NOZOMI NETWORKS | DER SECURITY

SOLUTION BRIEF

Physics-Informed Cyber-Physical Security for Distributed Energy Resources

Physics-Informed Analytics to Detect Sophisticated Living-off-the-Land Threats to Energy Systems

As tremendous shifts toward renewable and distributed energy for utility power, AI data center backup generation, and microgrid energy make them prime targets for sophisticated threat actors, Security Operations Center (SOC) teams need more than traditional network monitoring to detect threats to Distributed Energy Resources (DER) and associated critical infrastructure.

The integration of the Nozomi Networks platforms with DER Security (DERSec) Sentry provides a first-of-its-kind, energy-aware security layer. By combining Nozomi Networks' security visibility with DERSec's patented cyber-physical analytics, organizations can now detect stealthy, living-off-the-land attacks that manipulate control signals without triggering traditional cyber alerts.

The combined, behavior-based solution overcomes the common blind spots found in modern OT cybersecurity solutions deployed in energy environments. Traditional security tools often misclassify DER assets and cannot understand the physical meaning of the process variables, but the Nozomi Networks & DERSec architecture ensures full visibility of all exchanges with DER equipment. The customizable DERSec ruleset and analytical engine rapidly identifies direct attacks on the energy infrastructure and any local interface modifications, updates via backdoor access, malicious firmware changes, or insider threat actions that modify the normal electrical behavior of these devices.

Benefits

Cyber-Physical Threat Detection: Unparalleled real-time detection of attacks targeting energy infrastructure by validating physical process variables in the network traffic.

Deep DER Visibility: Expanded visibility into the native communication protocols of Distributed Energy Resources (DER) including solar inverters, EV chargers, wind systems, and battery storage.

Physical-Informed Resilience: Rapid identification of insider threats and malicious control signals using power-aware analytics, digital twin validation, and ML/AI classifiers.

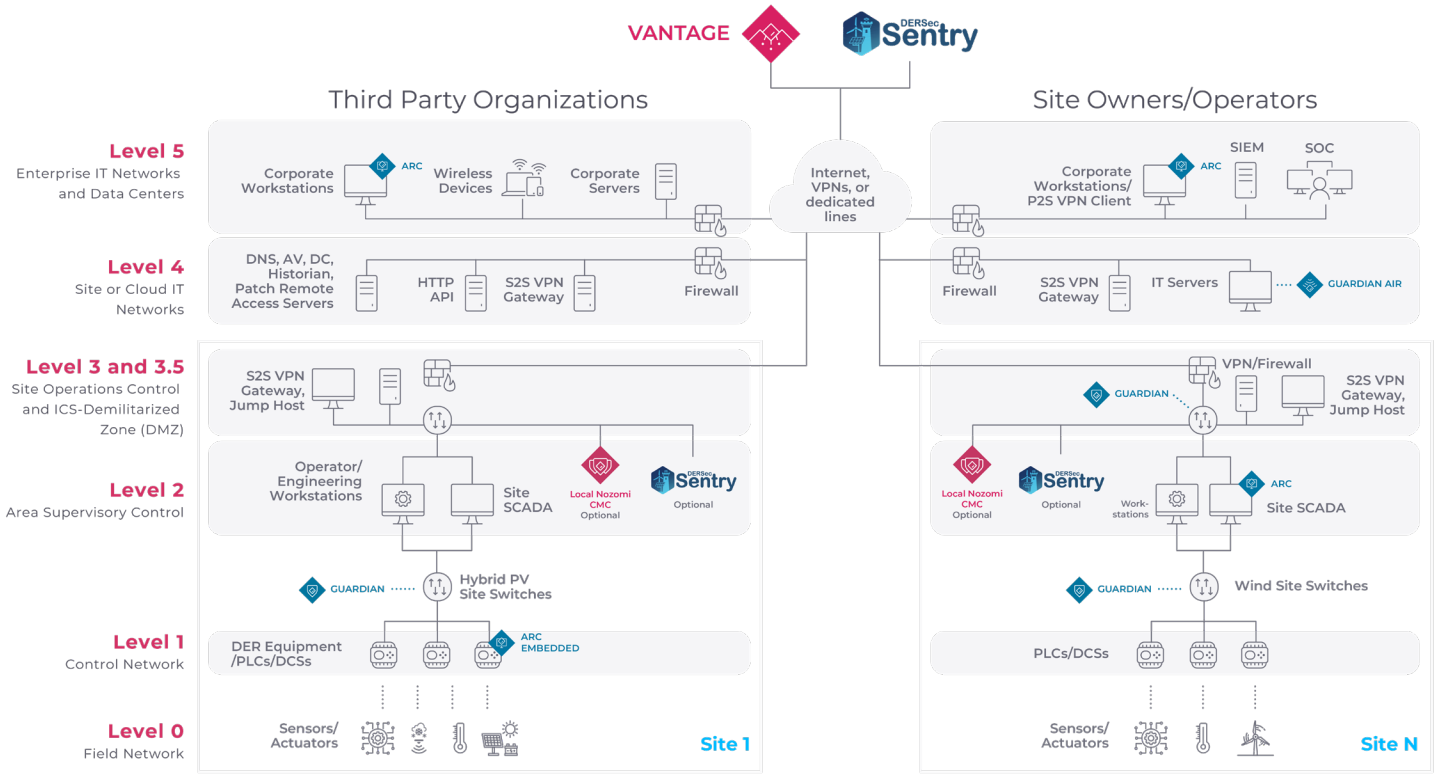
Better Together: Cyber-Physical Resilience

DERSec Sentry extends the capabilities provided by the Nozomi Networks platform with physics-based intelligence so defenders can see, secure, and monitor the entire energy, OT, DER, IoT, and IT landscape in real-time. This enables cyber-physical resilience with these core capabilities:

- **Analytical process variable integrity checks:** Detect maloperations using stateful analysis and digital twinning. This capability drastically expands the total indicators of compromise in energy systems.
- **High-fidelity detection of malicious control signals:** When malicious control signals are detected, the system generates alerts that indicate immediate defensive actions, recovery strategies, and, if desired, trigger defensive playbooks to isolate bad actors and/or reset equipment to known-good operating conditions.
- **Deep forensics context and power systems awareness:** Power-aware intelligence provides forensics tools for root cause analysis that help operational teams distinguish between physical faults and cyberattacks, accelerating response and recovery times.

Joint Solution Deployment

Adding cyber-physical intrusion detection capabilities to new or existing Nozomi Networks deployments is straightforward. The DERSec Sentry, deployed either locally or in the cloud, is configured with API keys to fetch process variables from either Nozomi Networks Central Management Console (CMC) or Guardian regularly. If malicious commands are issued or control variables are falsified, the DERSec Sentry alerts the SOC team and provides detailed information on the physical threat along with guidance to mitigate the threat.



Joint Solution Benefits

100% visibility across IT/OT Environments

- Clear view of all IT, DER, IoT and OT traffic.
- Physics-informed monitoring for inverters, battery energy storage systems, gensets, wind turbines, and EV charging infrastructure.

Reduced Organization Risk

- Eliminate DER attack surface blind spot using power-aware security metrics and diagnostics.
- Detect stealthy cyberattackts that manipulate measurement and control signals.

Security Operations Efficiency

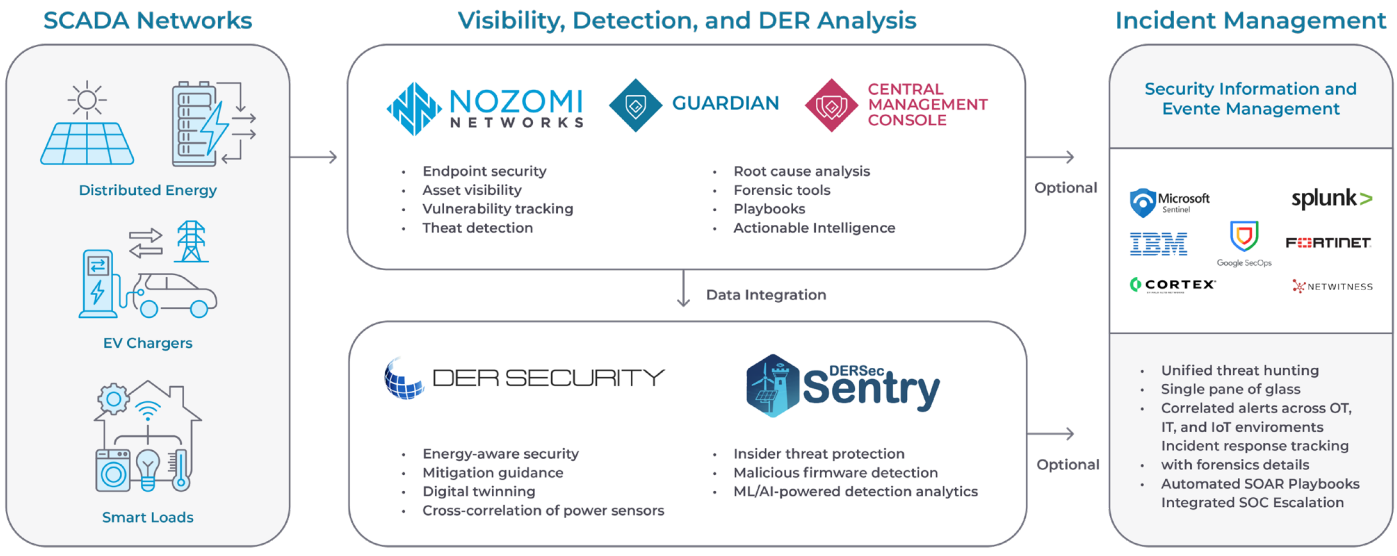
- Consolidate monitoring into a single pane of glass.
- Reduce the burden on security teams with AI-powered insights and response guidance.

Improve Energy System Performance

- Advanced diagnostics and real-time visibility into key power and security metrics.
- Deep insights into system behaviour to optimize performance.

Grid-to-SOC Integrated Solution

The joint solution provides a unified OT, IT, DER, and IoT threat hunting environment to thwart sophisticated adversaries and APTs across the entire field-to-cloud architecture. OT/DER security operations are verified with granular field-level physics analyses and attacks are mitigated with enterprise-level SOC workflows.



DER SECURITY

DER Security (DERSec) focuses on protecting renewable and distributed energy systems from advanced threat actors with energy-aware cyber-physical analytics. DERSec's cybersecurity technologies give asset owners and operators new visibility into the OT network, detect stealthy cyberattacks that manipulate measurement and control signals, and mitigate impacts to critical energy infrastructure.

Learn more at http://dersec.io

NOZOMI NETWORKS

About Nozomi Networks

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

---

nozominetworks.com