



Invinsense OT IDS

Discover OT assets.
Monitor cyber-physical
systems (CPS) traffic.
Investigate the signal.

What is it?

Invinsense OT IDS gives industrial security teams a working view of the assets and activity on monitored OT networks. It combines asset inventory, network and SCADA-protocol monitoring, detection, vulnerability-risk context and incident management in one OT-focused workflow.

Why it matters

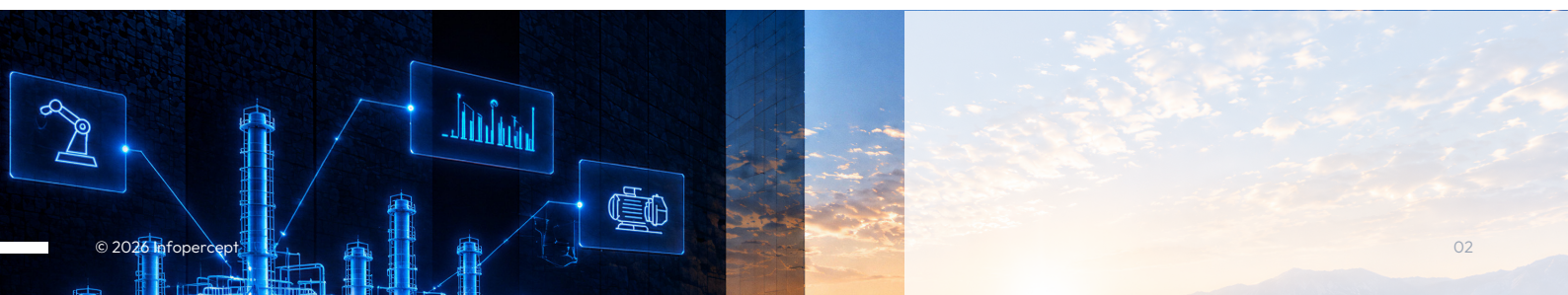
Industrial networks can be hard to inventory, and a security event is difficult to judge without knowing which asset is involved and what normal activity looks like. Invinsense OT IDS helps teams move from a network signal to an investigation with asset and risk context.

What you get

- 
See what is connected
 Asset management and inventory provide visibility into monitored OT systems. Asset-risk score visibility helps the team focus its review.
- 
Follow industrial activity
 Network event and SCADA-protocol monitoring, supported by dashboards and analytics, provide context for OT activity.
- 
Investigate what needs attention
 An alert and detection engine, notifications and incident management give analysts a path from finding to investigation. Audit logging helps preserve a record of platform activity.
- 
Bring risk into the decision
 Vulnerability intelligence and risk assessment help the team understand an asset's exposure when reviewing an alert.

When it makes sense

- 
 The team needs an inventory of monitored OT assets.
- 
 Industrial-protocol or network activity is difficult to review.
- 
 OT alerts need vulnerability and asset-risk context.
- 
 Plant security and the SOC need a clearer investigation workflow.



An example

A new asset appears in a monitored segment. OT IDS adds it to the asset view and monitors network and protocol activity. An unusual event triggers an alert; the analyst reviews the event, checks the asset and risk context, and manages the investigation as an incident.

Technical details

Area	Documented capability
Visibility	OT asset management and inventory.
Monitoring	Network events and SCADA protocols; security dashboard and analytics.
Detection	Alert and detection engine; real-time notifications.
Risk	Vulnerability intelligence, risk assessment and asset-risk visibility.
Operations	Incident management and audit logging.

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.®