AGGER
Powered by Gyala

HEALTH

CYBER RESILIENCE

Automated Cyber Resilience **IT/OT/IoT** per il settore **Sanitario**

GYALA
Cyber Security

AGGER
Powered by Gyala

5 Moduli

Endpoint Detection and Response

Network Security Appliance

Risk Management Tool

Correlation Module

OT Defence

Agger è la piattaforma di Cyber Automated Resilience **100% Made in Italy** progettata per proteggere infrastrutture IT, OT e IoT. Integra detection, analisi comportamentale e reaction automatica in un'unica architettura modulare e personalizzabile, riducendo il tempo di esposizione alle minacce e aumentando la resilienza dei servizi.

L'automazione e la personalizzazione delle regole di Detection & Reaction arrivano fino al singolo agent o endpoint.

4 Funzionalità in un'unica piattaforma

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

Applica automaticamente azioni di contenimento e contrasto attraverso playbook personalizzabili. Le reaction possono essere definite a livello di singolo agent, endpoint o sistema OT e possono agire direttamente sui sistemi o guidare l'operatore attraverso procedure dedicate.

Investigation

Raccoglie e correla eventi, incidenti e informazioni di contesto, mettendo a disposizione degli analisti gli elementi necessari per investigazione, threat hunting e post-analysis.

AGGER
Powered by Gyala

Cyber Resilience IT/OT/IoT

AUTOMATICA. PERSONALIZZABILE. IN TEMPO REALE.

DIFESA PER TUTTI I SISTEMI IT/OT
ANCHE LEGACY

INSTALLAZIONE
- CLOUD
- ON PREMISES
- RETI SEGREGATE

<1 SECONDO
TEMPO MEDIO
DI REAZIONE

INTEGRABILE CON SERVIZI GESTITI
(ES. SOC, SIEM)
LADDOVE GIÀ PRESENTI

Tempo medio di reazione **zero secondi**

DETECTION & REACTION
AUTOMATICHE E PERSONALIZZABILI

anche per singolo agent o endpoint

Recognized by Gartner®

SAMPLE VENDOR

2024
Emerging Tech:
AI in CPS Security

2026
Hype Cycle™ for
CPS Security

2026
Hype Cycle™ for
Zero-Trust Technology

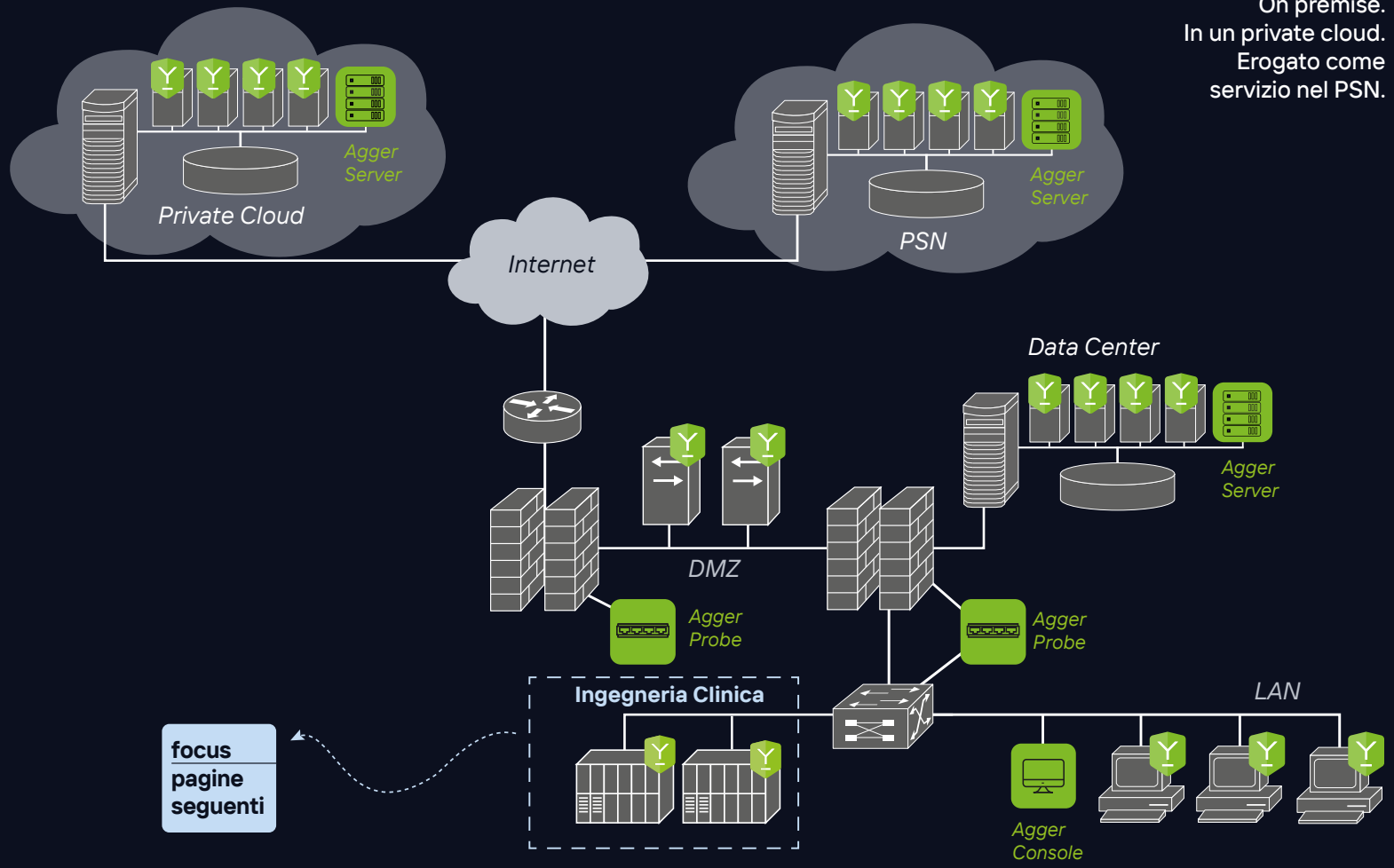
All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. Gartner does not endorse any company, vendor, product or service depicted in its publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner publications consist of the opinions of Gartner's business and technology insights organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this publication, including any warranties merchantability or fitness for a particular purpose.

Come lavora Agger:

- 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.

Agger Server può essere:

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

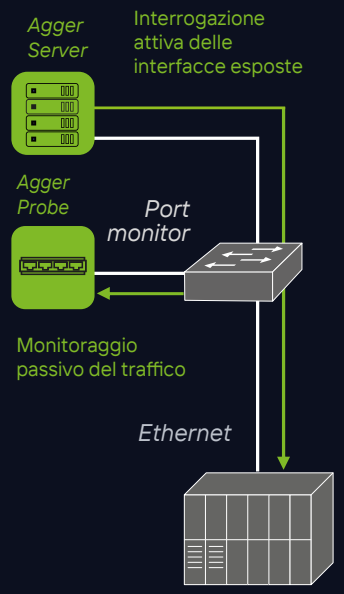


NB

- 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) a ogni end point e apparato agentless per creare insiemi 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.**

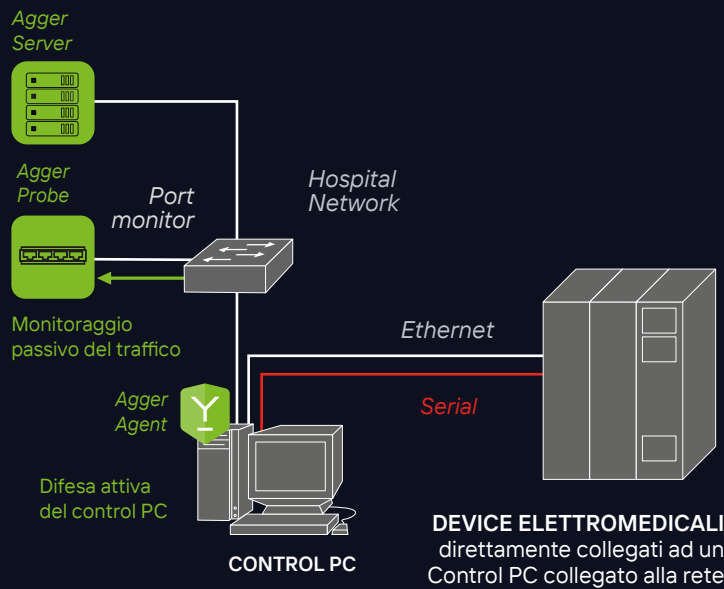
FOCUS INGEGNERIA CLINICA

Tipologia 1



DEVICE ELETTROMEDICALI
direttamente collegati alla rete

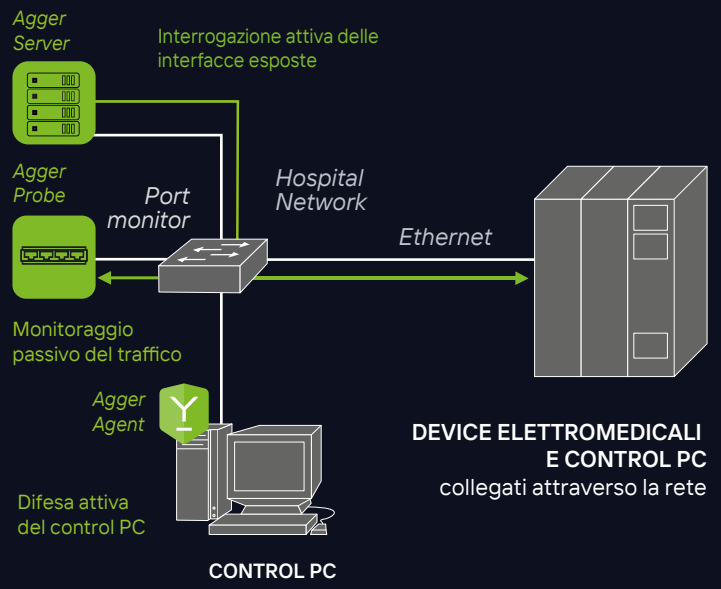
Tipologia 2



CONTROL PC

DEVICE ELETTROMEDICALI
direttamente collegati ad un Control PC collegato alla rete

Tipologia 3



CONTROL PC

DEVICE ELETTROMEDICALI E CONTROL PC
collegati attraverso la rete

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. **Ha inoltre esteso il perimetro delle infrastrutture da difendere** non solo ai sistemi informatici e di telecomunicazione, ma anche **a tutti gli apparati fisici connessi in rete (es. 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 cybersecurity.

Gyala, al sicuro. **Sempre.**

Agger, Soluzione Custom Made

Agger, la nostra **soluzione di cybersecurity** 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/OT/IoT**. Nata nel settore militare, oggi è anche a difesa delle infrastrutture civili.

Innovazione Made in Italy

Gyala è una **deep tech italiana** di Cyber Automated Security, nata per difendere ambienti critici, industriali e regolamentati, dalla **consolidata esperienza** dei 3 founder nella gestione di progetti di Cyber Protection di **infrastrutture critiche**, sviluppati con il Ministero della Difesa e con i principali System Integrator nazionali.

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

Gyala, il tuo Technology Partner

La **pluriennale esperienza in ambito di Difesa**, ci permette di affrontare **con efficienza** le sfide crescenti di cybersecurity.

Tecnologia abilitatrice per la compliance con le principali Normative come: **NIS2 · Framework Nazionale per la Cybersecurity · Regolamento Macchine (UE) 2023/1230 · DORA · IACS UR E26/E27 · IEC 62443 · Cyber Resilience Act.**

ISO 9001:2015
ISO IEC 27001

CYBERSECURITY™
MADE IN EUROPE

SCOPRI AGGER PER IL TUO SETTORE:
Consulta le soluzioni dedicate a Defence, Industrial, Naval, Health, Finance, Utilities, PA, PMI ed Enterprise.
Scarica le brochure.


GYALA
Cyber Security
marketing@gyala.com
gyala.com