



Invinsense OT Protection & Threat Detection

Protect the OT boundary.
Understand the activity
behind it.



What is it?

Invinsense OT Firewall and OT IDS address two parts of the cyber-physical systems (CPS) protection problem. The firewall is the network protection layer. OT IDS adds asset discovery, network and SCADA-protocol monitoring, detection and incident management so teams have more context when something needs investigation.

Why it matters

A network boundary matters, but a firewall alone does not tell the security team which OT assets are present or what activity is taking place beyond it. Pairing a protection layer with visibility and detection makes it easier to investigate a finding without asking the firewall to do the analyst's job.

What you get



A network protection layer

The supplied OT Firewall material describes automated installation, configuration and deployment, plus white-label customization/readiness. Specific traffic-policy and enforcement capabilities need confirmation in the technical specification.



OT network visibility

OT IDS builds an asset inventory and monitors network events and SCADA protocols. Dashboards and audit logs give teams a way to review activity.



Detection and incident follow-through

The alert and detection engine, notifications and incident management help teams move from an event to an investigation. Vulnerability intelligence and asset-risk visibility add useful context.

When it makes sense



A plant is reviewing how it protects an OT network boundary.



The security team needs visibility into assets and industrial network events



Alerts need asset and risk context before escalation.



The organization wants a Protect + Detect approach without treating the products as interchangeable.



An example

A plant team deploys the firewall at an agreed network boundary under its change process. OT IDS monitors selected segments and SCADA protocols. When the monitoring layer raises an alert, the team reviews the affected asset and records the incident. Automated IDS-to-firewall blocking must be designed and validated separately.

Technical details

Area	Documented capability
OT Firewall	Automated installation, configuration and deployment; white-label customization/readiness.
OT IDS visibility	Asset inventory; network event and SCADA-protocol monitoring; dashboards.
OT IDS detection	Alert engine; notifications; audit logging; incident management.
Risk context	Vulnerability intelligence and asset-risk visibility; SIEM integration support.
Portfolio fit	PROTECT + DETECT; Secure Remote Access provides a separate ACCESS layer.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation.

Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.

Gartner

Infopercept is recognized as a representative vendor in multiple Gartner® reports

- UEMP (Exposure Management)
- AMTD (Preemptive Security)
- AEV (Security Validation)

[Learn More](#) →

 **Ready to try it out?**

Sign up for a demo. Visit infopercept.com/book-a-meeting

Infopercept



Attacker's Mind. Defender's Brain.®