SECURITY SUMMIT

Security Summit

Napoli 23 settembre 2025

Clusit 25 2000-2025

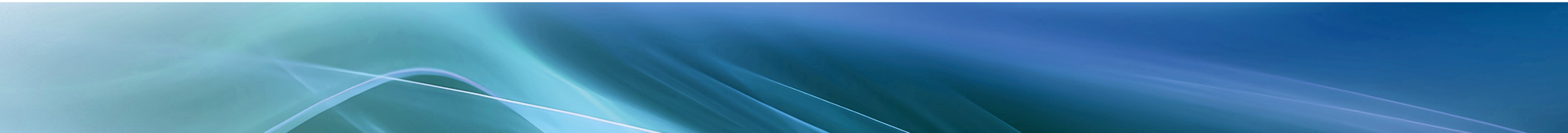
ASTREA

Ogni accesso ai servizi digitali mediante le VPN è un rischio:

dalla Campania una concreta innovazione

Relatori:

- **Valerio Mezzalira** – *CEO, Oplon Networks*
- **Giuseppe Doganiero** – *Responsabile Divisione Cyber Security, Enginfo Consulting*
- **Giuseppe Versace** – *Direttore Sistemi Informativi, A.O.R.N. Moscati*
- **Luca Bechelli** – *Comitato Direttivo CLUSIT – Partner @P4I – GRUPPO DIGITAL360*



oplon®

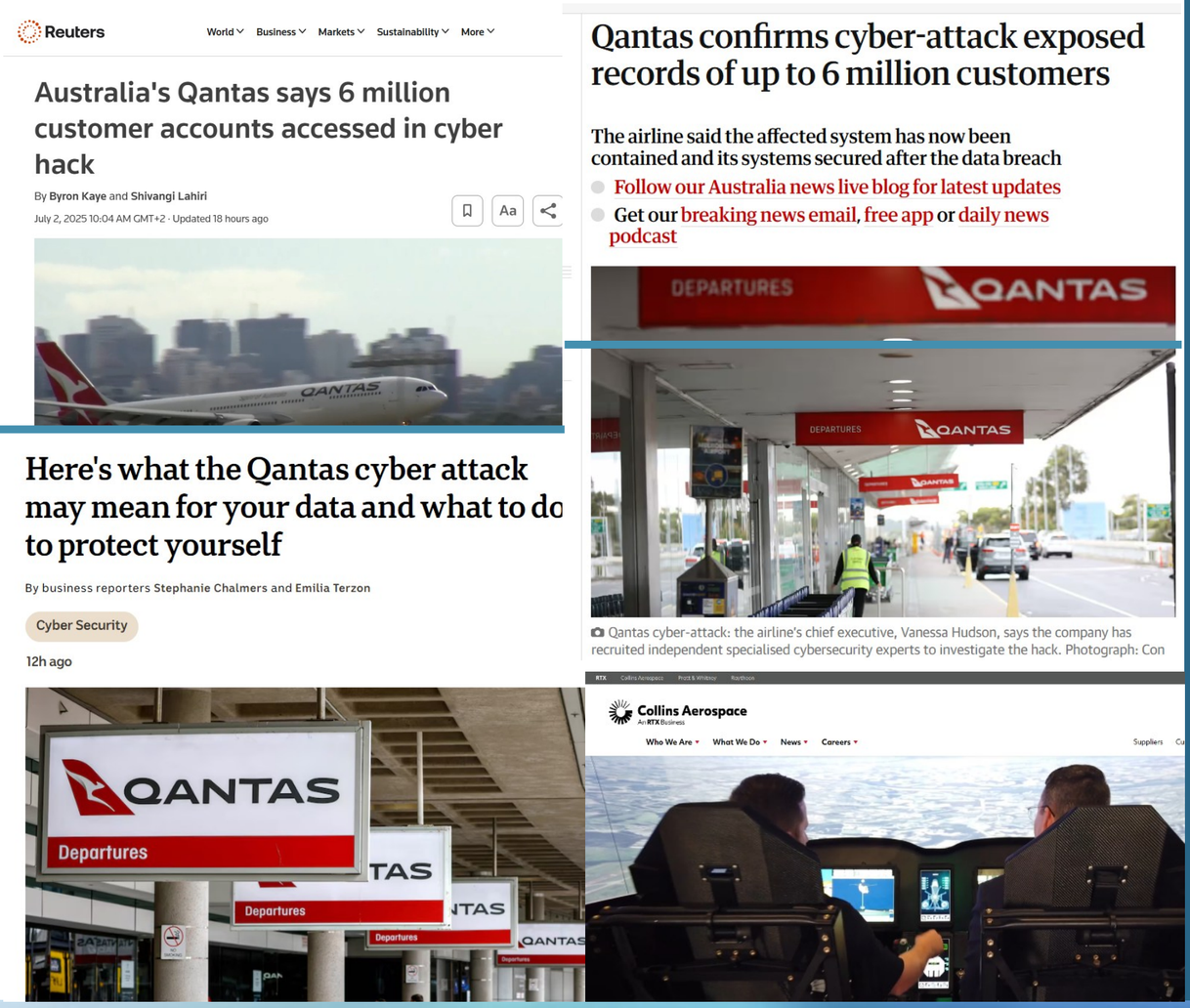
SECURE
SIMPLE
SCALABLE
SUSTAINABLE

Clusit 25th 2000-2025

SECURITY SUMMIT

ASTREA

Sfide attuali



Reuters World Business Markets Sustainability More

Australia's Qantas says 6 million customer accounts accessed in cyber hack

By Byron Kaye and Shivangi Lahiri

July 2, 2025 10:04 AM GMT+2 · Updated 18 hours ago

Here's what the Qantas cyber attack may mean for your data and what to do to protect yourself

By business reporters Stephanie Chalmers and Emilia Terzon

Cyber Security

12h ago

Qantas confirms cyber-attack exposed records of up to 6 million customers

The airline said the affected system has now been contained and its systems secured after the data breach

Follow our Australia news live blog for latest updates

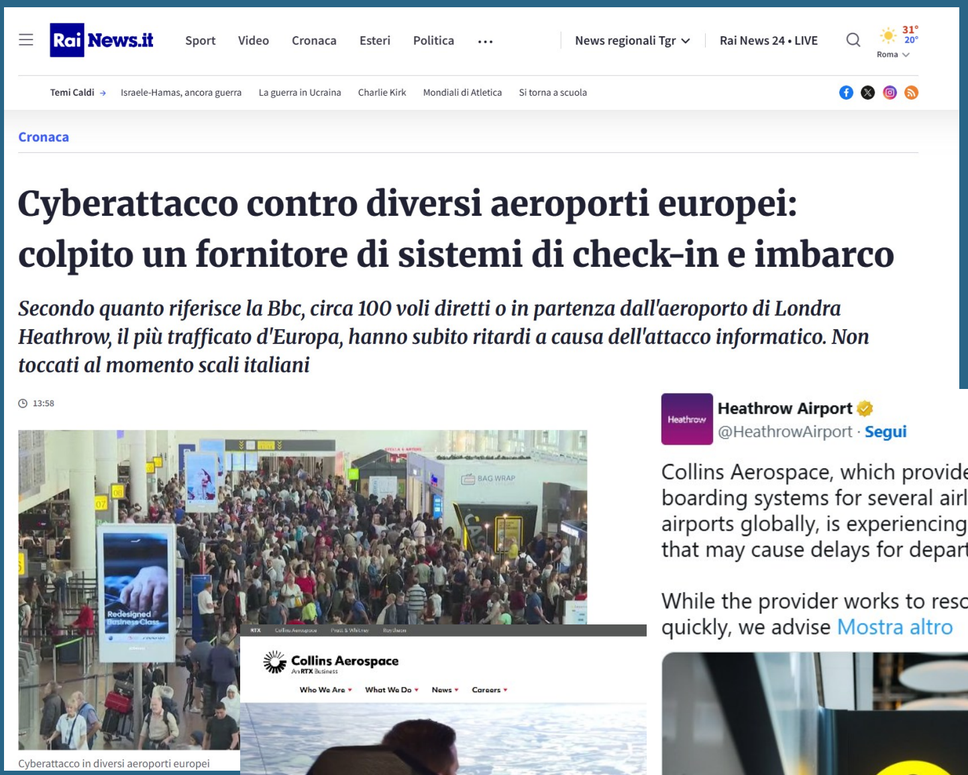
Get our breaking news email, free app or daily news podcast

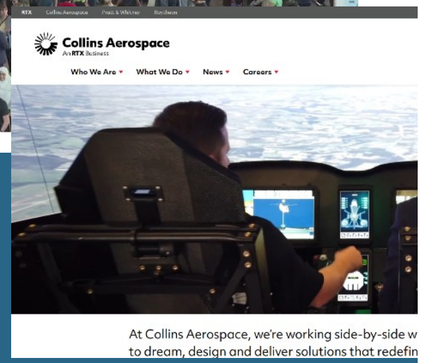
Qantas cyber-attack: the airline's chief executive, Vanessa Hudson, says the company has recruited independent specialised cybersecurity experts to investigate the hack. Photograph: Con

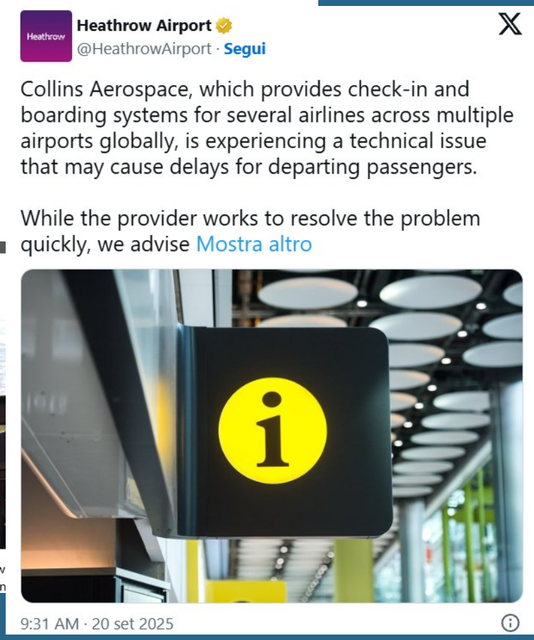
Il vettore dell'attacco è stato un fornitore terzo.
Ecco i punti chiave su come è avvenuto l'attacco

- **Vettore dell'attacco:** L'incidente è avvenuto quando un cybercriminale ha preso di mira un **call center** e ha ottenuto l'accesso a una **piattaforma di servizio clienti di terze parti**. Questa piattaforma esterna, non direttamente posseduta da Qantas, conteneva i record di circa 6 milioni di passeggeri.
- **Data della scoperta:** Qantas ha rilevato attività insolite su questa piattaforma di terze parti lunedì 30 giugno 2025.
- **Dati compromessi:** L'indagine iniziale ha confermato che i dati rubati includono:
  - Nomi dei clienti
  - Indirizzi email
  - Numeri di telefono
  - Date di nascita
  - Numeri di Frequent Flyer

Sfide attuali







Un **attacco informatico** che ha preso di mira un fornitore di servizi per i sistemi di check-in e imbarco ha interrotto le operazioni in diversi importanti aeroporti europei, tra cui anche Bruxelles, Berlino e Heathrow a Londra. Si registrano ritardi e cancellazioni dei voli. Secondo l'aeroporto di Bruxelles, l'**attacco ha reso inutilizzabili i sistemi automatizzati, consentendo solo le procedure di check-in e imbarco manuali**.

Secondo quanto riferisce la Bbc, circa **100 voli diretti o in partenza dall'aeroporto di Londra Heathrow, il più trafficato d'Europa, hanno subito ritardi** a causa dell'**attacco informatico che ha preso di mira la società Collins Aerospace** che fornisce sistemi di check-in e imbarco a diverse compagnie aeree in scali in tutto il mondo. **A Bruxelles i voli che hanno subito ritardi sono finora circa 70, a Berlino 15**.

Non c'è al momento alcun impatto sui sistemi informatici degli scali italiani. Da Fiumicino, secondo quanto viene riferito, è regolare: solo il volo Eju2981 per Bruxelles - uno degli aeroporti maggiormente colpiti - è stato cancellato. Altri due voli, sempre da Bruxelles (volo Sn3175 e volo Eju9043), stanno facendo registrare ritardi. Dalle prime ore di questa mattina, a quanto si apprende **il Cnaipic, Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche, unità specializzata del Servizio polizia postale e per la sicurezza cibernetica, è in costante contatto con Enav e Enac** per monitorare eventuali minacce cyber al sistema aereo nazionale.

Perchè accadono queste cose:

1. Problema della decidibilità (Teorema di Rice & Halting Problem)

Esistono problemi che non sono decidibili da una macchina algoritmica. In particolare:

- Il problema di arresto (Halting Problem) dimostra che non si può costruire un algoritmo che, per ogni programma e input, determini se il programma si fermerà.
- Il Teorema di Rice afferma che ogni proprietà non banale del comportamento di un programma è indecidibile.

Quindi, non esiste un algoritmo universale che possa analizzare ogni codice e decidere con certezza se è malevolo
o no.

2. Modello probabilistico dell'analisi comportamentale

Supponiamo di avere:
•P_m: probabilità che un programma sia malevolo
•D(p): funzione di rilevamento che restituisce 1 se il programma è rilevato come malevolo, 0 altrimenti
Allora, anche il miglior sistema può solo approssimare: \lim_{t \to \infty} \mathbb{E}[D(p)] < 1
Perché:

$$\lim_{t \to \infty} \mathbb{E}[D(p)] < 1$$

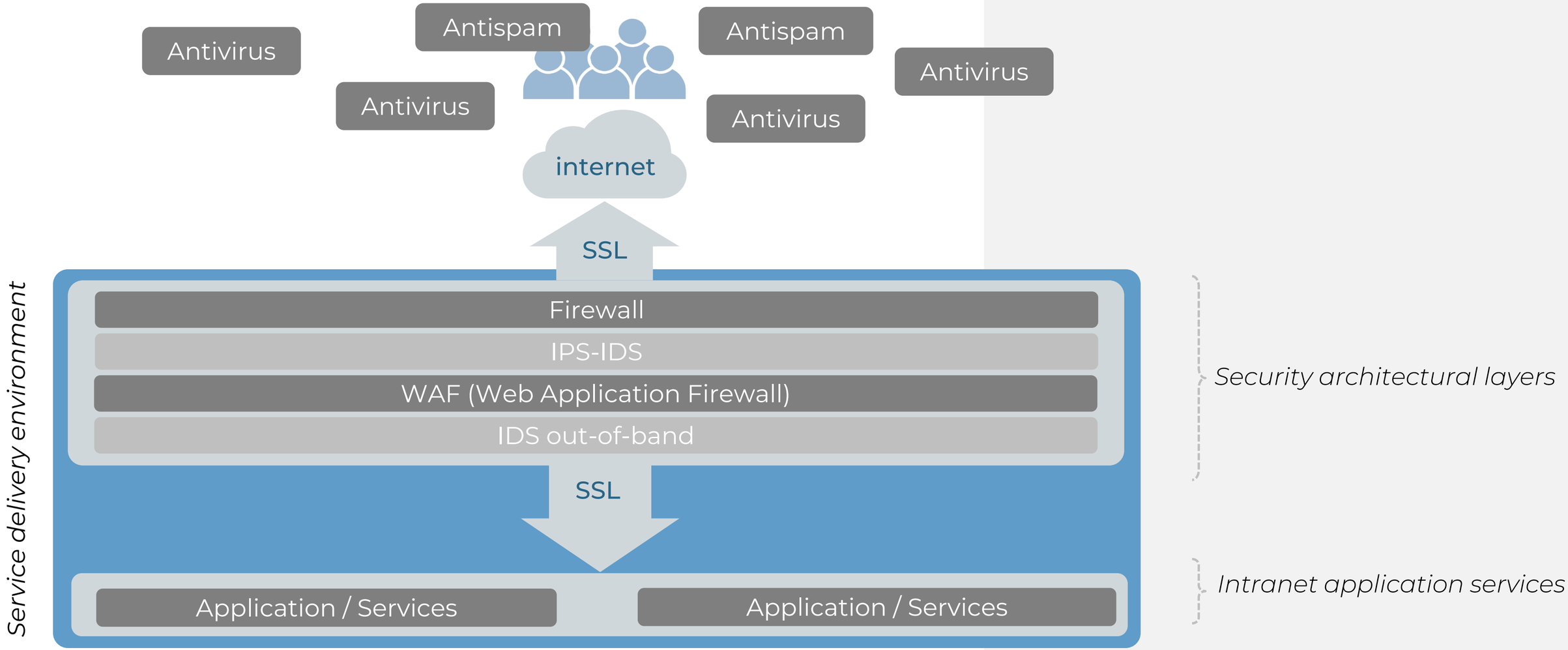
- Alcuni malware sono obfuscated, polimorfici, o time-triggered
- Alcuni comportamenti benigni possono simulare quelli malevoli

3. Anche con IA avanzata, possiamo modellare:

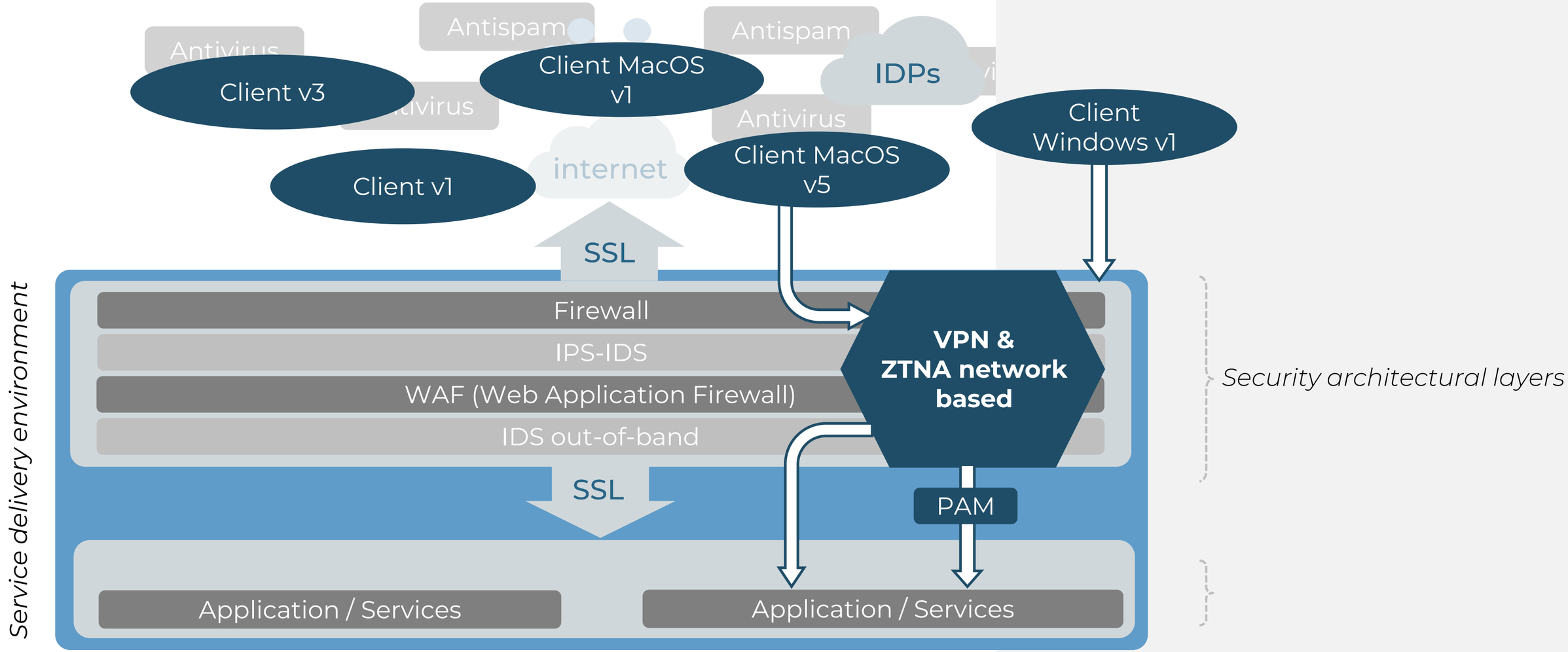
\text{Copertura massima} = \frac{M_k + \alpha M_u}{M_t}
Dove \alpha < 1 sempre, perché l'IA non può garantire
la rilevazione perfetta di minacce ignote.

$$\text{Copertura massima} = \frac{M_k + \alpha M_u}{M_t}$$

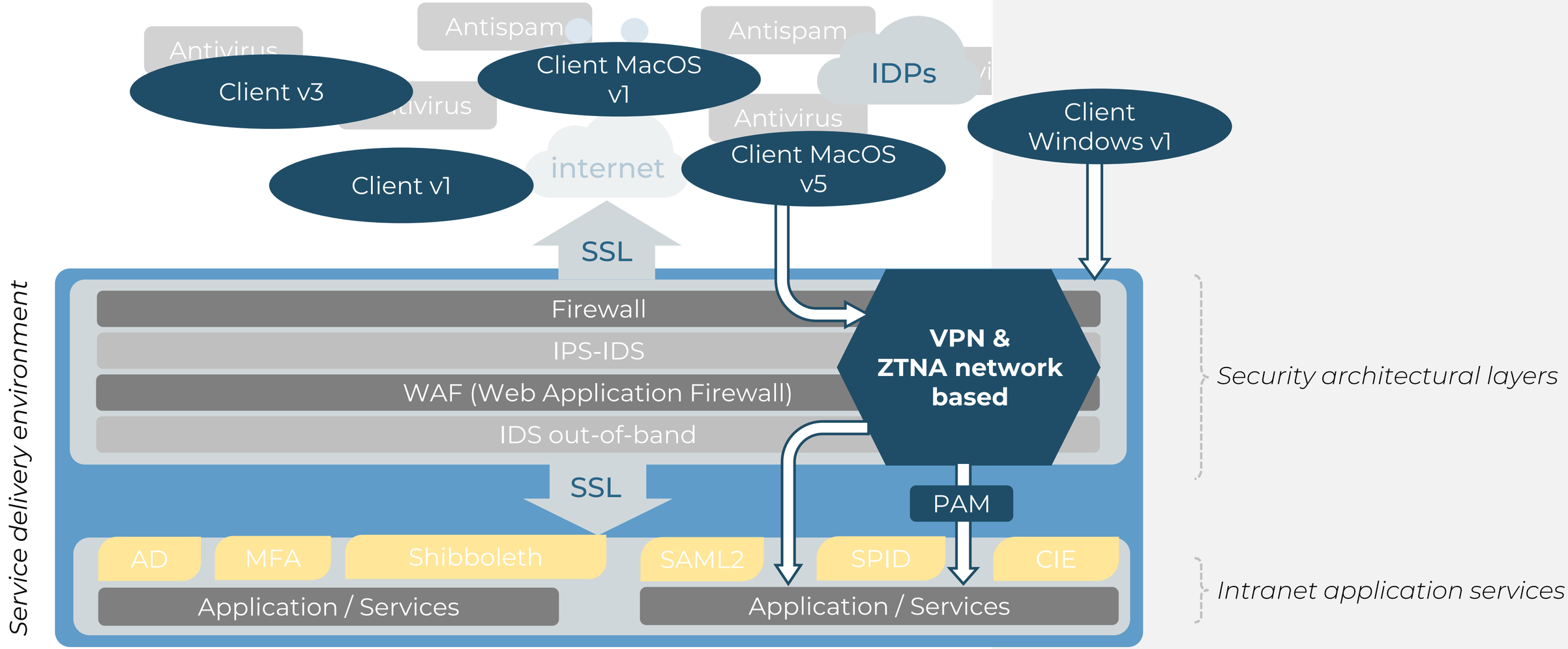
Security: Architectural Layers



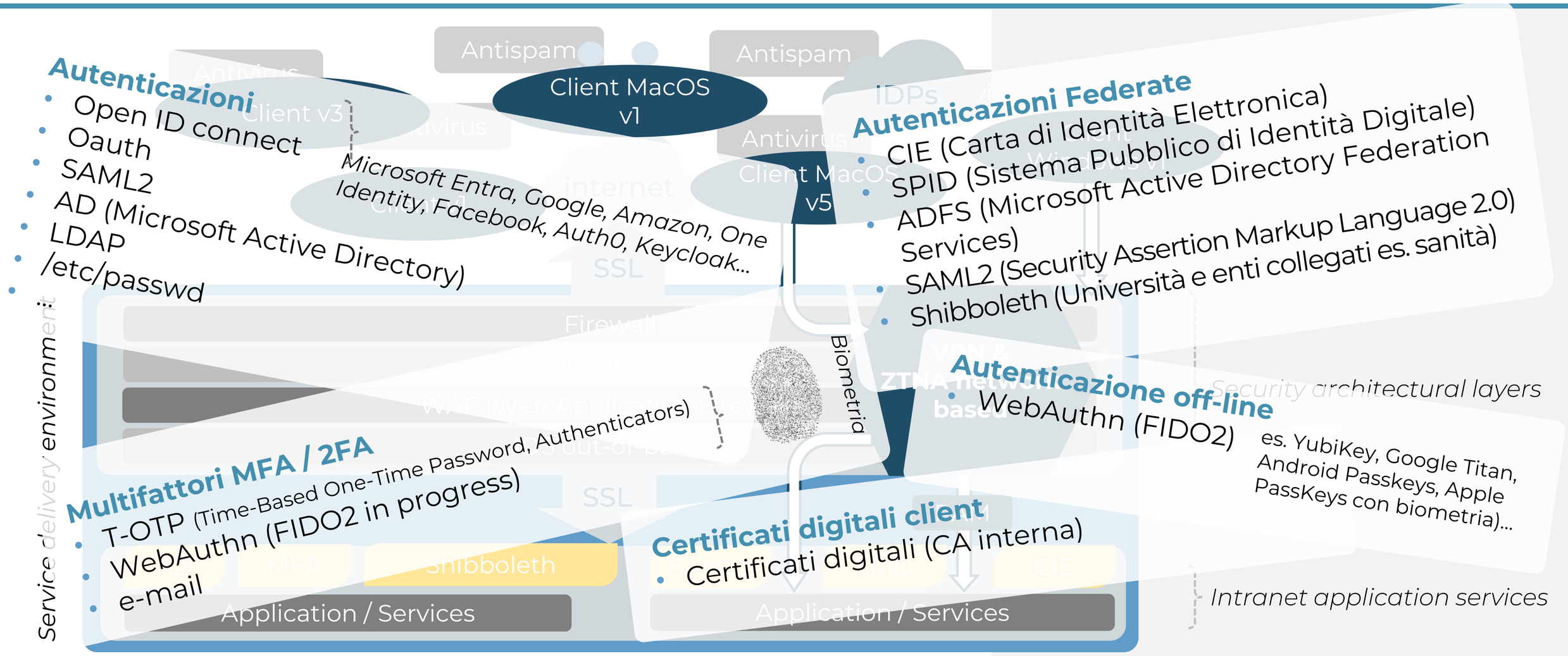
Security: Architectural Layers + Identity + PAM + Client + Agenti



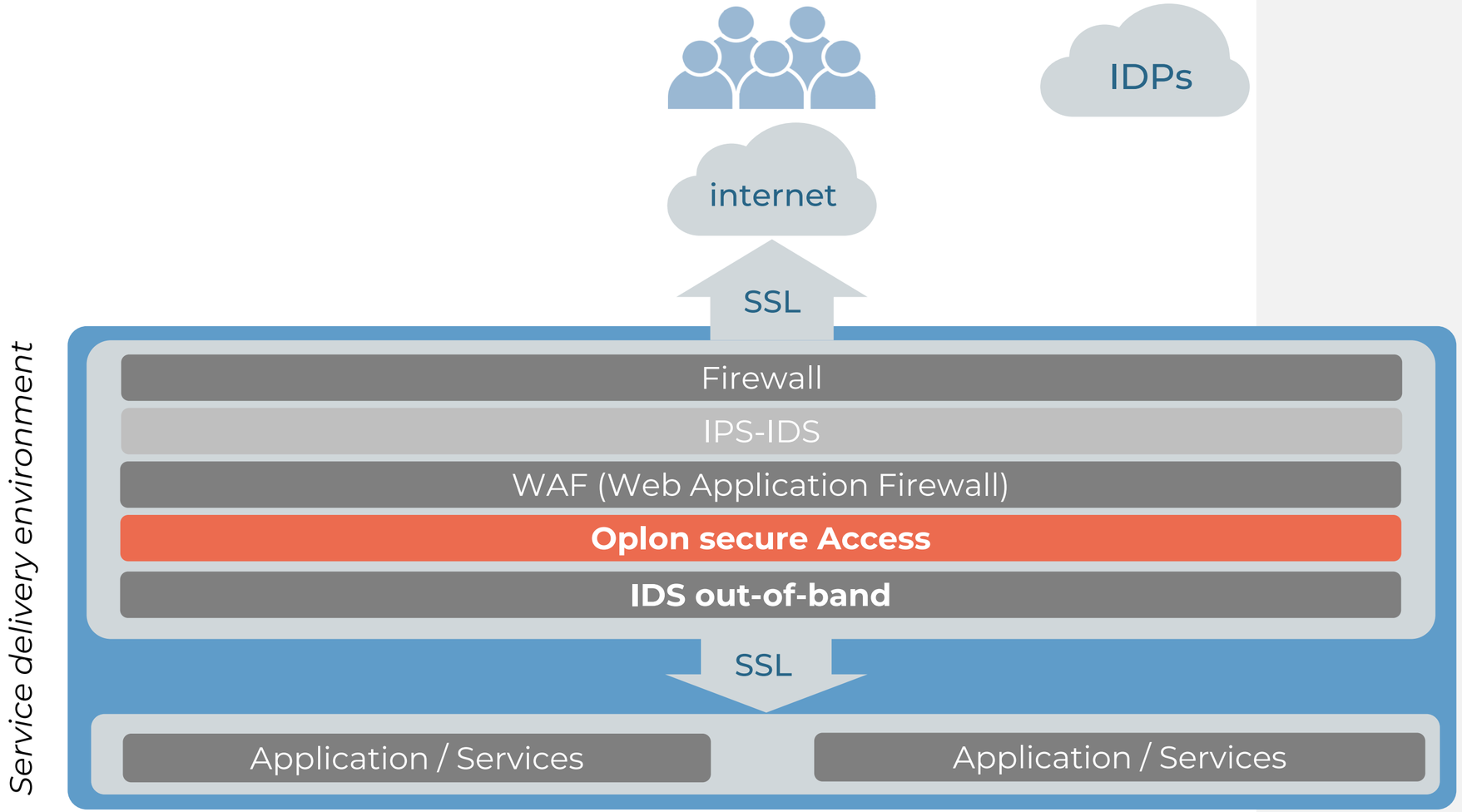
Security: Architectural Layers + Identity + PAM + Client + Agenti



Security: Architectural Layers + Identity + PAM + Client + Agenti

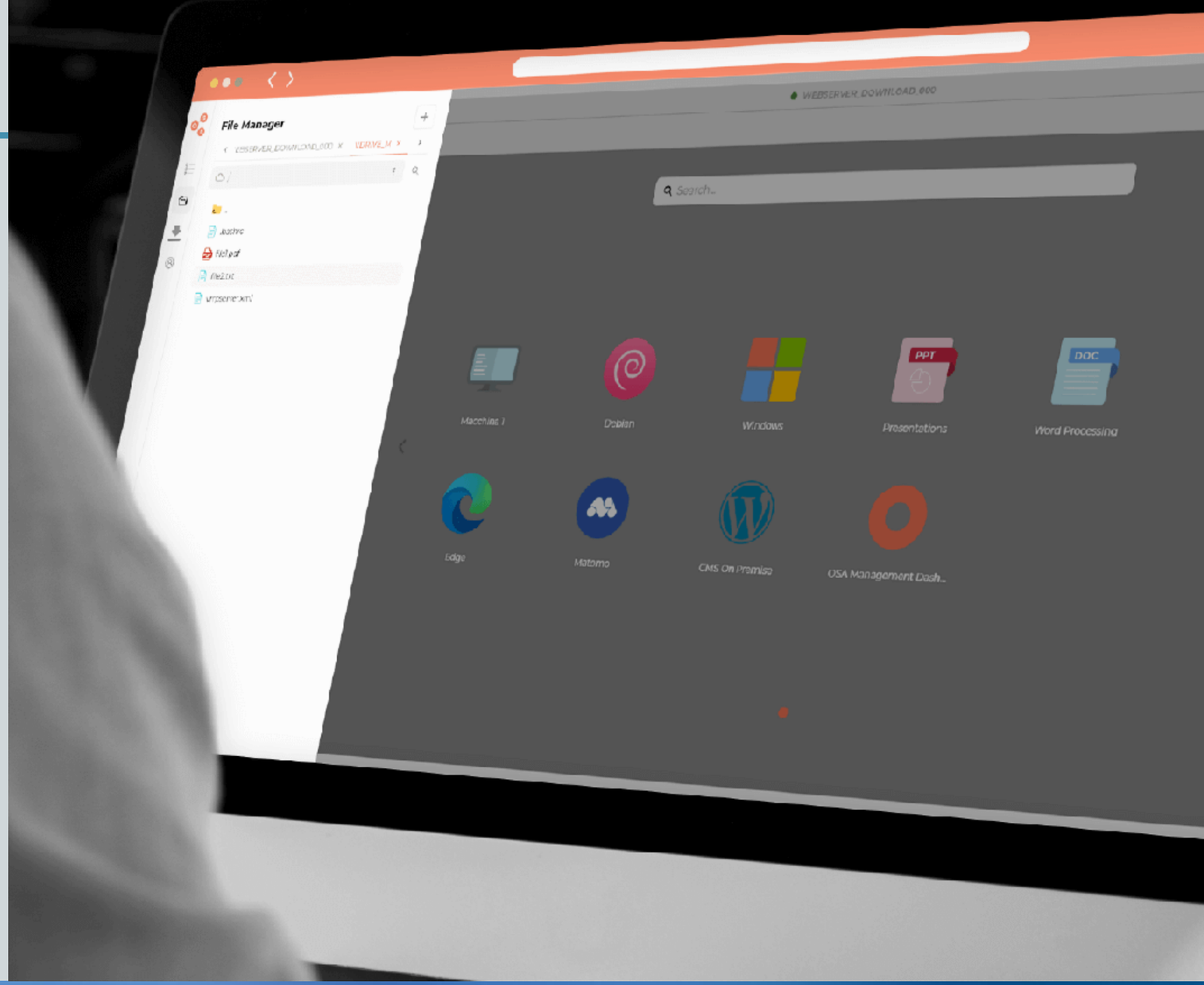


Security: Architectural Layers



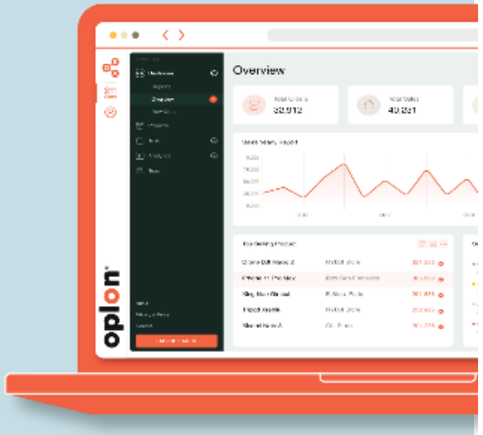
Oplon Secure Access

Il Browser come unico strumento d’accesso



Oplon Secure Access

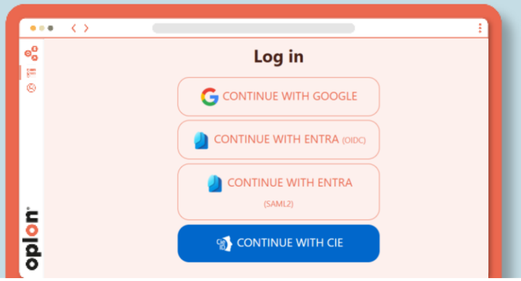
SERVIZI WEB



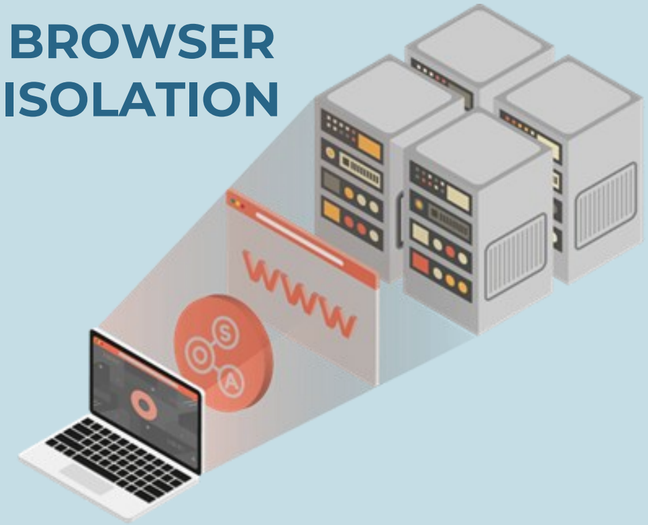
SERVIZI RDP VDI

SERVIZI SSH

AUTENTICAZIONI FEDERATE



BROWSER ISOLATION



Access Security

Work force
Application users
Manager
Students
Professors
Doctors
Nurses
...

Organization

Business

Privileged

Systems engineer
External suppliers
Developers

Citizens /Customers

Non Human Identity

Perimetro

Identity Management and Access Security

PAM

App1	App2	App3	App4	App5
Equipment	**Equipment**	**Equipment**	**Equipment**	**Equipment**

Access Security

Organization

Citizens /Customers

Non-Human

OPLON SECURE ACCESS

Web Application Gateway
Remote Access Gateway
Browser Isolation

OPLON SECURE ACCESS

Identity Link

OPLON SECURE ACCESS

NHI
Gateway

October 2025

App1	App2	App3	App4	App5
Equipment	**Equipment**	**Equipment**	**Equipment**	**Equipment**

Oplon Secure Access: Sardegna

Regione Autonoma della Sardegna

ARES Sardegna

REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

Azienda | Albo Pretorio | Bandi e Gare | Bandi di concorso e selezione | Formazione | Notizie

Home / Notizie / La cyber security nel Settore Sanitario: a Cagliari il convegno ACN

La cyber security nel Settore Sanitario: a Cagliari il convegno ACN

Presentato il Progetto di ARES per la Sicurezza Digitale del sistema sanitario regionale

INDICE DELLA PAGINA

Ulteriori informazioni

"La minaccia cibernetica al settore sanitario" è il titolo del convegno che si è svolto presso l'Aula Atza dell'Ospedale Brotzu di Cagliari: un evento di grande rilevanza per la sicurezza informatica del sistema sanitario regionale. L'iniziativa fa parte di un'ampia campagna nazionale portata avanti dell'**Agenzia per la Cybersicurezza Nazionale (ACN)**.

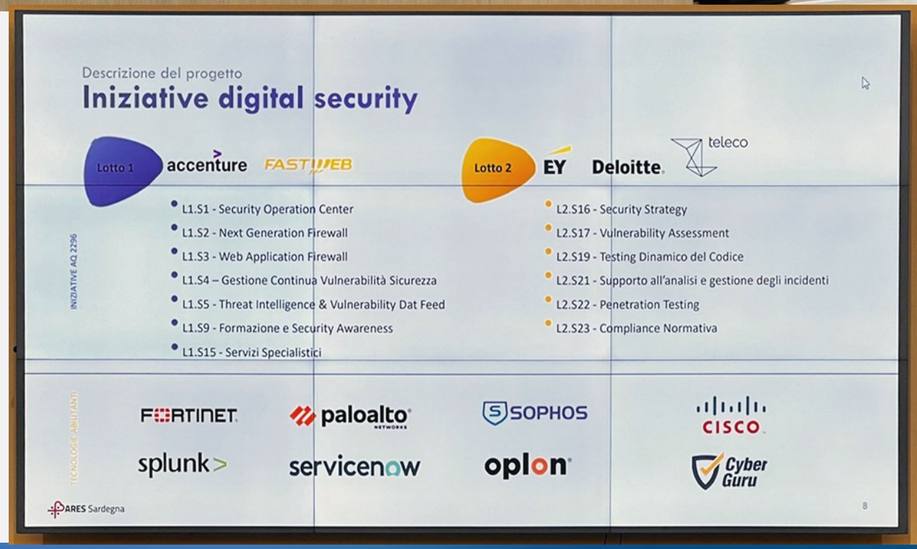
I lavori sono stati aperti con una tavola rotonda, moderata dal Prof. **Giorgio Giacinto** (Università di Cagliari), a cui hanno partecipato la Presidente della Regione **Alessandra Todde** e la Vicepresidente di ACN **Nunzia Ciardi**, con l'Assessore alla Sanità **Armando Bartolazzi**.

Nel corso della seconda parte del convegno, sono intervenuti il Capo delle Operazioni dell'ACN **Gianluca Galasso**, il Direttore Generale Innovazione e Sicurezza IT dell'Assessorato regionale Affari Generali **Marco Melis** che ha illustrato le azioni di cyber sicurezza in ambito non sanitario, e il Direttore Generale di ARES **Giuseppe Pintor** che ha introdotto il **piano di digital security dedicato alla sanità regionale**: un'iniziativa strategica volta a rafforzare la protezione delle infrastrutture digitali del sistema sanitario regionale.

14/02/2025

Fonte:

https://www.aressardegna.it/convegno-acn-a-cagliari-la-minaccia-cibernetica-al-settore-sanitario//



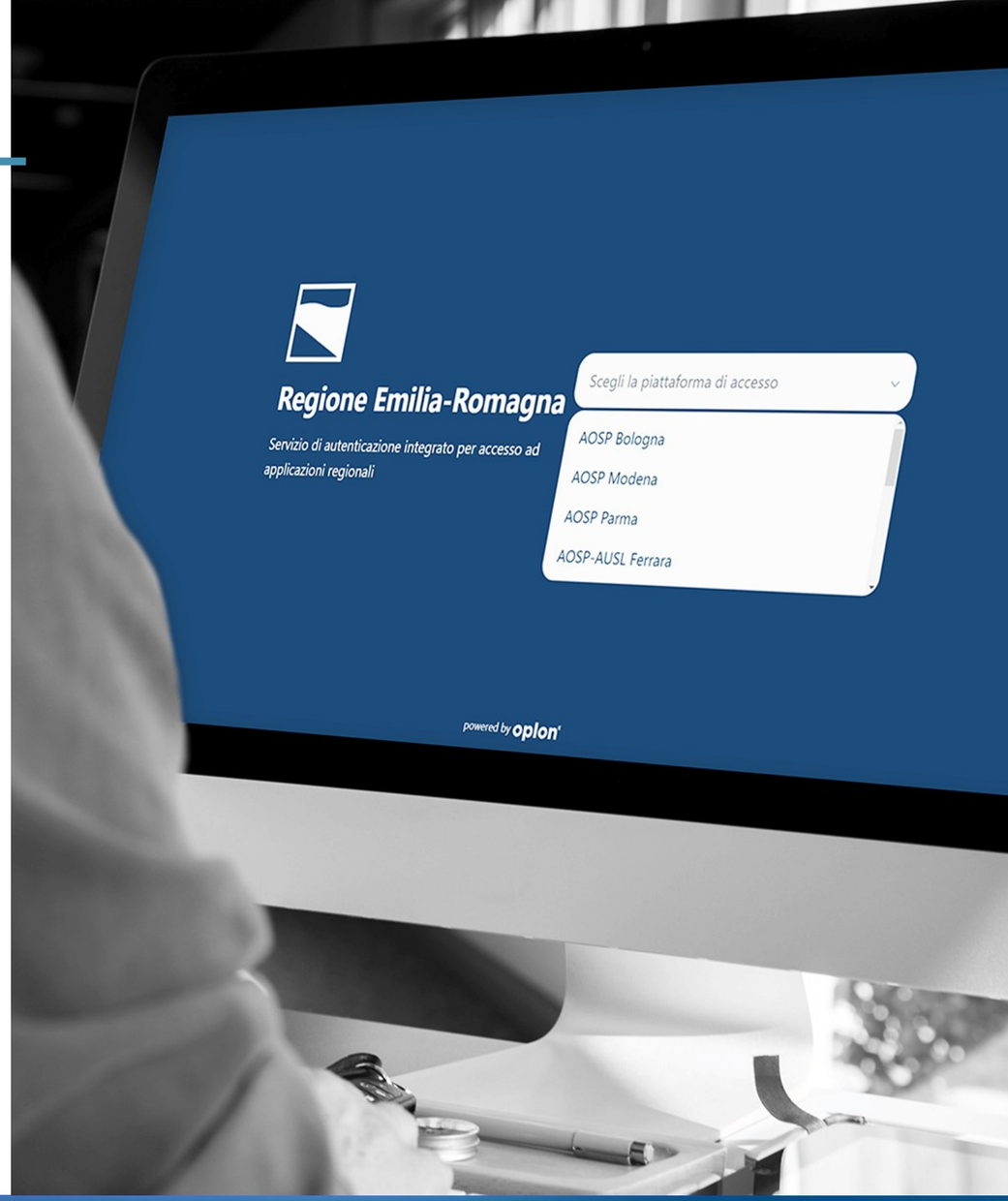
Identity Link: Regione Emilia Romagna

Motivi per adottare Identity Link

- La Direzione Generale Cura della Persona, Salute e Welfare di RER ha necessità di una nuova infrastruttura per fornire uno strumento semplificato per Autenticare e Autorizzare gli utenti attraverso i provider di Identity Management già esistenti

- Dismissione utenti per il dominio EXTRARER, sostituito in autenticazione dal nuovo sistema Oplon Secure Access

Struttura Sanitaria	IdP
AUSL 01	Entra ID
AUSL 02	SAML2/ADFS
AUSL 03	SAML2/Shibbolet
AUSL 04	SAML2/Shibbolet
AUSL 05	SAML2/Shibbolet
AUSL 06	SAML2/Shibbolet
AUSL 07	SAML2/ADFS?
AUSL 08	SAML2/ADFS
AUSL 09	SAML2/Shibbolet
AUSL 10	Open ID/ADFS
AUSL 11	SAML2/ADFS
AUSL 12	SAML2/Shibbolet



Autenticazioni supportate

Autenticazioni

- Open ID connect
- Oauth
- SAML2
- AD (Microsoft Active Directory)
- LDAP
- /etc/passwd
- ...

Autenticazioni Federate

- CIE (Carta di Identità Elettronica)
- SPID (Sistema Pubblico di Identità Digitale)
- ADFS (Microsoft Active Directory Federation Services)
- SAML2 (Security Assertion Markup Language 2.0)
- Shibboleth (Università e enti collegati es. sanità)

Multifattori MFA / 2FA

- T-OTP (Time-Based One-Time Password, Authenticators)
- WebAuthn (FIDO2 in progress)
- e-mail

Biometria

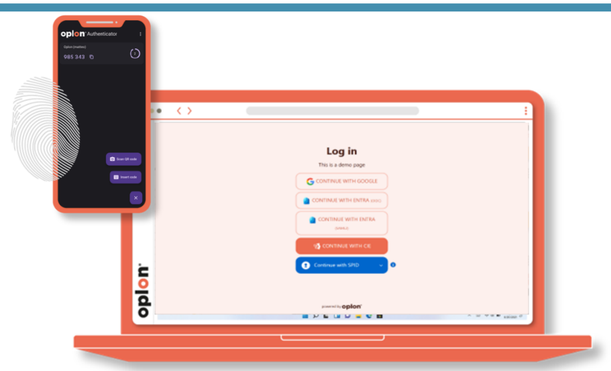
Autenticazione off-line

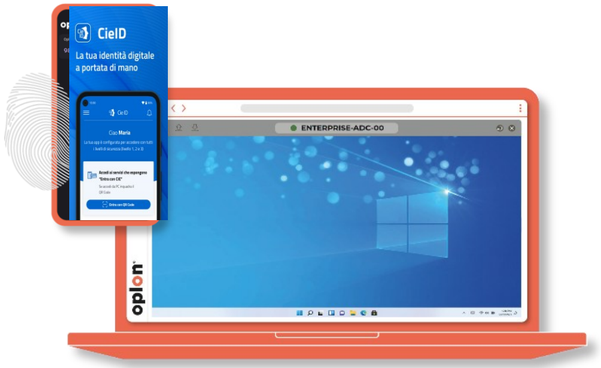
- WebAuthn (FIDO2) es. YubiKey, Google Titan, Android Passkeys, Apple PassKeys con biometria)...

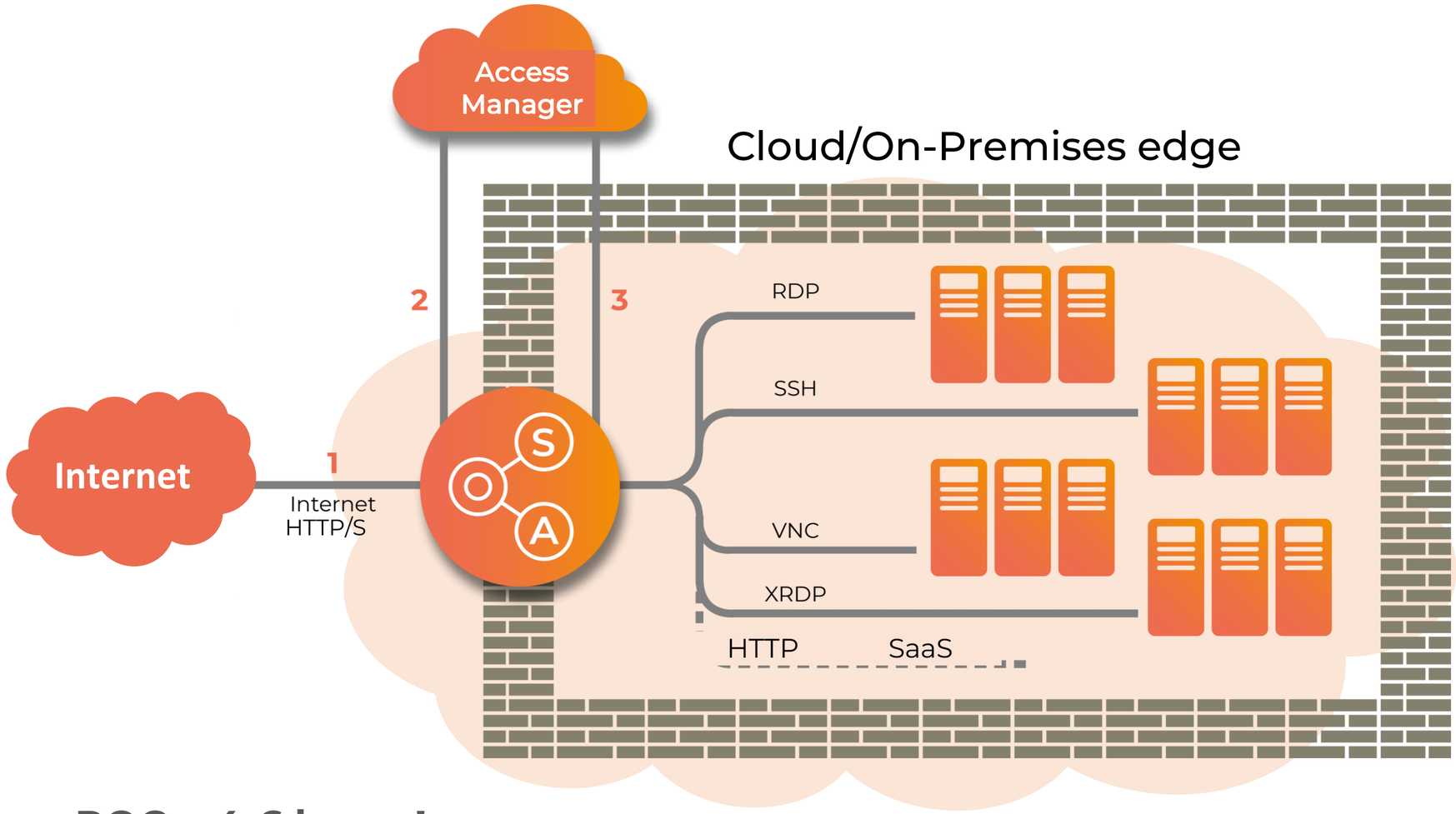
Certificati digitali client

- Certificati digitali (CA interna)

Oplon secure Access: architecture end-to-end (SASE)

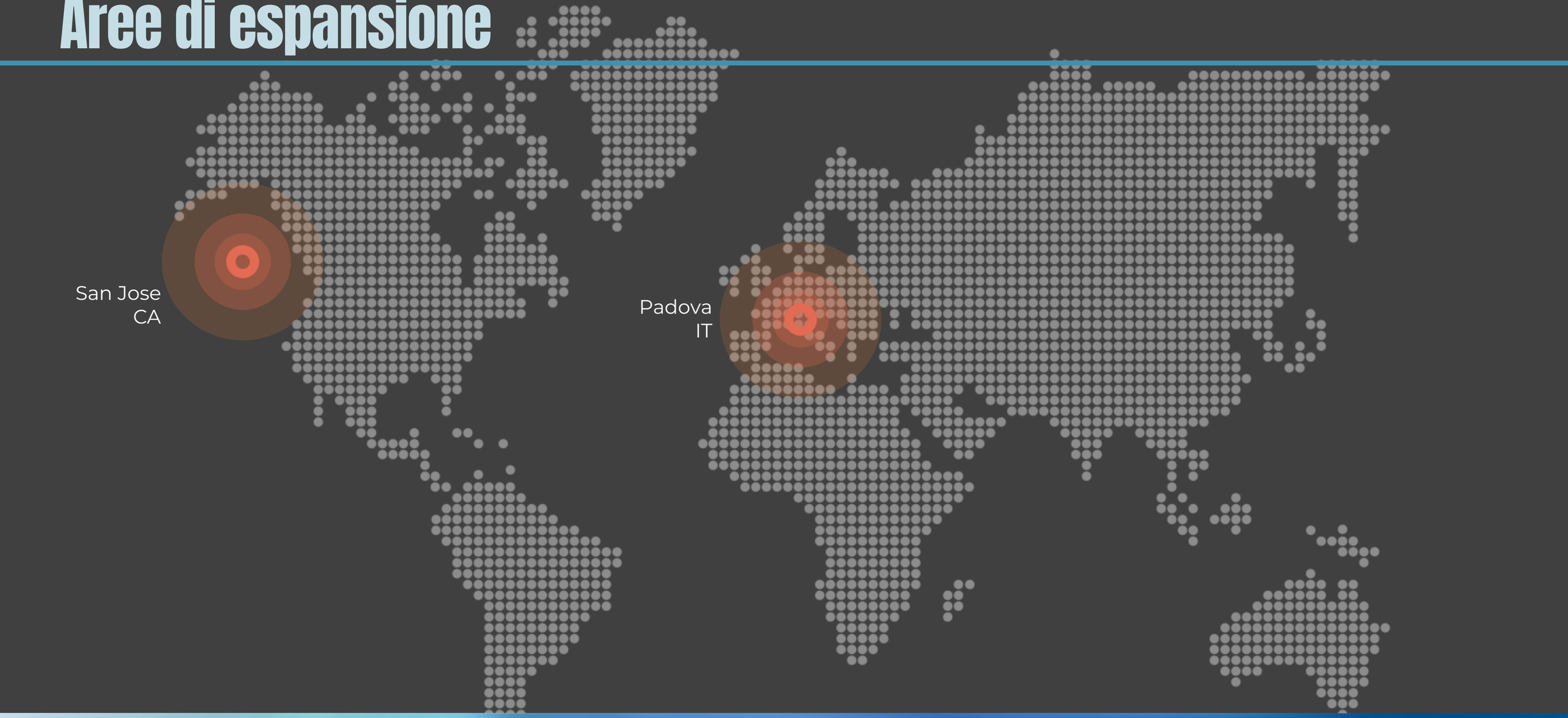






POC = 4-6 hours!

Aree di espansione



oplon®

info@oplon.net
www.oplon.net

Vieni a trovarci al nostro stand!

Clusit 25th 2000-2025

SECURITY SUMMIT

oplon®