



Powered by Gyalá

**HEALTH
CYBER RESILIENCE**

Cyber Resilience

IT/OT

per il settore

sanitario





**HEALTH
CYBER RESILIENCE**

5 Moduli

Extended Detection
and Response

Network Security
Appliance

Risk Management Tool

Correlation Module

OT Defence

4 Funzionalità in un'unica piattaforma

Gyala è l'unico Vendor di Cyber Security ad aver portato l'automazione dei processi di Detection e Reaction anche all'interno dei singoli agent.

Agger è l'unica piattaforma **Made in Italy all-in-one** di Cyber Security che, grazie a sofisticati algoritmi di intelligenza artificiale di derivazione militare, è in grado di prevenire, identificare e gestire automaticamente ogni tipo di minaccia di tipo informatico, massimizzando la IT/OT resilience dell'infrastruttura aziendale.

Detection

Identifica condizioni anomale tramite l'analisi comportamentale dei processi in esecuzione nei computer, del traffico di rete, dei log di sicurezza già disponibili nelle infrastrutture e grazie alla verifica d'integrità e disponibilità dei dispositivi OT.

Artificial Intelligence

Crea modelli comportamentali dinamici sulla base dei dati raccolti e li utilizza per identificare eventuali scostamenti.

Reaction

Le reazioni vengono eseguite dagli agent pre-istruiti con le azioni di contenimento e contrasto che gli esperti di Cyber Security eseguirebbero affrontando i vari tipi di incidente o comandando azioni sul sistema IT/OT stesso o guidando gli operatori umani con procedure operative manuali dettagliate. **Le regole di reaction (e detection) sono personalizzabili per singolo agent/endpoint e sistema OT, consentendo di ottenere la resilienza dei servizi IT/OT difesi.**

Investigation

Raccoglie informazioni, eventi e incidenti utili per la post-analysis degli esperti di cyber security.



**HEALTH
CYBER RESILIENCE**

**REGOLE CUSTOMIZZABILI
ANCHE PER SINGOLO AGENT**

PIATTAFORMA ALL-IN-ONE

CLOUD | ON PREMISE | RETI SEGREGATE

SUPPORTA OGNI SISTEMA LEGACY

RESILIENZA IT/OT

DETECTION & REACTION AUTOMATICHE

ESTESA THREAT INTELLIGENCE

PREVIENE | IDENTIFICA | GESTISCE

**TEMPO MEDIO DI REAZIONE
ZERO SECONDI**

UN AGGER PER OGNI MERCATO:

**INDUSTRIAL
CYBER RESILIENCE**

**NAVAL
CYBER RESILIENCE**

**HEALTH
CYBER RESILIENCE**

**ENTERPRISE
CYBER RESILIENCE**

**PMI
CYBER RESILIENCE**

**UTILITIES
CYBER RESILIENCE**

**PA
CYBER RESILIENCE**

**DEFENCE
CYBER RESILIENCE**

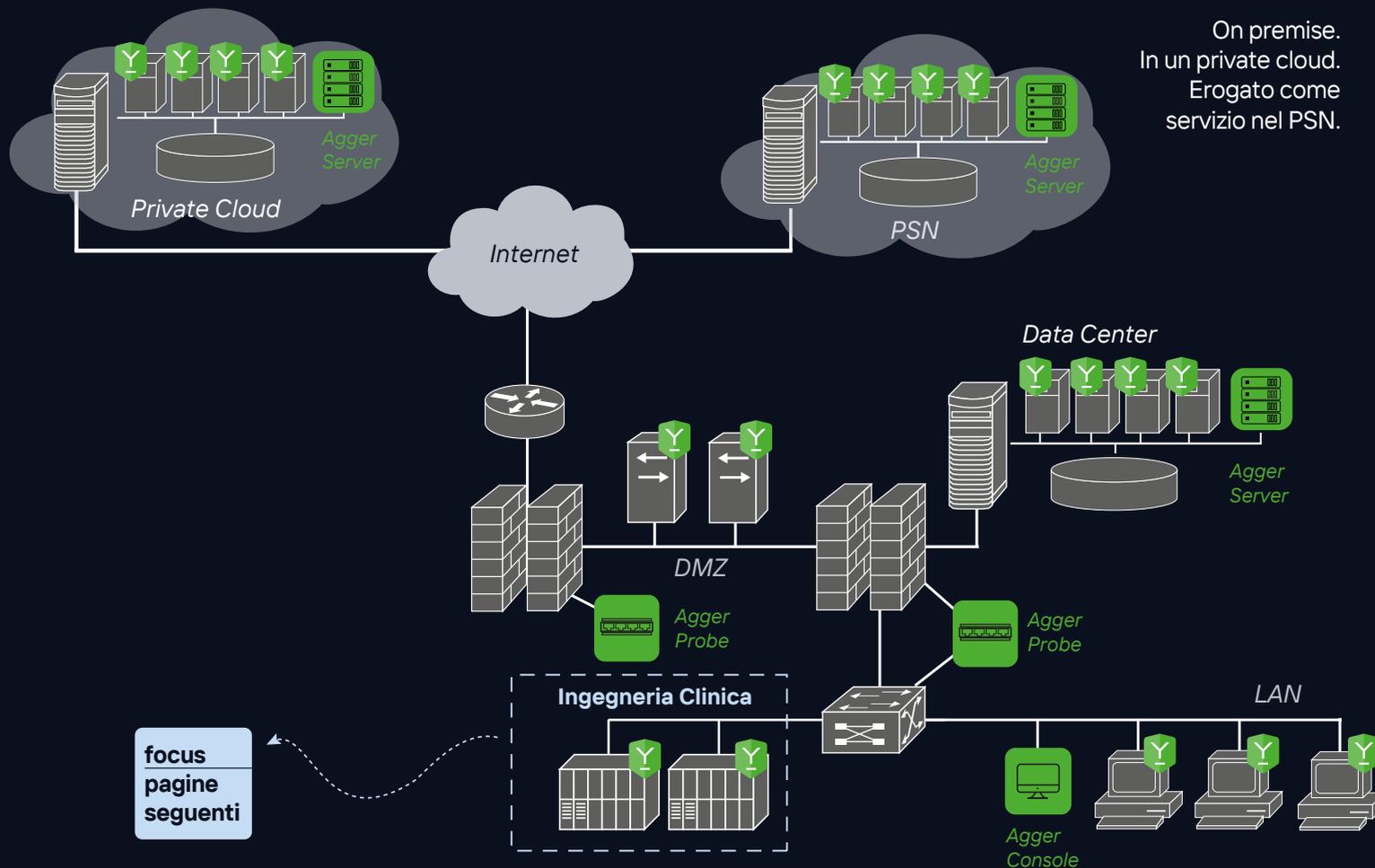
**FINANCE
CYBER RESILIENCE**

Come lavora Agger:

Agger Server
può essere:

On premise.
In un private cloud.
Erogato come servizio nel PSN.

- ← Vengono installati agent per l'analisi comportamentale dei processi in esecuzione, sonde per l'analisi passiva delle comunicazioni di rete e un sistema di monitoraggio attivo delle interfacce esposte dagli apparati agentless.
- ← Agger mappa e studia tutti i processi e connessioni.
- ← Riconosce un attacco e reagisce in 0 secondi.
- ← Applica la reaction più adatta secondo regole custom.
- ← In ambito OT, se richiesto, ripristina lo stato pre-attacco.
- ← Salva log e telemetrie per le analisi post incidente.



NB



Possibilità di creare regole di detection e reaction sia a livello centralizzato che a livello di singolo agent, per ottenere la resilienza dei servizi erogati da tutti i sistemi anche legacy.



Un'unica piattaforma con cui coprire tutti i requisiti tecnici, di analisi del rischio e reportistici per Identificazione, Protezione, Rilevamento, Risposta e Recupero richiesti dalle autorità nazionali (ACN).

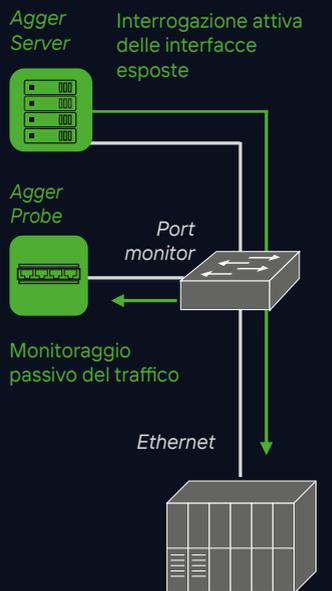


Consente di ottenere la massima protezione senza interferire o limitare l'erogazione dei servizi operativi sanitari.



Possibilità di assegnare tag personalizzati (colore e testo) ad ogni end point e apparato agentless per creare raggruppamenti logici. Ad esempio la posizione fisica, il servizio a cui appartengono, il fornitore che li gestisce, ecc...utili sia per l'analisi del rischio che in fase di gestione dell'incidente.

Tipologia 1



DEVICE ELETTROMEDICALI direttamente collegati alla rete

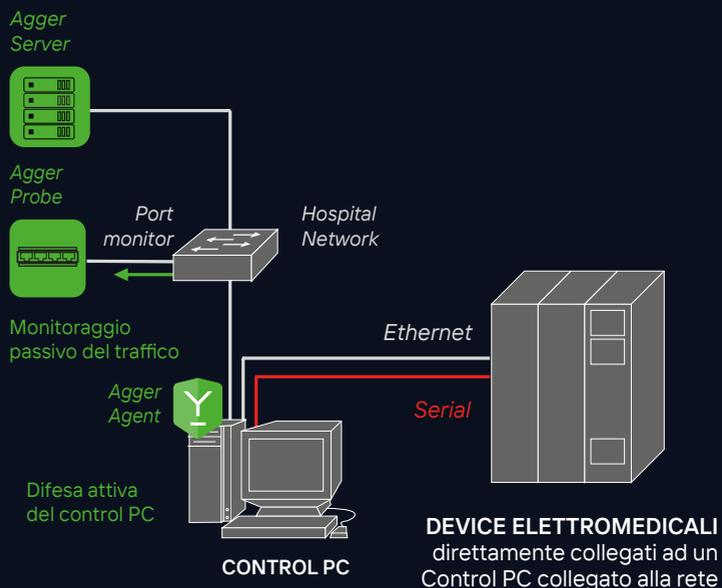
FOCUS INGEGNERIA CLINICA

La soluzione per le aziende sanitarie:

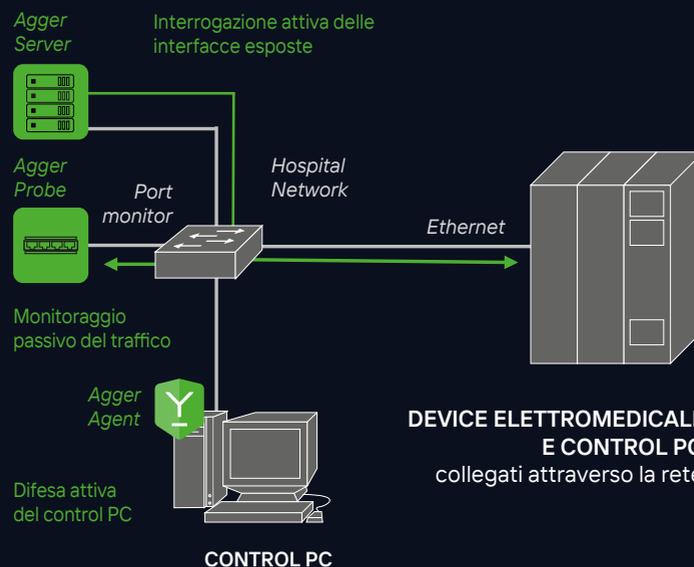
Nel 2019, le aziende sanitarie nazionali sono state incluse nel Perimetro di Sicurezza Nazionale Cibernetica in quanto strutture strumentali all'esercizio di funzioni essenziali dello Stato e necessarie per l'esercizio e il godimento dei diritti fondamentali. L'ACN ha messo a disposizione delle infrastrutture critiche il Framework Nazionale di Cybersecurity, un importante strumento per la realizzazione di un sistema di gestione della sicurezza Cyber. **Il Framework richiede la definizione di concrete azioni dal punto di vista organizzativo, procedurale e tecnico** per la prevenzione, identificazione e gestione degli incidenti informatici, e **ha esteso il perimetro delle infrastrutture da difendere** oltre che ai sistemi informatici e di telecomunicazione, anche **a tutti gli apparati fisici connessi in rete, come gli elettromedicali.**

Gyala ha sviluppato un processo di messa in sicurezza degli elettromedicali dell'ingegneria clinica, attraverso soluzioni dedicate alle varie tipologie di apparati, che consente la piena compliance ai requisiti tecnici del Framework Nazionale di Cyber Security.

Tipologia 2



Tipologia 3



Gyala, Al sicuro. Sempre.

Agger, Soluzione Custom Made

Agger, la nostra soluzione di **Cyber Security all-in-one** interamente modulabile e personalizzabile, offre supervisione e reazione automatica per ogni tipo di rischio, grazie a un sofisticato sistema AI di derivazione militare, che garantisce stabilità e resilienza degli ambienti IT e OT.

Innovazione Made in Italy

Gyala coniuga l'**approccio "agile"** tipico di una startup innovativa con il consolidato **know-how maturato** dai 3 Founder nella gestione di progetti di Cyber Protection di infrastrutture critiche, sviluppati grazie al PNRM, con il Ministero della Difesa e ora sul mercato grazie ai principali System Integrator nazionali.

Sviluppiamo soluzioni all'avanguardia di Automatic Defense per proteggere le risorse strategiche IT e OT di aziende pubbliche e private dagli attacchi informatici.

Gyala, il tuo Technology Partner

Grazie alla nostra **pluriennale esperienza in ambito di Difesa**, affrontiamo con competenza e **con la massima efficienza** le sfide crescenti del panorama della cybersecurity.

Ci avvaliamo di un ecosistema di system integrator, advisor company e solution provider che integrano la nostra soluzione all'interno dell'infrastruttura del cliente.



ISO 9001:2015
ISO IEC 27001



COMPLIANCE NIS2
E REQUISITI
FRAMEWORK
CYBERSECURITY
NAZIONALE



CYBERSECURITY
MADE IN EUROPE



marketing@gyala.com

gyala.com  [Gyala](#)