



Invinsense OT Secure Access & Detection

Control who enters
cyber-physical systems (CPS).
See what happens inside.



What is it?

Invinsense brings OT Secure Remote Access and OT IDS together for teams that need to manage human access into cyber-physical systems (CPS) and monitor activity in the surrounding OT environment. The access gateway controls the connection; OT IDS adds asset, network and SCADA-protocol visibility. The two controls play complementary roles, rather than doing the same job.

Why it matters

A support engineer or third-party vendor may need urgent access to a plant system. Giving them connectivity is only half the job. The plant team also needs clear access rules, a record of the session and a way to investigate activity in the environment.

What you get



A controlled entry point

Browser-based HTML5 access works without an endpoint VPN client. The zero-trust proxy provides a centralized entry point, with RBAC, enterprise SSO and MFA, credential injection, session recording and forensic auditing. The gateway proxies the connection and separates IT and OT at the TCP/IP level.



Visibility inside the environment

OT IDS maintains an asset inventory and monitors network events and SCADA protocols. Dashboards, a detection engine, notifications and incident management help the security team investigate what it sees.



Risk context for investigation

Vulnerability intelligence and risk assessment help teams decide which assets & findings need attention first.

When it makes sense



Contractors and vendors require access to selected OT systems.



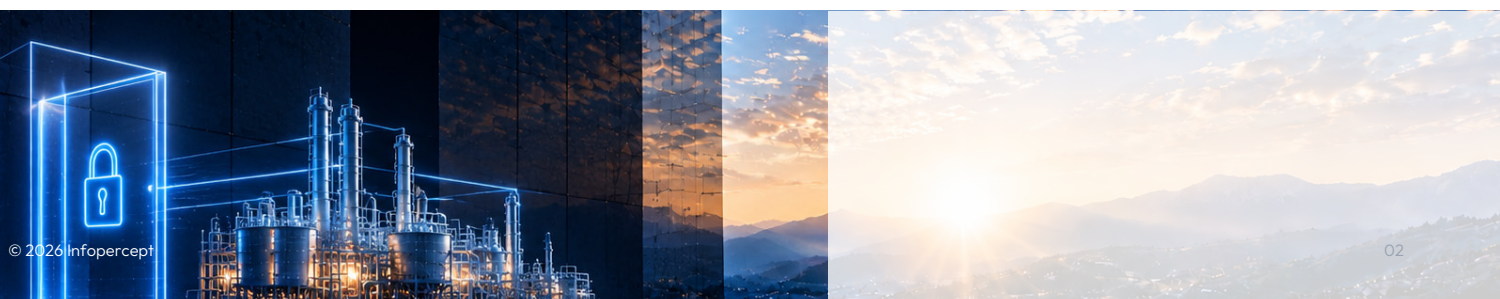
The organization needs recorded remote sessions for review or investigation.



Plant and security teams lack a common view of assets and monitored network activity.



The team wants to combine access governance with an OT detection workflow.



An example

A maintenance provider connects to an approved system through the access gateway. Identity controls apply to the session and the connection is recorded. OT IDS monitors the relevant industrial traffic; if an alert appears, the team can review the OT activity and the access record. Linking these records automatically is an integration requirement to validate, not an assumed feature.

Technical details

Area	Documented capability
Remote access	Clientless HTML5; zero-trust proxy; RBAC; enterprise SSO/MFA; credential injection.
Session evidence	Session recording and forensic audit.
OT visibility	Asset inventory; network event and SCADA-protocol monitoring.
Detection	Alerts, dashboards, notifications and incident management.
Portfolio fit	ACCESS + DETECT; OT Firewall provides a separate PROTECT 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.®