CERBEYRA
your safe digital future

Sovranità Digitale & Intelligence

Seguici su

Priorità chiave che motivano le decisioni sulla sovranità digitale

Privacy
- GDPR
- DPF

Sicurezza
- NIS2
- DORA
- CAD (Codice dell'Amministrazione Digitale)

Controllo
- ACN
- AGID
- Garante Privacy

L'Unione Europea ci prova con il CLOUD SERVICES SCHEME (EUCS)

Un'infrastruttura dati federata e sicura

Gaia-X punta all'innovazione attraverso la sovranità digitale.

Il nostro **obiettivo** è creare un ecosistema in cui i dati vengano condivisi e resi disponibili in un ambiente affidabile.

Il nostro **intento** è restituire il controllo agli utenti, mantenendo la sovranità sui loro dati.

Il nostro **risultato** non sarà un cloud. È un sistema federato che collega molti provider di servizi cloud e utenti insieme in un ambiente trasparente che guiderà l'economia dei dati europea di domani.

gaia-x

GAIA-X è un'iniziativa europea lanciata nel 2019 per creare un'infrastruttura digitale aperta, sicura e sovrana per il trattamento e la gestione dei dati. Il progetto nasce dalla necessità di garantire maggiore autonomia e sicurezza nella gestione dei dati in Europa, in un contesto dominato dai grandi provider di cloud statunitensi (come Amazon Web Services, Microsoft Azure e Google Cloud) e cinesi.

Sovranità Digitale e gli hyperscaler

CERBEYRA
your safe digital future

Gli hyperscaler rispondono alle richieste di sovranità digitale

20 marzo 2023

Google offre un portafoglio di **Sovereign Solutions** ed il tool Digital Sovereignty Explorer di Google Cloud.

20 giugno 2023

Oracle serve i clienti tramite il suo servizio **EU Sovereign Cloud** ospitato in Spagna e Germania.

3 ottobre 2023

Microsoft lancia Microsoft **Cloud for Sovereignty** per soddisfare il settore governativo globale.

25 ottobre 2023

AWS annuncia il suo **Digital Sovereignty Pledge** concentrandosi sul mercato tedesco.

CERBEYRA
your safe digital future

Potenziali svantaggi degli hyperscaler

Rischi di sicurezza e privacy

A causa della loro dimensione e visibilità, gli hyperscaler sono spesso obiettivi primari per attacchi informatici su larga scala. Anche se investono molto in sicurezza, la loro dimensione li rende più esposti a tentativi di attacco sofisticati. L'uso condiviso delle risorse su larga scala può aumentare i rischi di violazioni della sicurezza, anche se le divisioni virtuali tra i clienti sono progettate per essere sicure.

Difficoltà nel controllo dei dati

Gli hyperscaler gestiscono tutta l'infrastruttura fisica e l'orchestrazione delle risorse cloud, il che può comportare una minore trasparenza o controllo per l'utente finale su come vengono gestiti i dati e le risorse. Alcune aziende preferiscono non affidarsi completamente a soluzioni cloud pubbliche per motivi di sicurezza o proprietà dei dati, e gli hyperscaler potrebbero non offrire soluzioni private o on-premises sufficientemente flessibili.

Localizzazione e compliance

Poiché gli hyperscaler operano su scala globale, potrebbero non essere in grado di rispondere in modo ottimale alle esigenze normative e di compliance specifiche di un mercato locale. In alcuni settori regolamentati o in specifici paesi, c'è preoccupazione riguardo alla sovranità dei dati.

Complessità di gestione

vasta gamma di servizi, la gestione può diventare molto complessa, specialmente per aziende più piccole o con team IT limitati. L'interfaccia e la varietà di opzioni possono risultare difficili da navigare.

Costi elevati

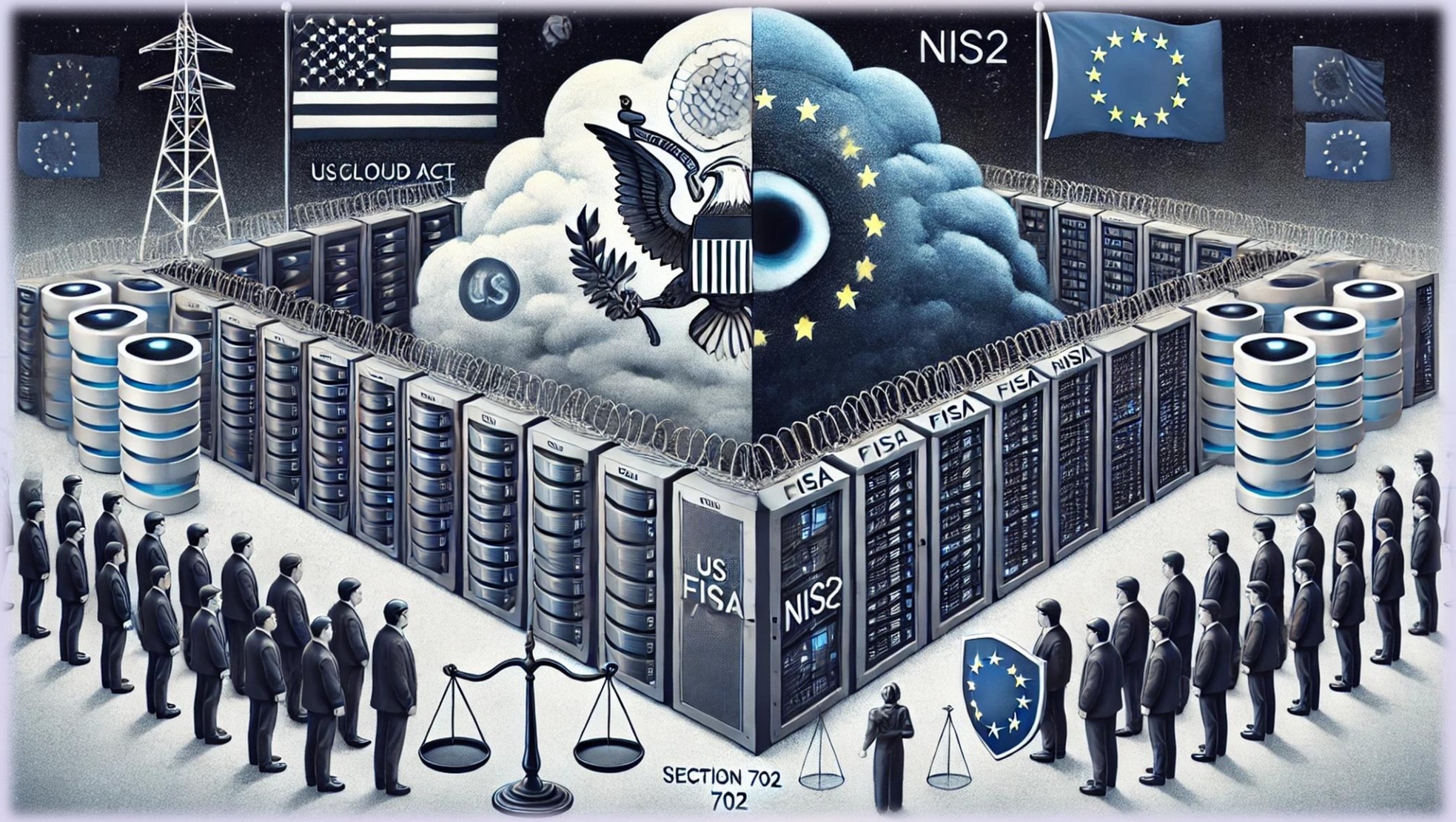
Il pricing degli hyperscaler può essere complesso e difficile da prevedere. Le aziende rischiano costi imprevisti legati a dati in uscita, storage o altre risorse. Nonostante le economie di scala, i costi possono aumentare rapidamente con l'uso crescente, rappresentando un problema per aziende con budget limitati.

Lock-in tecnologico (vendor lock-in)

Una volta che un'azienda adotta i servizi di un hyperscaler, può diventare difficile e costoso migrare a un altro cloud provider o tornare a soluzioni on-premises. Spesso i servizi cloud di un hyperscaler usano tecnologie e API proprietarie, rendendo difficile l'interoperabilità o il trasferimento verso altri fornitori.

CERBEYRA
your safe digital future

..e la normativa ?



LEGGI EXTRATERRITORIALI AMERICANE

Le Big Tech statunitensi sono soggette a leggi come il Patriot Act, Cloud Act (Clarifying Lawful Overseas Use of Data Act) e la sezione 702 del Foreign Intelligence Surveillance Act (FISA) che consente alle autorità americane di richiedere l'accesso ai dati detenuti da società statunitensi, anche se questi dati sono ospitati al di fuori degli Stati Uniti e di proprietà di utenti stranieri.

Il Data Protection Framework (EU-U.S. Data Privacy Framework), l'autocertificazione è una delle principali caratteristiche del Data Protection Framework. Assenza di verifiche indipendenti, Conformità volontaria se l'azienda americana non aderisce può comunque trasferire i dati attraverso meccanismi già previsti nel GDPR come :

- Clausole contrattuali standard (SCCs)
- Norme vincolanti d'Impresa (BCRs)
- Deroghe specifiche ai sensi dell'articolo 49 del GDPR

CAPACITA' STRATEGICA

La sovranità digitale implica non solo la protezione dei dati e la loro gestione all'interno del territorio nazionale, ma anche il controllo sull'infrastruttura digitale strategica. L'affidamento alle Big Tech riduce la capacità strategica dell'Italia di sviluppare tecnologie indipendenti e controllare le proprie risorse digitali.

Codice chiuso: software proprietario, significa che le autorità italiane o europee non hanno piena visibilità o controllo su come vengono gestiti i dati, né possono verificare in modo indipendente la sicurezza di tali sistemi.

Vulnerabilità: Senza accesso al codice sorgente, è difficile per le autorità italiane verificare se esistono backdoor o vulnerabilità nel sistema che potrebbero essere sfruttate da entità esterne.

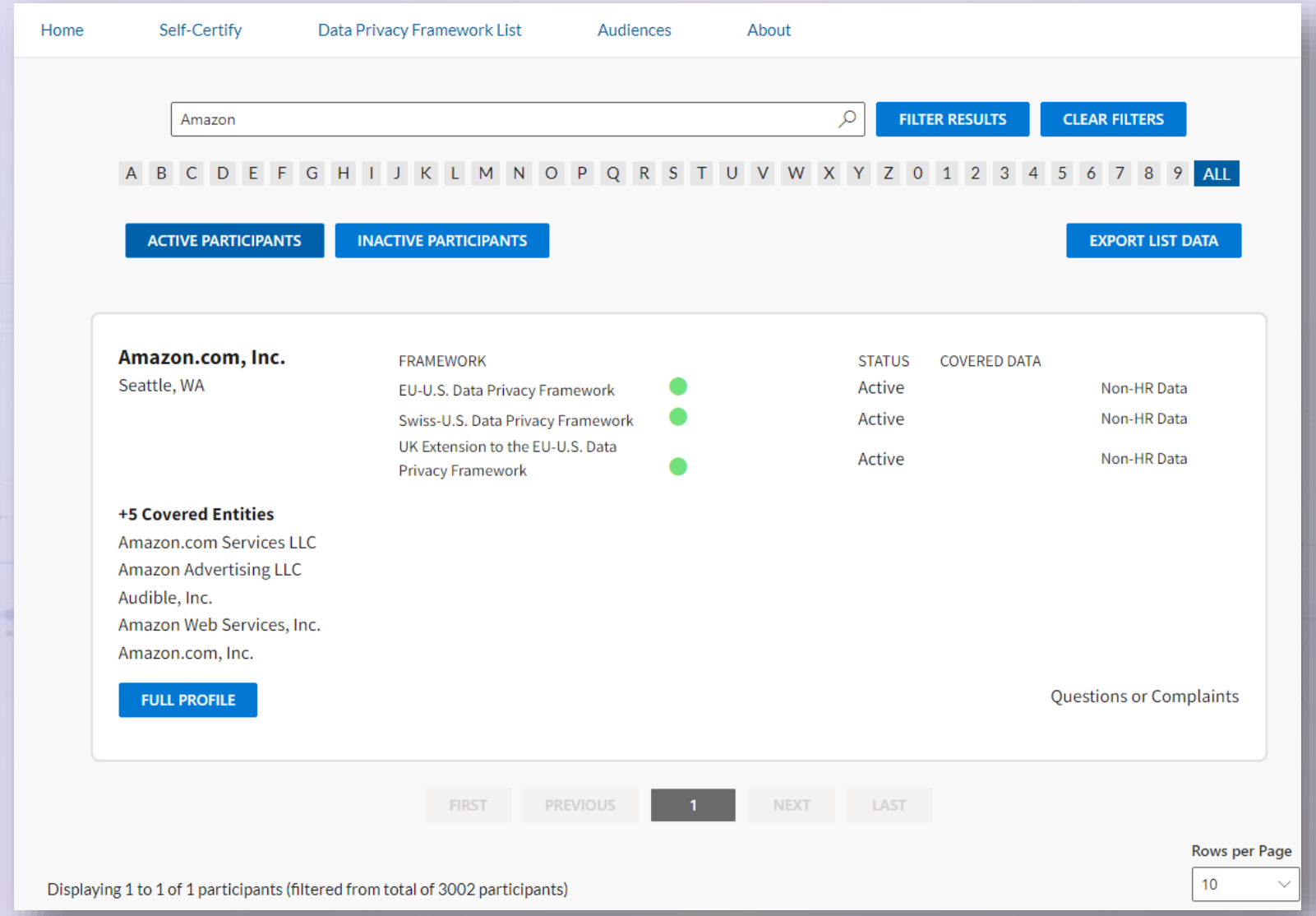
Mancanza di Controllo: L'Italia non ha controllo diretto su molte delle tecnologie critiche utilizzate per la gestione dei dati. In caso di conflitto geopolitico o commerciale, l'Italia potrebbe non avere il pieno controllo sui propri sistemi digitali.

https://nsa.gov1.info/utah-data-center/

La vera libertà non è solo vivere senza catene ma anche poter camminare in mezzo alla folla senza essere osservati.

Oggi, anche una semplice foto di una folla può rivelare dettagli individuali, poiché algoritmi avanzati possono riconoscere e identificare le persone, minando l'idea stessa di anonimato.

https://www.dataprivacyframework.gov/list

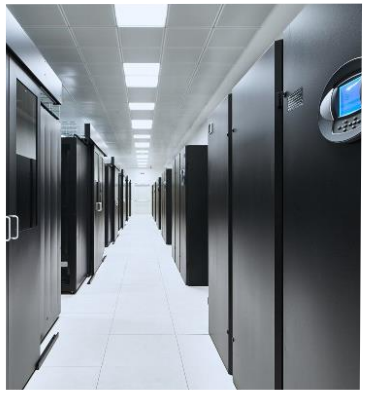


Ecosistemi Digitali Nazionali

sovranità digitale senza compromessi, controllo e sicurezza oltre gli hyperscaler

Benvenuti nell'ecosistema

vianova



La tua sovranità digitale inizia qui

Livello 1 : **Il controllo**

vianova

Sovranità digitale non significa solo proteggere i dati, ma garantirti il pieno controllo su di essi.

68,9%

è la percentuale di disservizi intercettati e anticipati ai Clienti nel 2023

95,1%

risposte in 3 squilli

la percentuale di chiamate a cui abbiamo risposto in 3 squilli nel 2023

2 Data Center

Data Center localmente e geograficamente ridondati

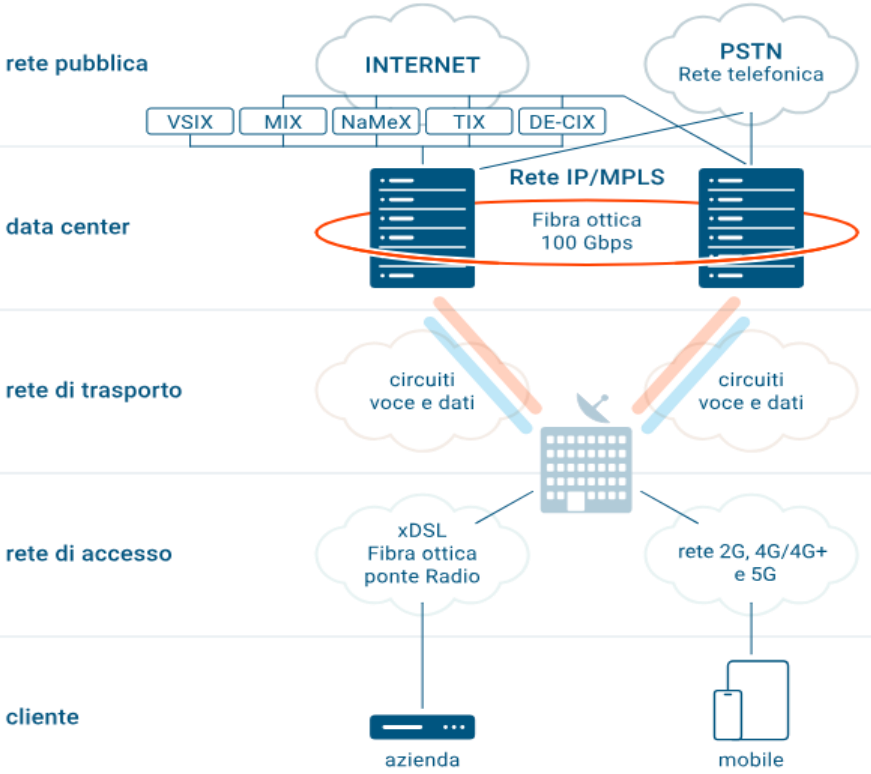
16 POP

(Point Of Presence) colocati presso le infrastrutture di Telecom Italia rilegati in fibra e ridondati con i due Data Center

30 Aree di raccolta

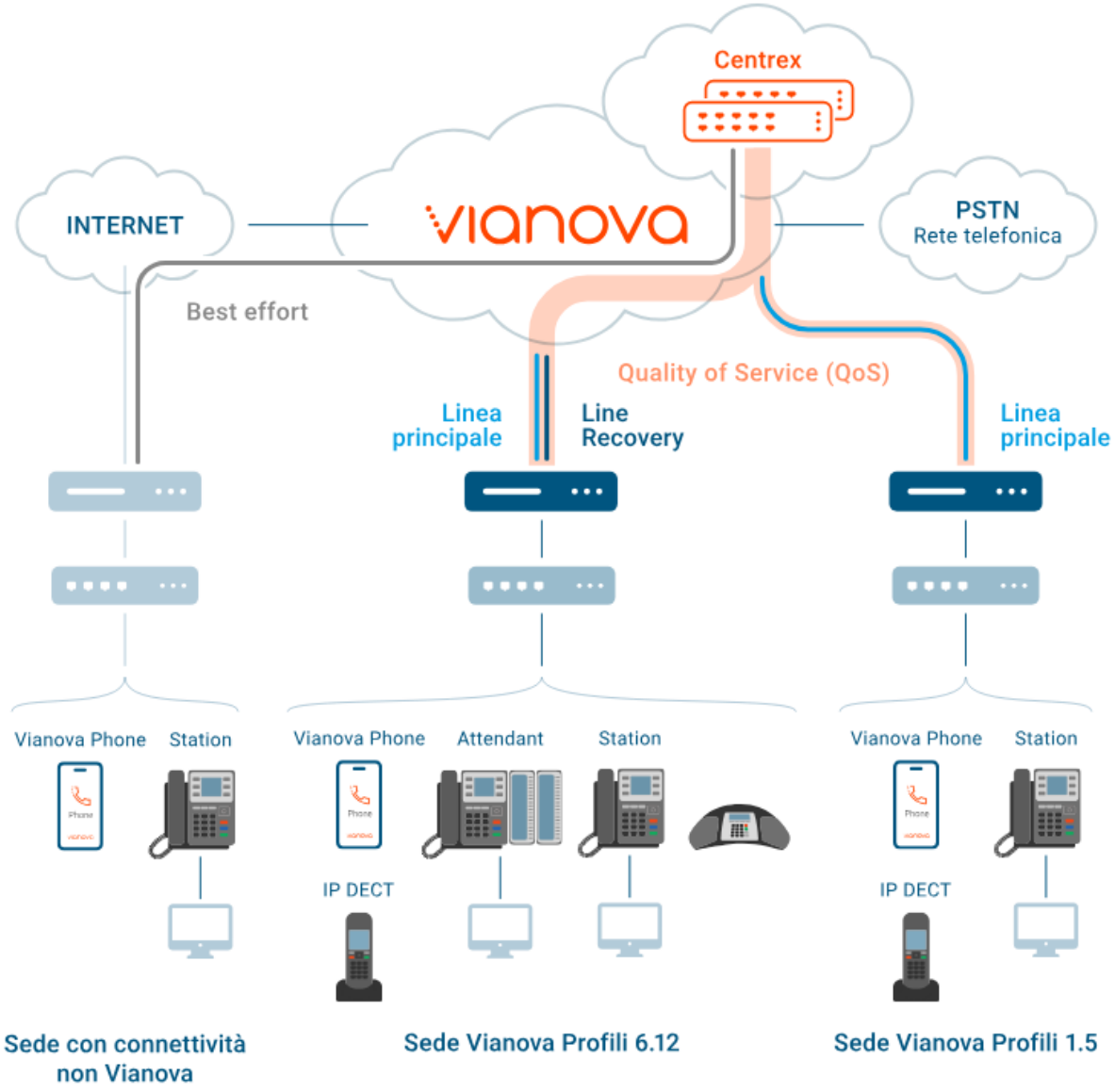
Interconnessioni con le Aree di Raccolta ridondate con i due Data Center

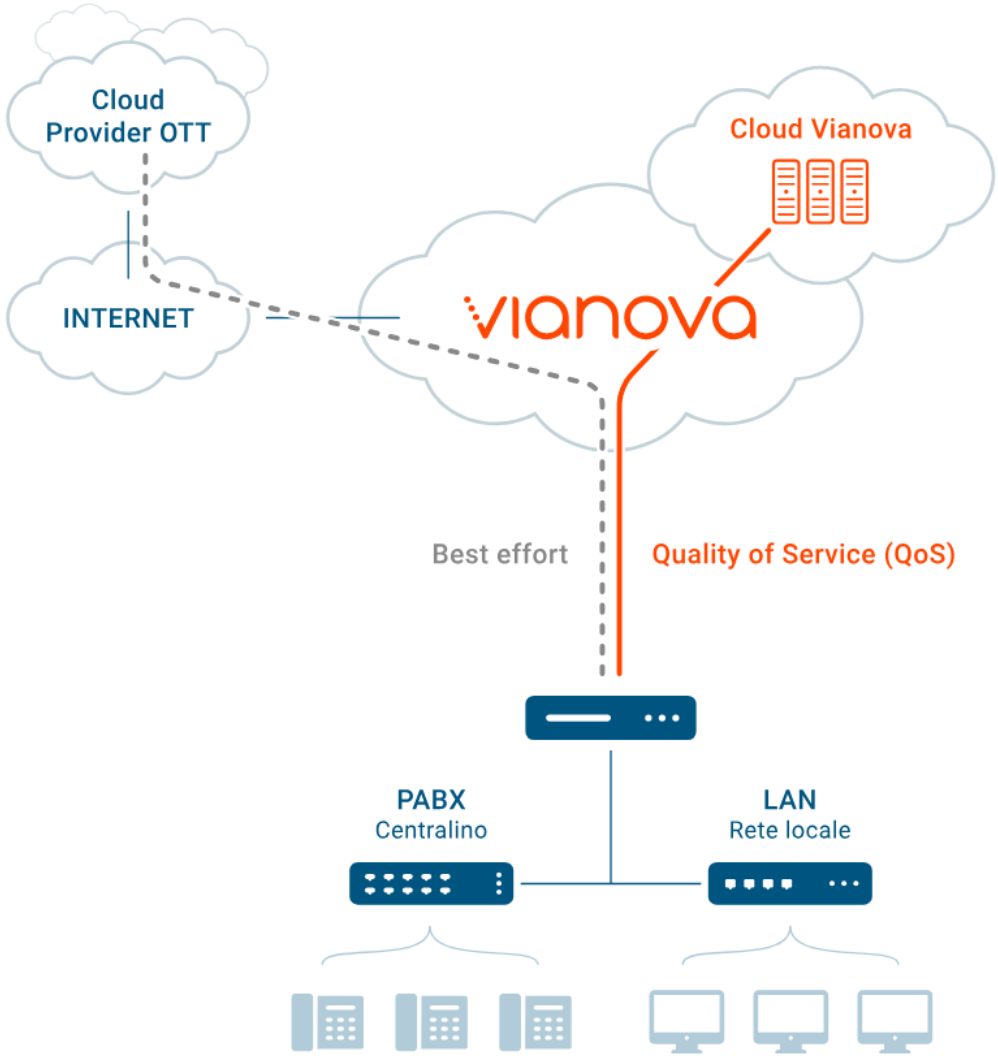
La rete Vianova, basata su un'infrastruttura di ultima generazione (NGN), costituisce la portante di tutti i servizi trasmissivi dell'azienda e permette di erogare servizi di telecomunicazione e IT con i più alti livelli di affidabilità, sicurezza e bassa latenza.



Livello 2 : **l'affidabilità**

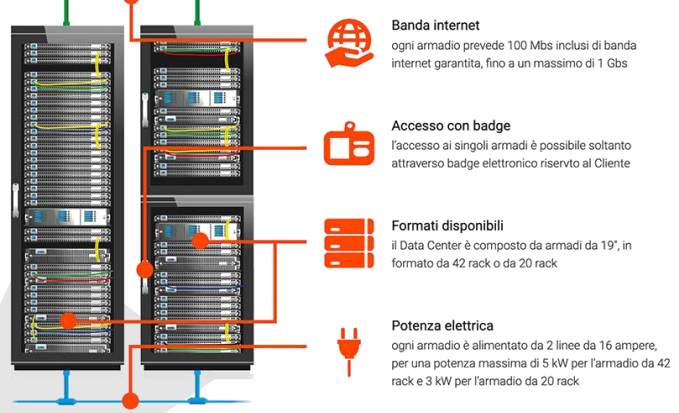
Qualità del servizio: Separazione Voce, Dati e Cloud

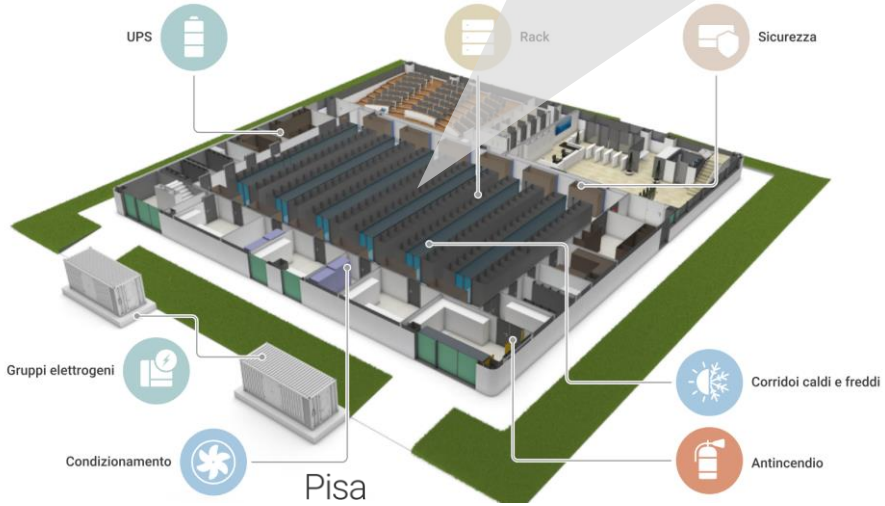


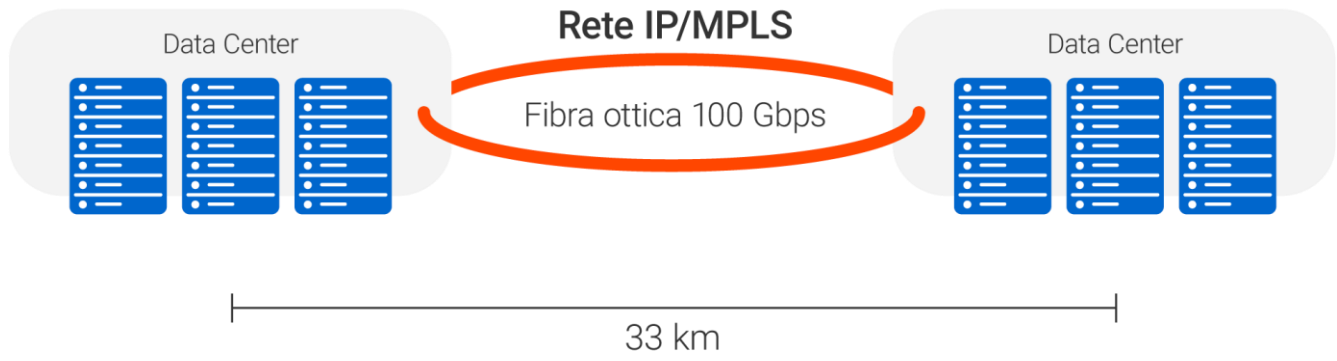


Affidabilità e Privacy senza Compromessi

Data Center **Tier IV compliant**, sono realizzati con sistemi di sicurezza, alimentazione, condizionamento e ridondanza in grado di prevenire interruzioni dei servizi ed assicurare la business continuity anche in caso di manutenzione, guasto o incidente.







ISO 9001 — ISO/IEC 27001

Agenzia per la cybersicurezza nazionale

Infrastrutture digitali e dei Servizi cloud

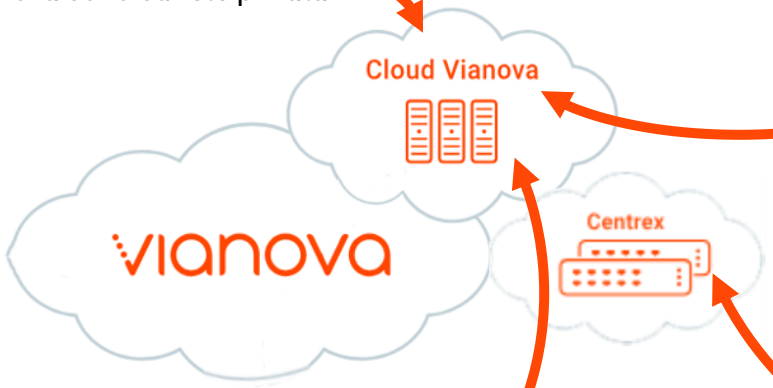
Vianova Cloud — Livello di qualificazione 2

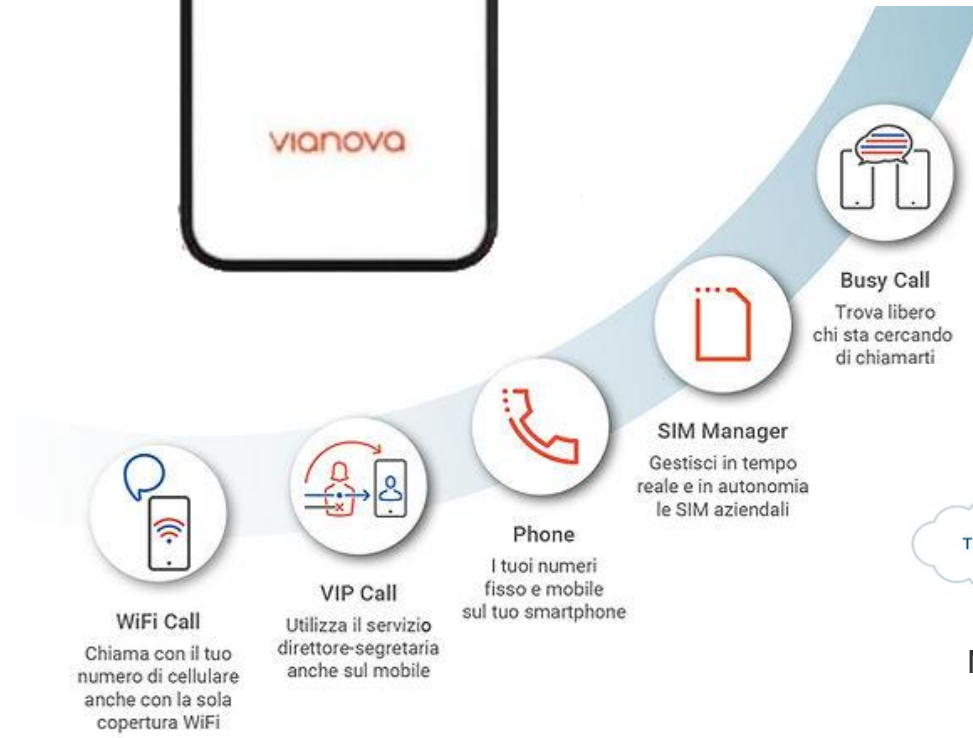
Livello 3 : **la sicurezza**

La sicurezza nelle telecomunicazioni è la chiave per proteggere la tua voce e custodire i tuoi dati.

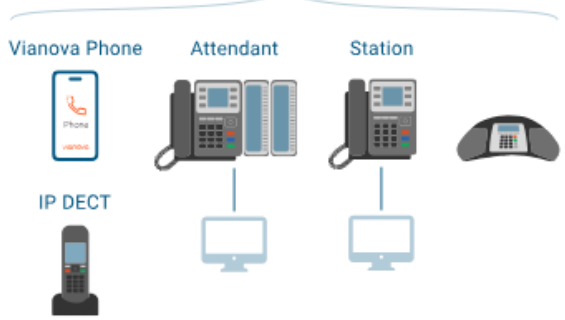
Le comunicazioni dati delle SIM Vianova sono su rete privata

Tutte i dati ed i servizi Vianova come ad es. Hosting, Mail, Meeting, Drive, etc.. sono gestiti e ospitati nei datacenter Vianova.





Uno spazio di backup nel **Cloud italiano di Vianova** in cui salvare una copia dei tuoi dati Microsoft come documenti, caselle di posta elettronica, singole mail, allegati e note.



Centralino telefonico in Cloud Vianova

CERBEYRA
your safe digital future

Cyber Security integrata

Integrazione e riduzione dei costi

Totale integrazione con l'infrastruttura del cliente per una maggiore efficienza e con il FWaaS, i clienti possono accedere a una soluzione di sicurezza avanzata con un costo prevedibile basato su abbonamento, evitando spese iniziali elevate e riducendo i costi operativi.

Sicurezza avanzata senza complessità

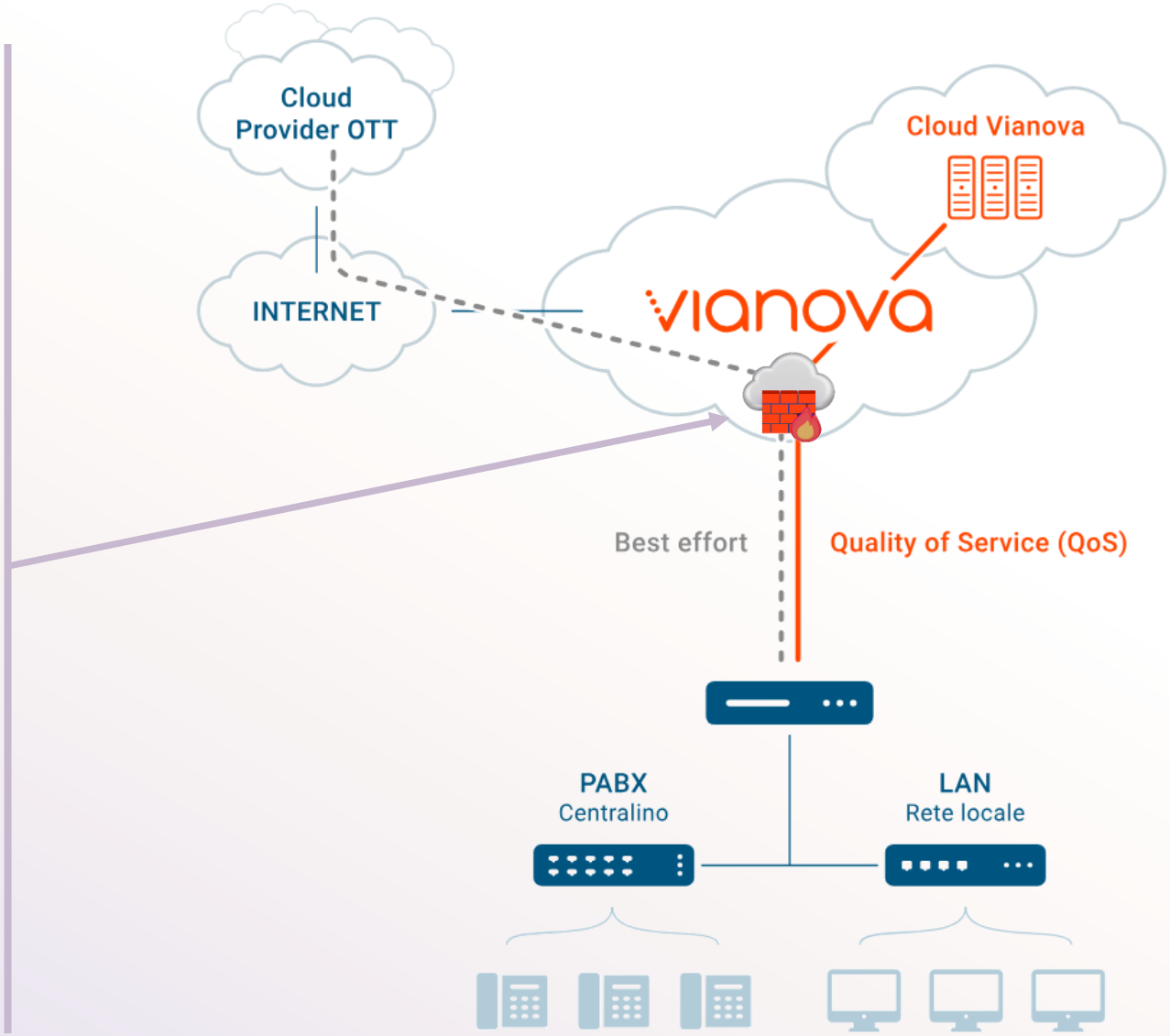
Con il FWaaS, i clienti possono beneficiare di **protezione di alto livello** senza dover gestire direttamente l'hardware o la complessità delle configurazioni.

Scalabilità senza limiti

I firewall tradizionali possono diventare rapidamente insufficienti man mano che un'azienda cresce. Con il FWaaS, la **scalabilità è semplice e immediata**, adattandosi alle necessità dell'azienda senza dover acquistare o configurare nuovo hardware. Questo permette alle aziende di espandere le loro operazioni digitali senza preoccuparsi di limiti di sicurezza.

Protezione globale

Il FWaaS offre una protezione globale a livello di rete, coprendo tutti i dispositivi e utenti, indipendentemente da dove si trovano.



Livello 4 : **l'intelligence**

CERBEYRA
your safe digital future

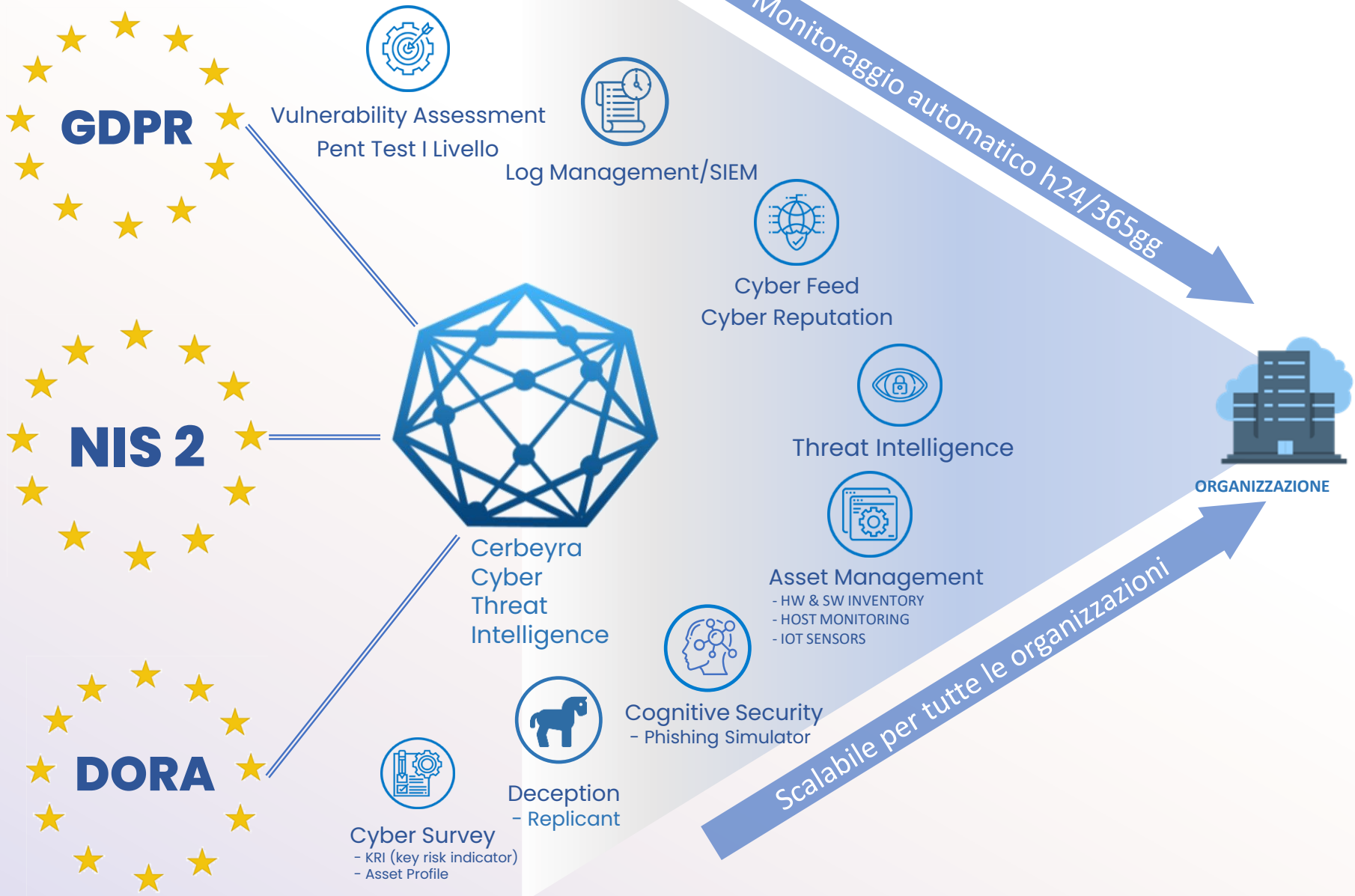
Misurare il livello di Cyber Security dell'organizzazione

L'art. 32 del GDPR, al comma 1 lettera d), richiede al titolare di definire **una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative**.

La **Direttiva NIS2** prevede tra i sui principali **requisiti minimi** :

1. **analizzare e valutare i rischi di sicurezza dei sistemi informativi con operazioni di vulnerability assessment, penetration test ecc.;** gestire gli incidenti di sicurezza informatici con un piano e **un'attività di monitoraggio continuo** e incident response;
2. **testare regolarmente la sicurezza dell'infrastruttura IT e l'efficacia delle misure di gestione del rischio adottate; assicurare la sicurezza delle supply chain**, controllando che i propri fornitori dispongano di adeguati requisiti in termini di sicurezza.

Art. 21 del DORA, le entità finanziarie dovrebbero disporre di politiche per **testare sistemi, controlli e processi ICT, nonché per la gestione del rischio ICT di terze parti.**



CERBEYRA
your safe digital future

Vola S.p.A. | Gruppo Vianova S.p.A.

"La sovranità digitale è la chiave per proteggere il futuro, chi gestisce i dati, controlla il destino."

Grazie per l'attenzione

web : www.cerbeyra.com

mail : info@cerbeyra.com

Seguici su