AGGER

Powered by Gyala

HEALTH
CYBER RESILIENCE

IT/OT Cyber Resilience for healthcare companies

GYALA
Cyber Security

AGGER
Powered by Gyala

HEALTH
CYBER RESILIENCE

5 Modules

Extended Detection and Response

Network Security Appliance

Risk Management Tool

Correlation Module

OT Defence

Gyala is the only Cyber Security vendor to have brought the automation of the Detection and Reaction Processes even within individual agents.

Agger is the only cyber security all-in-one platform **Made in Italy** that thanks to sophisticated AI algorithms developed for military use for supervision and automatic reaction, can prevent, identify, and automatically manage any IT threat and anomaly 24/7, maximizing infrastructure IT/OT resilience.

4 Features one platform

Detection

Identifies conditions abnormal by analyzing behavioural running processes in computers, traffic network, security logs already available in infrastructure and thanks to the integrity check and availability of OT devices.

Artificial Intelligence

It creates models of dynamic behavior - based on the data collected - then used to identify any deviations.

Reaction

The reactions are performed by agents previously instructed with the actions of containment and contrast that Cyber Security experts would perform by addressing various types of incidents or controlling actions on the system IT/OT itself, or guiding human operators with operating procedures detailed manuals. **The rules of reaction (and detection) are customizable for single agent/endpoint and OT system, allowing you to get the resilience of IT/OT services defended.**

Investigation

It collects information, events and incidents useful for the post-analysis by the cyber security experts.

AGGER
Powered by Gyala

HEALTH
CYBER RESILIENCE

CUSTOMIZABLE RULES ALSO FOR EACH AGENT

ALL-IN-ONE PLATFORM

CLOUD | ON PREMISE | SEGREGATED NETWORKS

SUPPORTS EVERY LEGACY SISTEMS

IT/OT RESILIENCE

AUTOMATIC DETECTION & REACTION

EXTENSIVE THREAT INTELLIGENCE

PREVENTS | IDENTIFIES | MANAGES

AVERAGE REACTION TIME 0 SECONDS

AN AGGER FOR EACH MARKET:

INDUSTRIAL CYBER RESILIENCE

NAVAL CYBER RESILIENCE

HEALTH CYBER RESILIENCE

ENTERPRISE CYBER RESILIENCE

PMI CYBER RESILIENCE

UTILITIES CYBER RESILIENCE

PA CYBER RESILIENCE

DEFENCE CYBER RESILIENCE

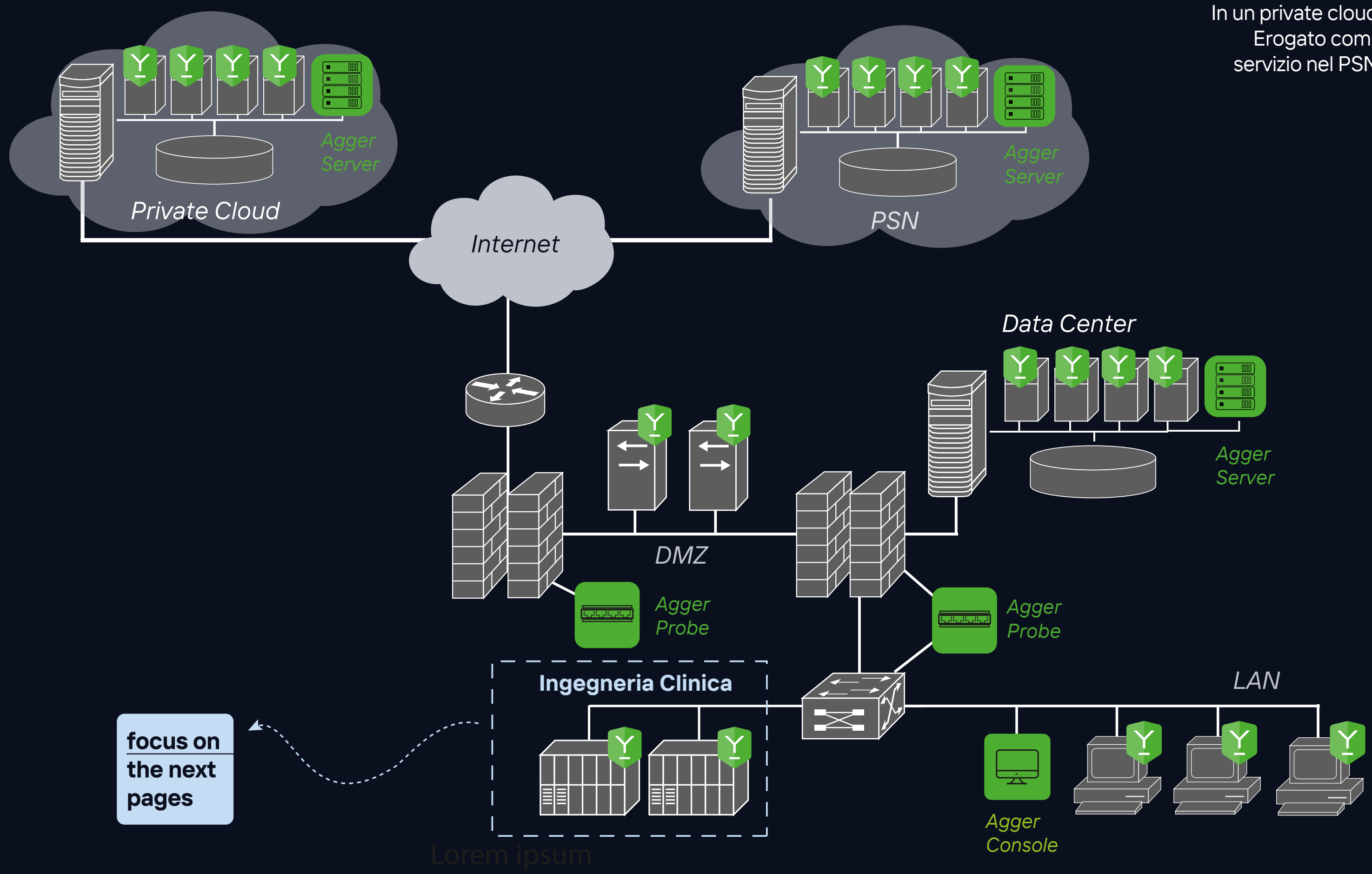
FINANCE CYBER RESILIENCE

How Agger works:

- Behavioral analysis agents are installed for monitoring running processes, probes are deployed for passive analysis of network communications, and an active monitoring system is in place for interfaces exposed by agentless devices.
- Agger maps and studies all processes and connections.
- It recognizing an attack and reacting within 0 seconds.
- It applies the most appropriate reaction based on custom rules.
- In the OT context, if required, it restores the pre-attack state.
- It saves logs and telemetry for post-incident analysis.

Agger Server può essere:

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



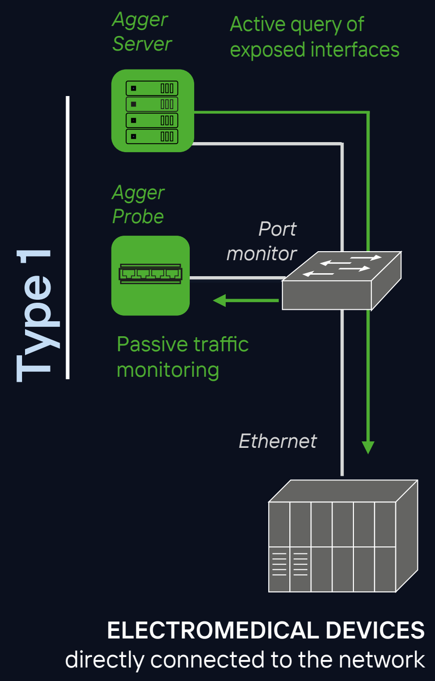
note

Possibility to create detection and reaction rules both centrally and at the level of individual agents to achieve resilience of services provided by all systems, including legacy ones.

A single platform to cover all technical, risk analysis, and reporting requirements for Identification, Protection, Detection, Response, and Recovery required by national authorities (ACN).

It allows for maximum protection without interfering with or limiting the delivery of healthcare operational services.

Possibility to assign custom tags (color and text) to each endpoint and agentless device to create logical groupings, such as physical location, the service they belong to, the provider managing them, etc., useful for risk analysis and incident management.

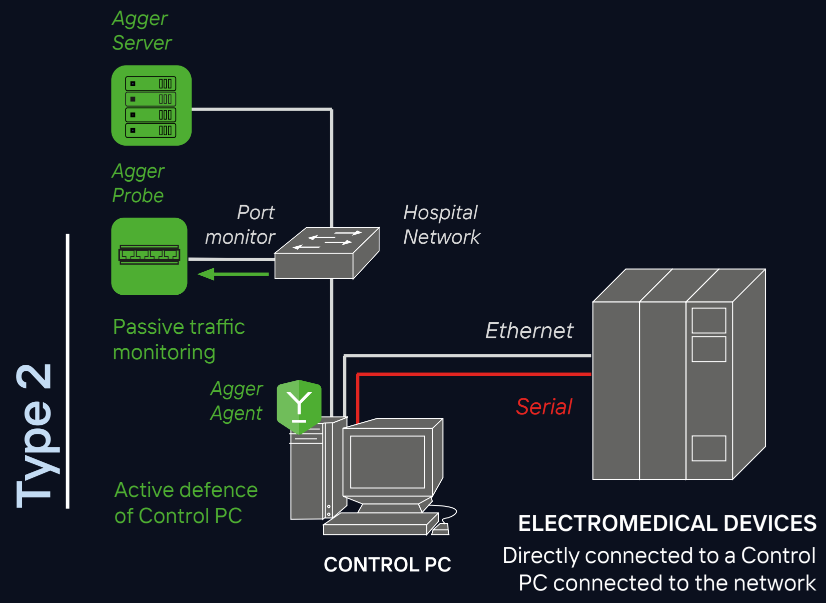

Type 1
Agger Server
Active query of exposed interfaces
Agger Probe
Port monitor
Passive traffic monitoring
Ethernet
ELECTROMEDICAL DEVICES
directly connected to the network

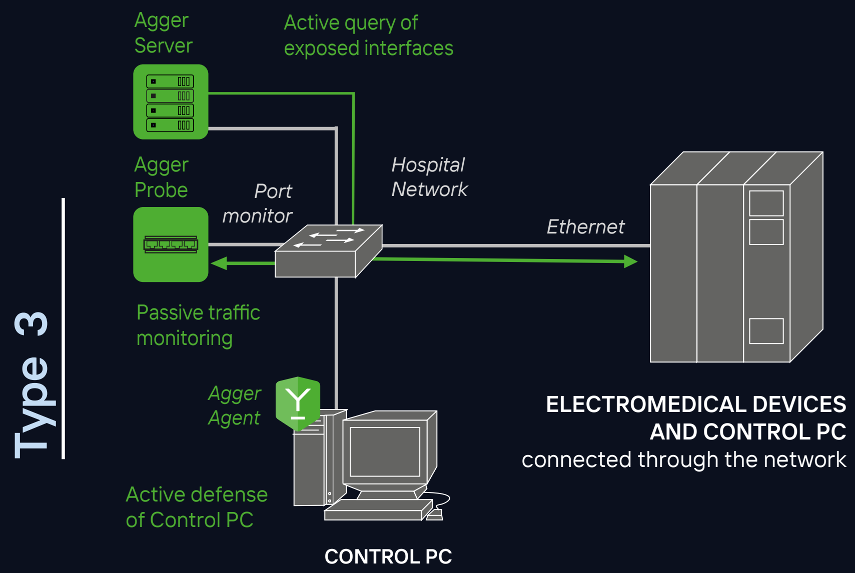
CLINICAL ENGINEERING FOCUS

The solution for healthcare enterprises:

In 2019, national healthcare enterprises were included in the National Cybersecurity Framework as instrumental structures for the exercise of essential state functions and necessary for the exercise and enjoyment of fundamental rights. The National Cybersecurity Agency (ACN) has provided critical infrastructures with t**he National Cybersecurity Framework, which is a crucial tool for implementing a Cybersecurity management system. The Framework requires the definition of concrete actions from an organizational, procedural, and technical perspective for the prevention, identification, and management of cyber incidents.** It has expanded the perimeter of defended infrastructures beyond information and telecommunication systems to include all network-connected physical devices, such as electromedical equipment.

Gyala has developed a security process for clinical engineering electromedical devices through solutions tailored to various types of equipment. This process ensures full compliance with the technical requirements of the National Cybersecurity Framework.




Type 3
Agger Server
Active query of exposed interfaces
Agger Probe
Port monitor
Hospital Network
Ethernet
Passive traffic monitoring
Agger Agent
Active defense of Control PC
CONTROL PC
ELECTROMEDICAL DEVICES AND CONTROL PC
connected through the network

Gyala,
Safe. **Always.**

Agger, Custom Made Solution

Agger, our **Cyber Security all-in-one** totally modular and customizable according to needs, thanks to sophisticated AI algorithms developed for military use for supervision and automatic reaction, can prevent, identify, and automatically manage any IT threat and anomaly 24/7 and guarantee the IT/OT resilience.

Agile approach to innovation

Gyala combines **the "agile" approach** typical of an innovative start-up with the consolidated **know-how gained** by the three Founders in the management of Cyber Protection projects for critical infrastructures, developed with various Ministry of Defence units and major national System Integrators.

We develop cutting-edge Automatic Defense solutions to protect companies' strategic IT and OT public and private assets from cyber attacks.

Gyala, your Technology Partner

Thanks to our **many years of experience in the Defense Sector,** we deal with competence and **with maximum efficiency** the growing challenges of the cybersecurity landscape.

We use an ecosystem of system integrators, advisor company and solution providers that integrate our solution within the customer's infrastructure.

ISO 9001:2015
ISO IEC 27001

COMPLIANCE NIS2
E REQUISITI
FRAMEWORK
CYBERSECURITY
NAZIONALE

CYBERSECURITY
MADE IN EUROPE

GYALA
Cyber Security

marketing@gyala.com
gyala.com in Gyala