DER SECURITY

dersec.io | info@dersec.io

DERSec Sentry

Cyber-Physical Security for Distributed Energy

Problem Statement

As power grids worldwide shift to renewable and distributed energy, distributed assets have become prime targets for sophisticated threat actors. Weekly reports indicate **escalating reconnaissance, probing, and attacks** on solar inverters, battery energy systems, EV chargers, microgrid controllers, and large loads. Traditional network monitoring cannot detect living-off-the-land attacks that manipulate DER equipment, control signals, or measurement data.

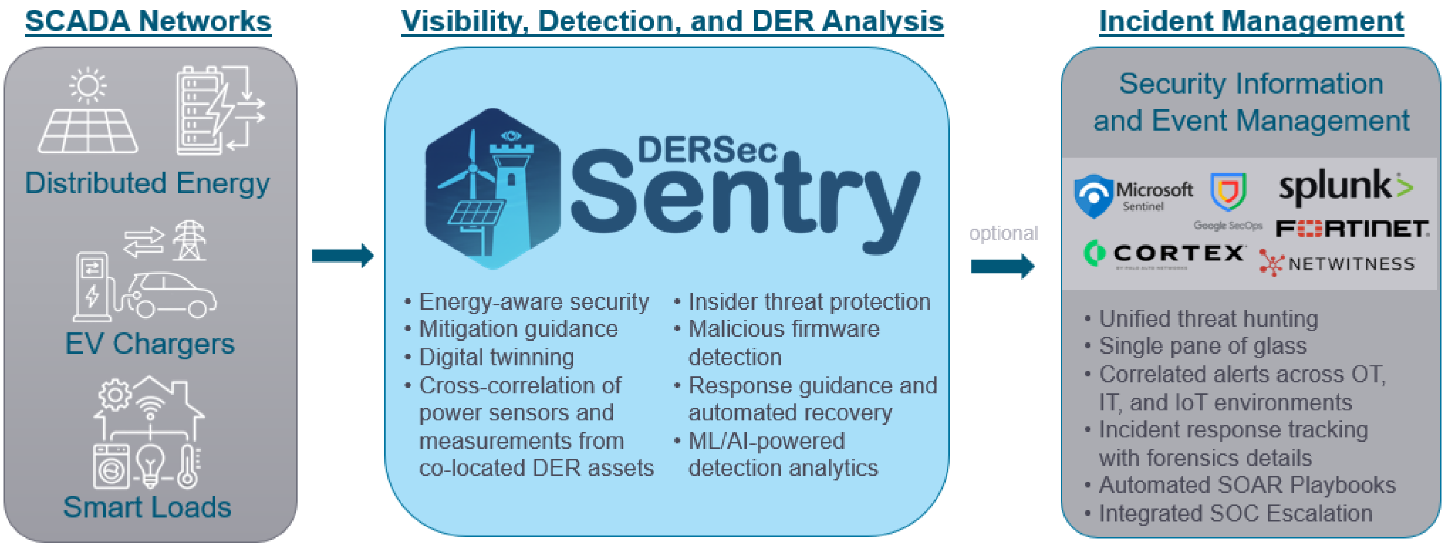
The Solution: DERSec Sentry

DERSec Sentry delivers the world’s first energy-aware cybersecurity layer purpose-built for Distributed Energy Resources (DER). Combining **patented, physics-informed analytics** with deep packet inspection across native DER protocols, the DERSec Sentry detects dangerous commands, falsified telemetry, firmware changes, and insider threats in real time.

Core Capabilities

- **Deep Packet Inspection** — Parses SunSpec Modbus, OPC-UA, DNP3, IEEE 2030.5, OCPP, and other traffic to extract and validate measurement and control signals
- **Digital Twin Analytics** — Physics-based power simulation run in parallel with physical systems to detect maloperations and false data injection attacks
- **ML/AI Cyber Detection** — Inference engine trained on 1B+ DER data points using NVIDIA Morpheus
- **Response Playbooks** — Autonomous threat response to block endpoints, revoke credentials, and reset to known-good states
- **Stateful Detection** — Tracks operational state over time to detect slow-burn adversarial campaigns
- **Forensics Context** — Power-aware intelligence distinguishes physical faults from cyberattacks, accelerating recovery

Integrated Architecture



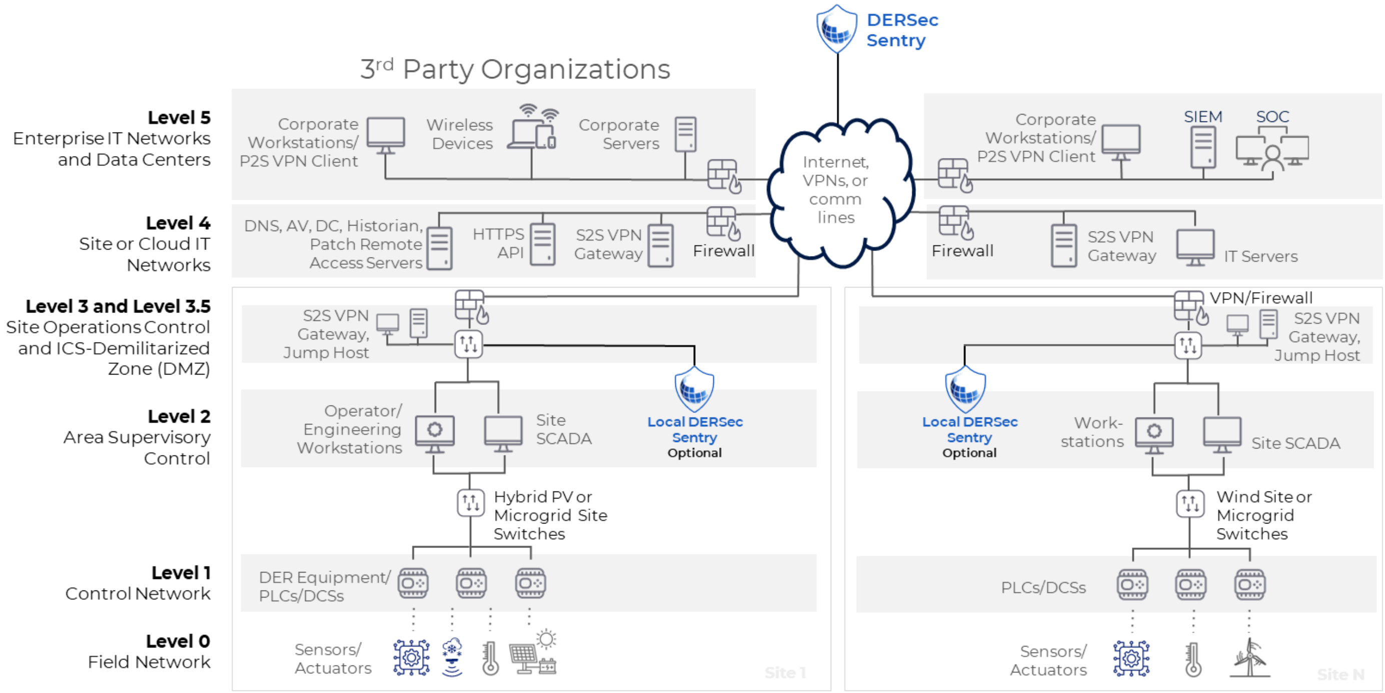
- Energy-aware security
- Mitigation guidance
- Digital twinning
- Cross-correlation of power sensors and measurements from co-located DER assets
- Insider threat protection
- Malicious firmware detection
- Response guidance and automated recovery
- ML/AI-powered detection analytics

- Unified threat hunting
- Single pane of glass
- Correlated alerts across OT, IT, and IoT environments
- Incident response tracking with forensics details
- Automated SOAR Playbooks
- Integrated SOC Escalation

DERSec Sentry integrates with SCADA Platforms, IT/OT/IoT IDSs, and SIEM Tools for unified DER visibility and response.

Deployment Across DER Infrastructure

DERSec Sentry deploys flexibly across all Purdue model levels—from field networks through enterprise IT. Whether in the cloud, on-premises with rackmount hardware, or containerized on DER gateways, the Sentry provides fail-safe monitoring via mirror/SPAN ports while alerting operators to threats targeting field assets or head-end systems.


DERSec Sentry
3rd Party Organizations
Level 5
Enterprise IT Networks and Data Centers
Level 4
Site or Cloud IT Networks
Level 3 and Level 3.5
Site Operations Control and ICS-Demilitarized Zone (DMZ)
Level 2
Area Supervisory Control
Level 1
Control Network
Level 0
Field Network
Corporate Workstations/ P2S VPN Client
Wireless Devices
Corporate Servers
Internet, VPNs, or comm lines
Corporate Workstations/ P2S VPN Client
SIEM
SOC
DNS, AV, DC, Historian, Patch Remote Access Servers
HTTPS API
S2S VPN Gateway
Firewall
Firewall
S2S VPN Gateway
IT Servers
S2S VPN Gateway, Jump Host
VPN/Firewall
S2S VPN Gateway, Jump Host
Operator/ Engineering Workstations
Site SCADA
Local DERSec Sentry
Optional
Local DERSec Sentry
Optional
Work-stations
Site SCADA
Hybrid PV or Microgrid Site Switches
Wind Site or Microgrid Switches
DER Equipment/ PLCs/DCSs
PLCs/DCSs
Sensors/ Actuators
Sensors/ Actuators
Site 1
Site N

Why DERSec Sentry

Energy-Aware Security

Purpose-built for DER protocols and power systems—not a generic IT tool retrofitted for OT.

Insider Threat Protection

Detects unauthorized local interface modifications, backdoor access, and malicious firmware changes.

Grid-to-SOC Integration

Unified threat hunting across OT, IT, DER, and IoT environments with SIEM/SOAR integration.

Rapid Deployment

Cloud, on-premises, or containerized. Integrates with traditional SCADA and IDS platforms seamlessly.

Target Environments

Utility-Scale DER
Solar farms, BESS, and wind installations

AI Data Centers
Backup Generation and on-site renewable power

Microgrids
Campus, military, and community microgrids

eMobility Fleets
EV charging infrastructure and fleet management

Proven Technology

Built on patented, R&D100 Award-winning research from Sandia National Laboratories, DERSec Sentry integrates with SCADA Systems (e.g., Inductive Automation Ignition), OT IDS tools (e.g., Nozomi Networks Guardian), and SIEM/SOAR tools (e.g., Splunk SOAR) to provide comprehensive, single-pane-of-glass IT/OT/IoT/DER visibility, detection, and response capabilities.

Ready to secure your energy infrastructure? Contact us at info@dersec.io | dersec.io