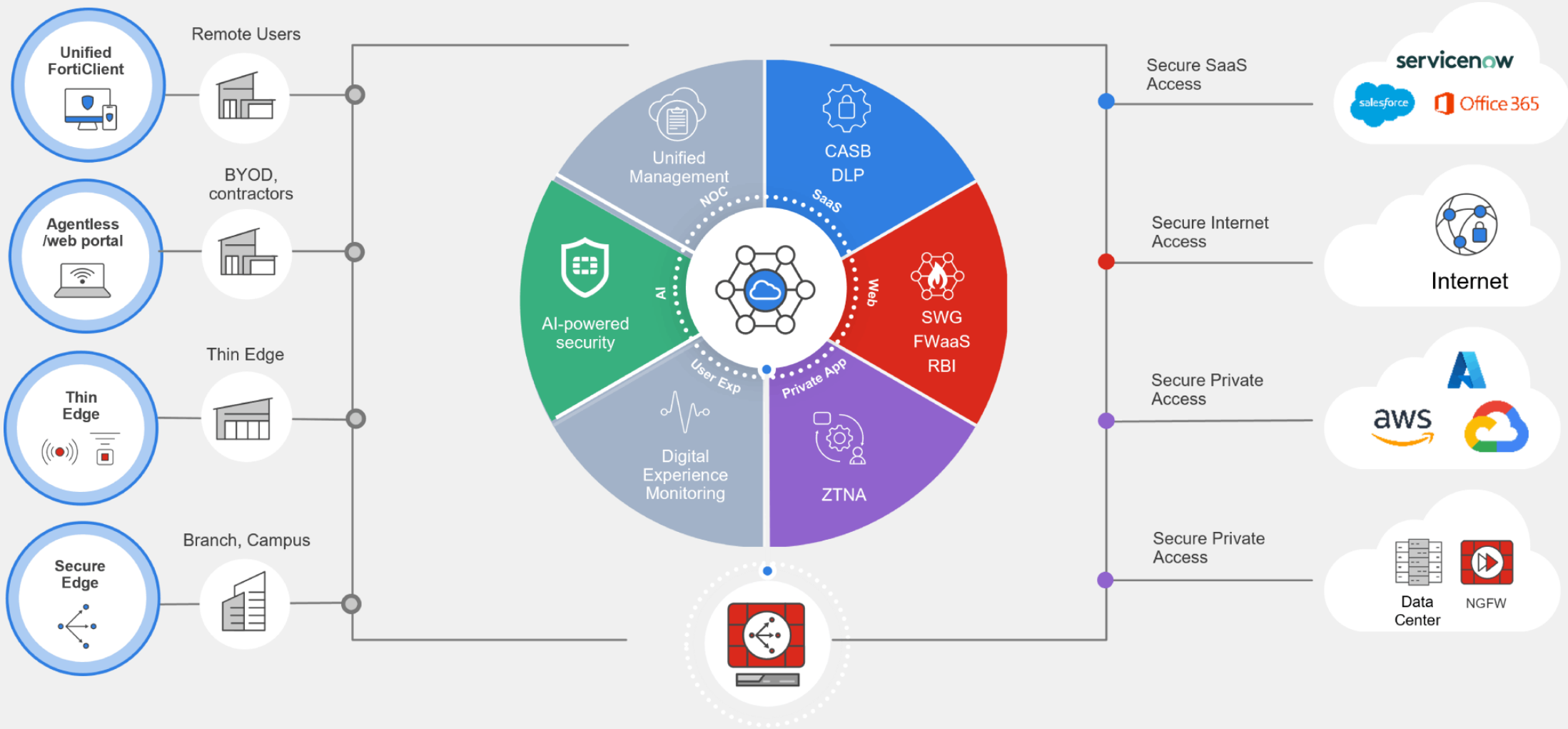
+40Mld IoT Devices 2033

Costo medio Data Breach 10.5B$

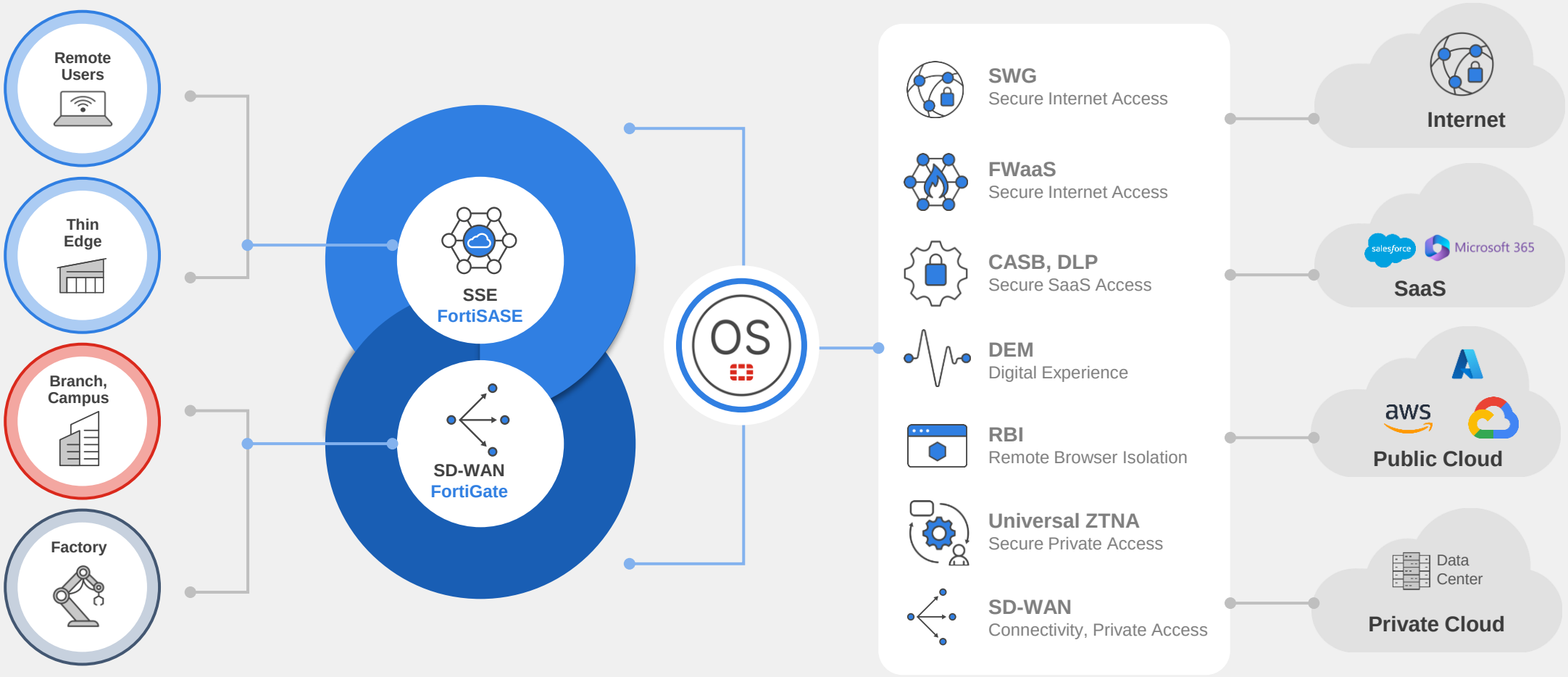
125+ Distributed applications used by enterprise

x1.7 +digitalizzazione dopo il 2020 (Covid)

Digital Networking & Infrastructure Evolution Accelerating: Unified-SASE (Secure Access Service Edge)



Digital Networking & Infrastructure Evolution Accelerating Unified-SASE Architecture



Unified Console, Agent, Data-lake

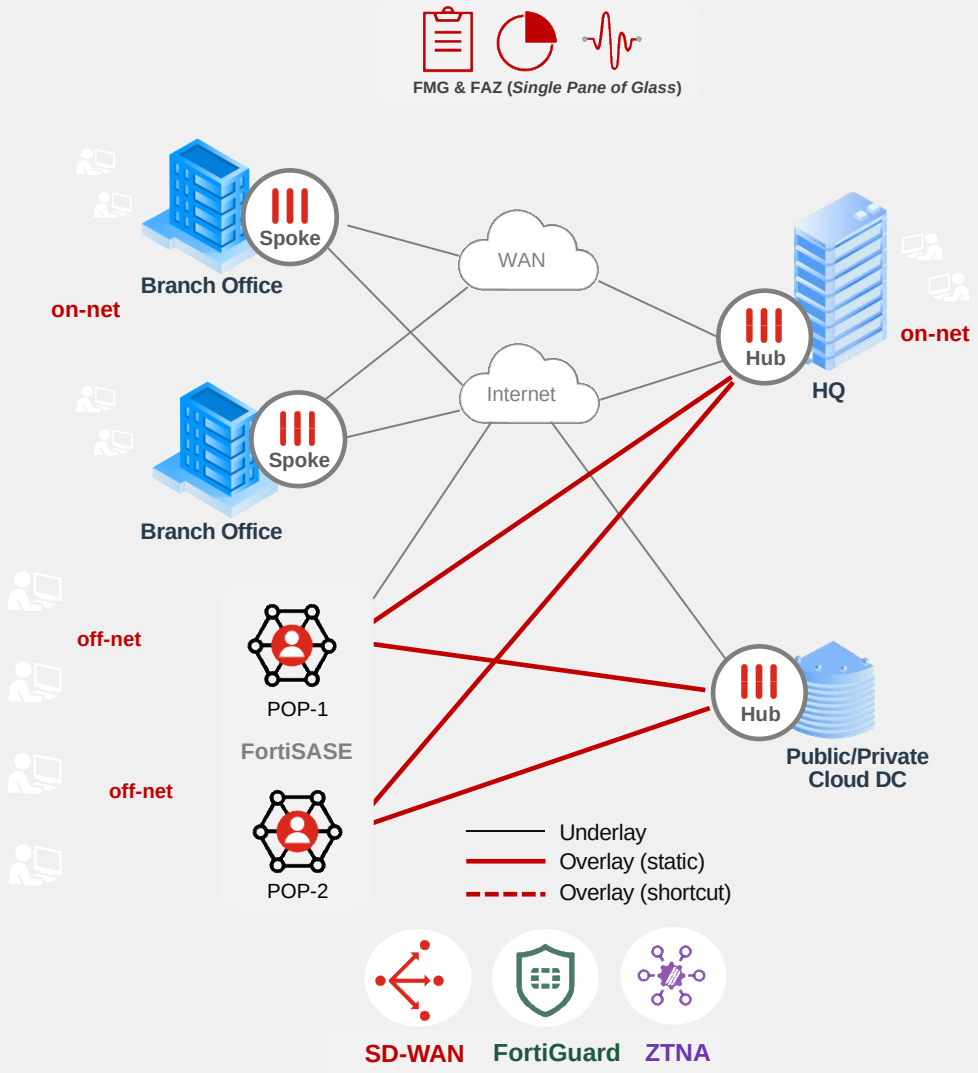
Flexible Enforcement, Connectivity

AI-Powered Intelligence

Digital Networking & Infrastructure Evolution Accelerating Unified-SASE Architecture

Providing All-in-One Remote Users and Site Protection

- **Connectivity**:
  - Remote users (FCT based, and agentless via FortiSASE)
  - Branches (over Fortinet SDWAN Network)
- **Secure Access:**
  - Local Network Protection
  - Secure Internet Access (SIA)
  - Secure SaaS Access (SSA)
  - Secure Private Access (SPA)
- **Native integration** into Fortinet ecosystem
- **Consistent security enforcement**, across the entire enterprise footprint (on-net & off-net)
- Consistent **ZTNA** filtering (EMS Security Fabric)
- **Central Management and Analytics**



Digital Networking & Infrastructure Evolution Accelerating

Gestire la supply chain quindi richiede Zero Trust Access.

1

- Identify and Authenticate device
- Authorized device or BYOD?
- Approved for access? revoked?

2

- User identity should be verified
- Strong MFA
- Role-based access controls

3

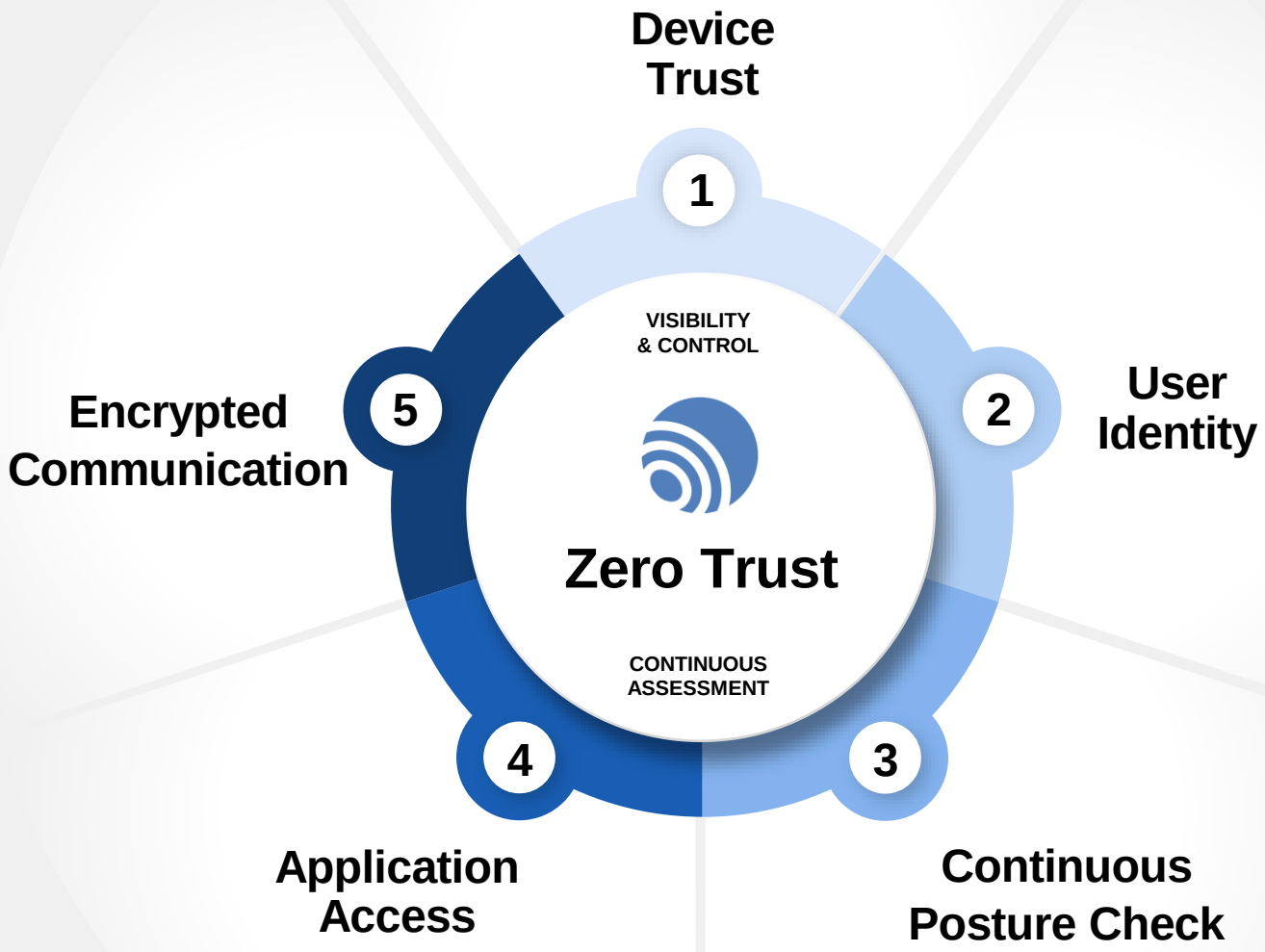
- Adaptive and conditional access
- Security Compliance
- Device Vulnerabilities

4

- Verify Application Access Rights
- Application Specific Access
- Application not available to internet

5

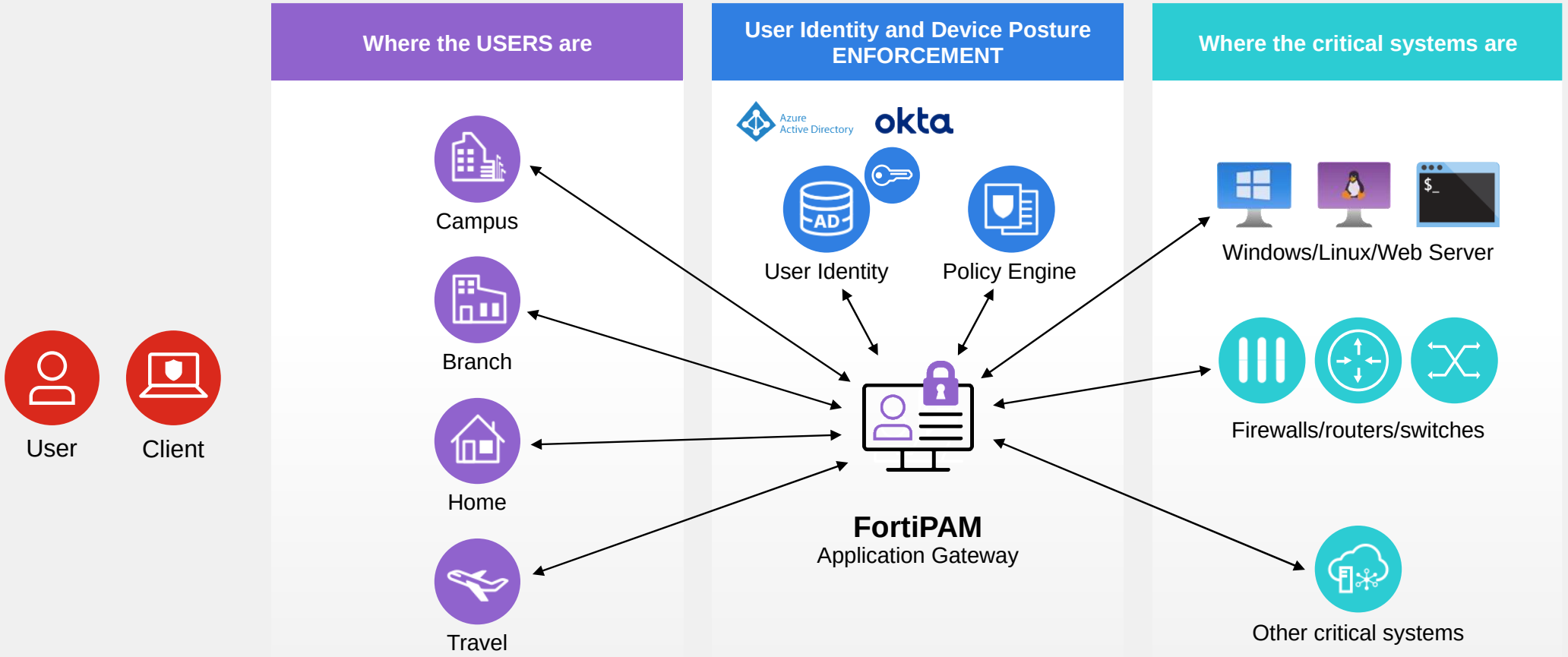
- End-to-end encryption- even on-prem
- Data protection
- All communication is logged



Digital Networking & Infrastructure Evolution Accelerating

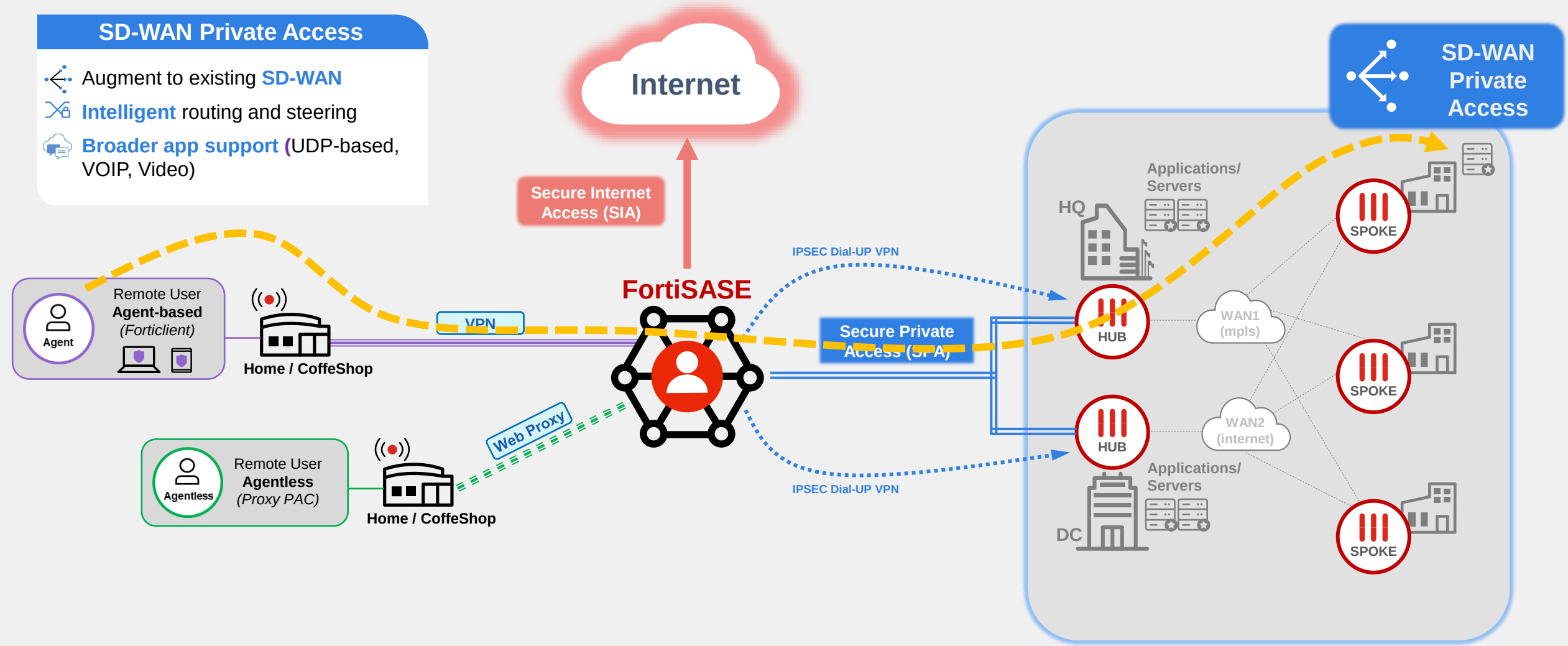
ZTNA Elements – FortiPAM as Access Proxy

The components of a client-based ZTNA solution



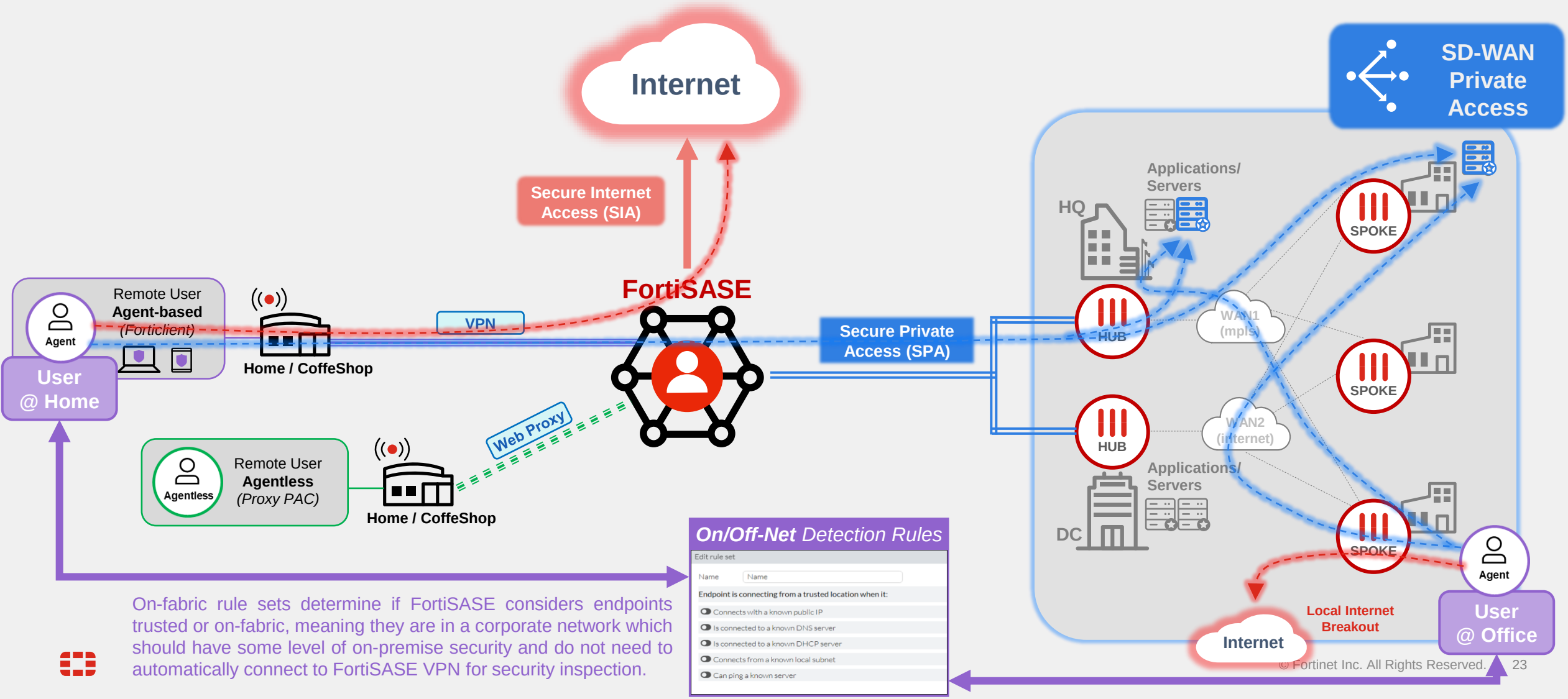
Digital Networking & Infrastructure Evolution Accelerating Secure Private Access

SD-WAN Seamless Integration



Digital Networking & Infrastructure Evolution Accelerating Secure Private Access

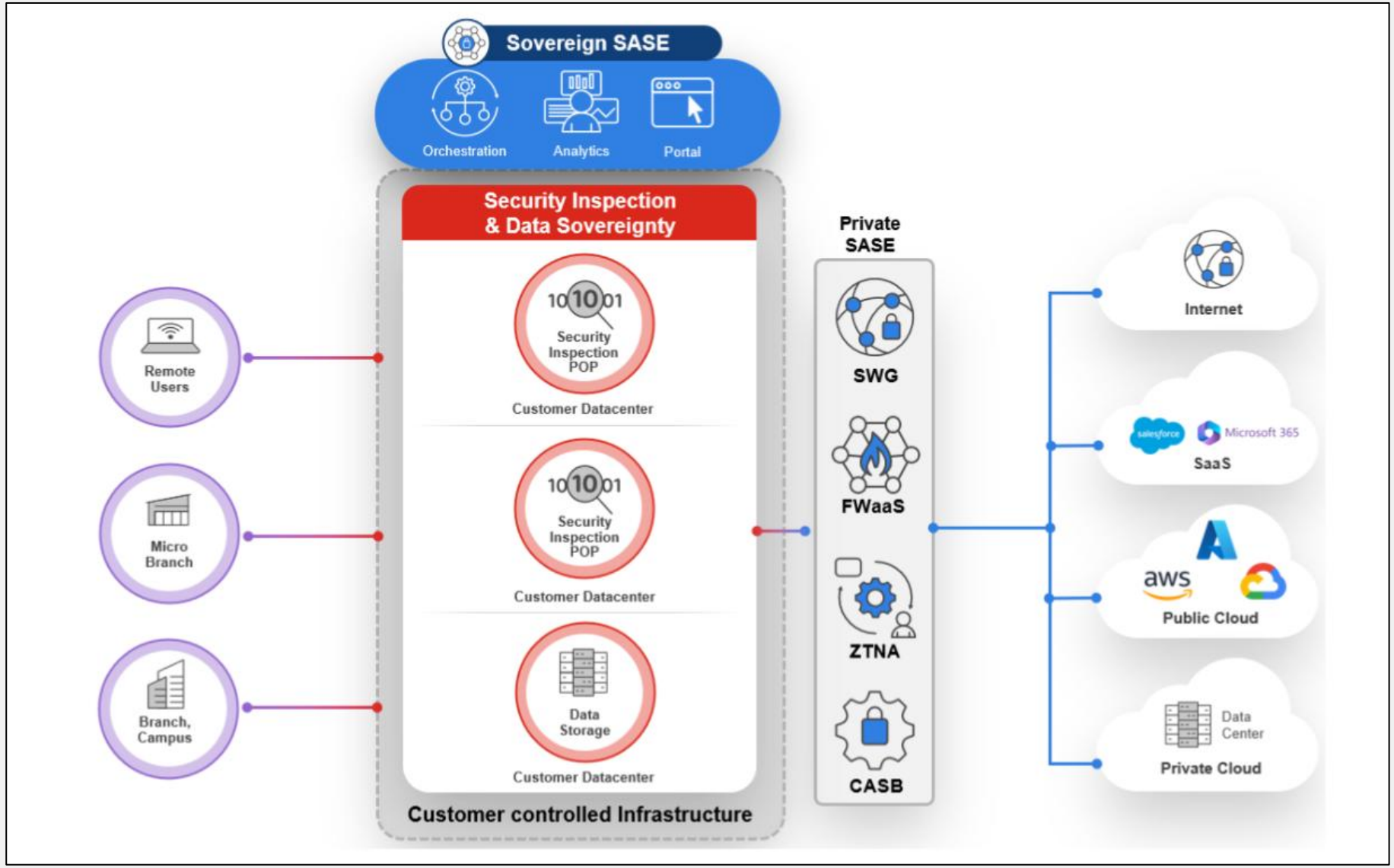
On-Net / Off-Net Detection Rules



On-fabric rule sets determine if FortiSASE considers endpoints trusted or on-fabric, meaning they are in a corporate network which should have some level of on-premise security and do not need to automatically connect to FortiSASE VPN for security inspection.

Digital Networking & Infrastructure Evolution Accelerating Sovereign SASE

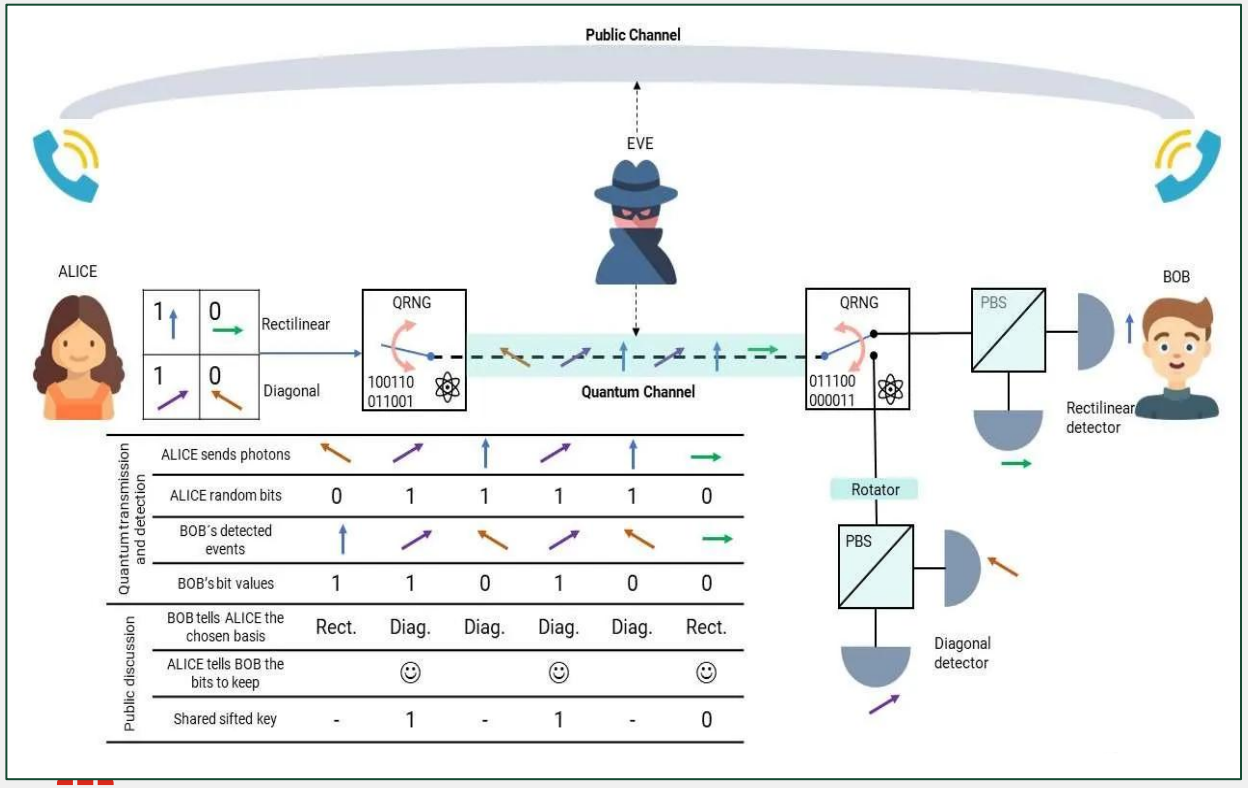
Il servizio SASE in casa

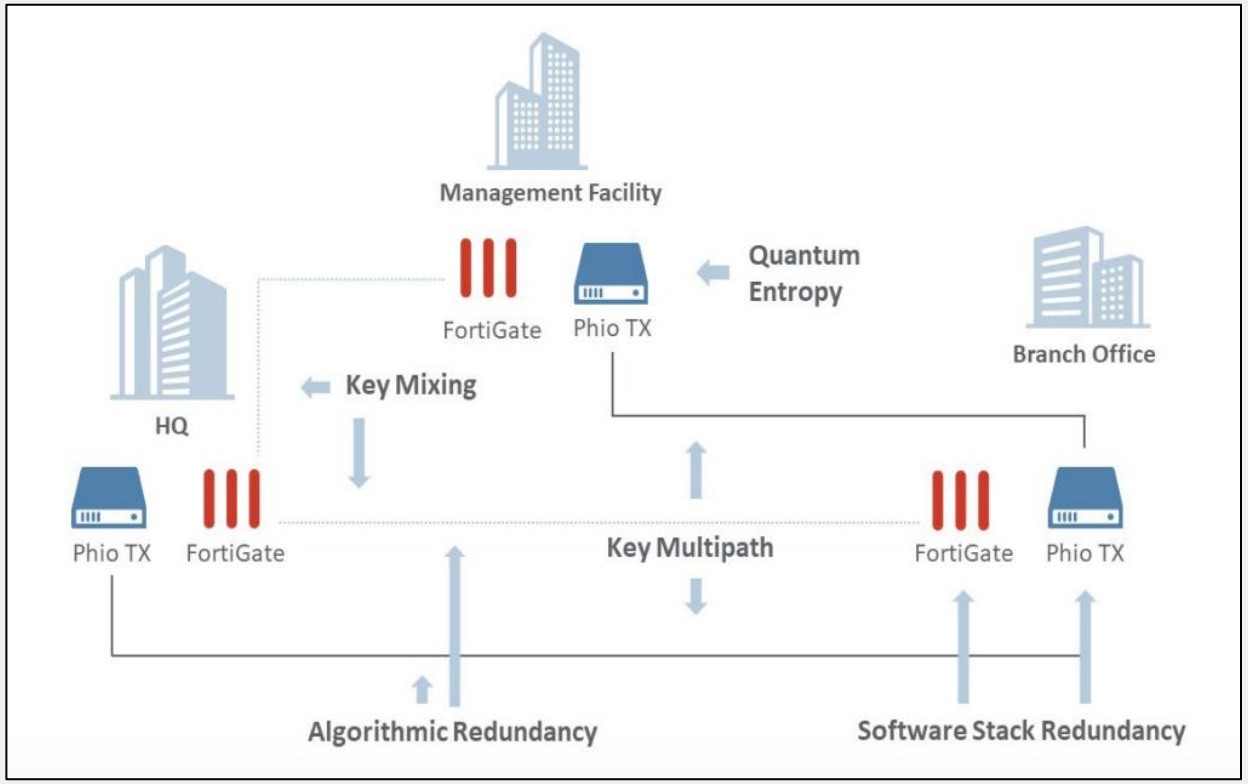


Digital Networking & Infrastructure Evolution Accelerating QKD Quantum Key Distribution

Mezzi di trasmissione utilizzati in QKD

- Fibre ottiche
- Spazio libero (Free-Space Optics, FSO)
- Satelliti per QKD globale






FORTINET