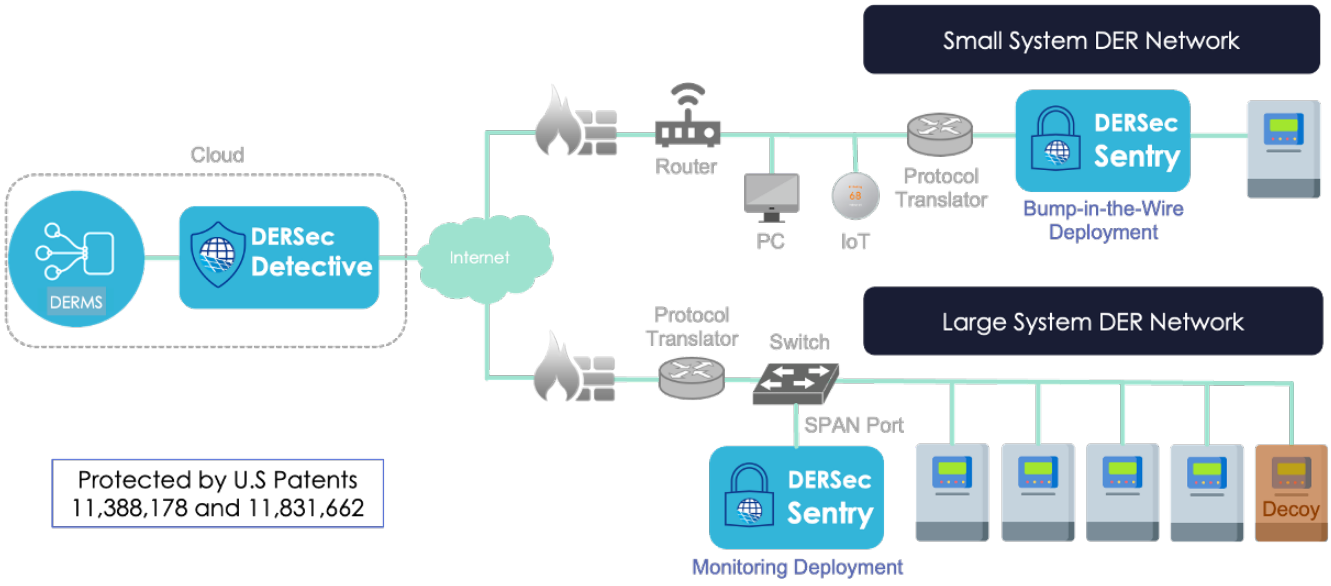
Energy-Informed Detection and Prevention Technology for Distributed Energy Systems

Background DER Security Corp (DERSec) was founded in 2022 as a spin-off of the SunSpec Alliance, a communication standards developer for the distributed energy industry. With leadership from the SunSpec Alliance, Sandia National Laboratories, and the cybersecurity industry, the DERSec team is delivering the world's first Energy-Informed Cybersecurity Protection, Detection, and Response software solution for interoperable Distributed Energy Resource (DER) systems and devices.

Threats An ever-expanding collection of public reports of attacks on DER systems describe how adversaries exploit vulnerabilities in products, networks, and cloud infrastructure; deface EV chargers; compromise local DER products and cloud infrastructure; prevent visibility and control of 100s of megawatts of DER assets; and maliciously update firmware on DER systems to prevent operation. Near-daily disclosures indicate that threat actors are escalating their attacks on DER systems as they become more important to the grid.

Solution DERSec has developed a two-part cybersecurity offering, **DERSec Sentry** and **DERSec Detective**, to address threats to DER systems and the power grid. DERSec Sentry, installed in DER systems for monitoring, threat detection, and threat protection, are configured as a bump-in-the-wire (BITW) or attached to a network router Switched Port Analyzer (SPAN) port. DERSec Detective is deployed in network operating centers of aggregators, DER vendors, and utility companies in front of the DER Management System (DERMS) to monitor network traffic, isolate and mitigate suspicious packets, and maintain network traffic flow.

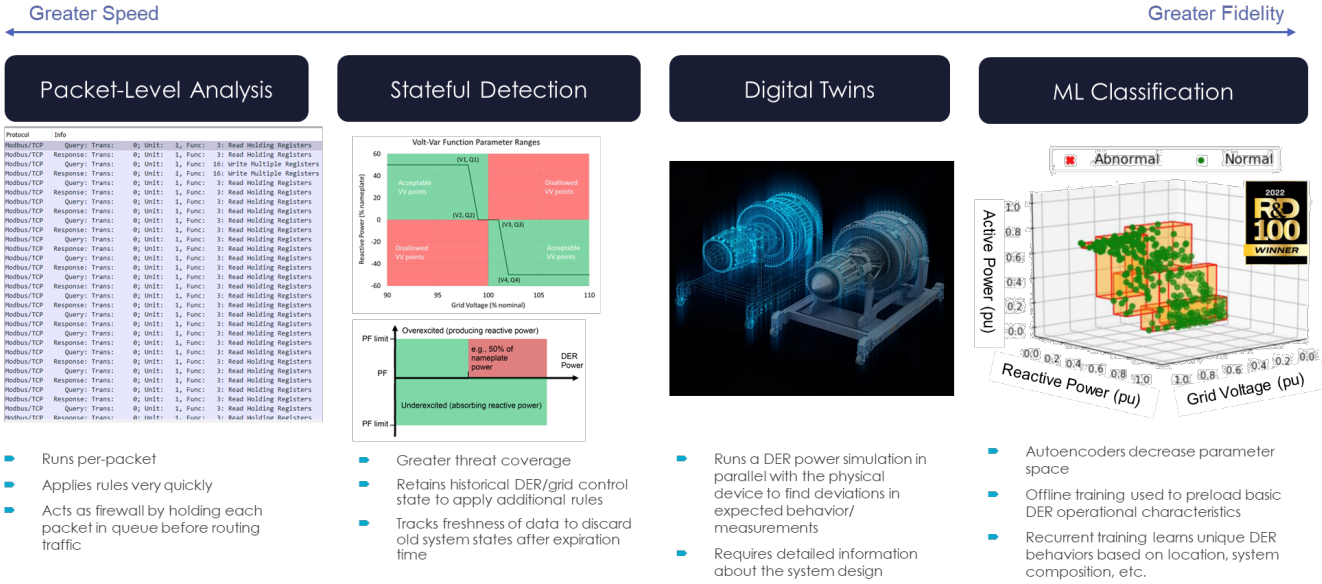
DERSec Sentry and DERSec Detective work together to detect malicious firmware updates, nefarious control operations, and false data injection attacks on the network; learn adversarial tactics; increase grid resilience; and maximize asset uptime. Both products implement DERSec Deep Packet Inspection technology to parse network traffic to extract monitoring and control signals and validate those signals against a set of power system rules. When falsified power data or malicious control signals are detected, DERSec Sentry and Detective suppress incoming network traffic and notify network operators of the activity.



DERSec Detective additionally decrypts and parses traffic using a Next-Generation Firewall and tests payloads for malware by validating them against anti-virus tools, AI classifiers, and cross-correlation with the DER fleet. DERSec Security Orchestration, Automation, and Response (SOAR) playbooks are then triggered to mitigate threats by autonomously blocking malicious endpoints, revoking credentials & permissions for bad actors, or resetting

endpoint systems to a known-good state. DERSec Detective incorporates DER Decoys on field networks to detect adversary reconnaissance operations and ascertain attacker tactics and techniques.

Detection DERSec Deep Packet Inspection detection rulesets, shown below, can be applied to filter and drop packets before reaching the intended target, but with varying speeds of detection and accuracy. Customer-tunable heuristic rules that describe known-bad network operations can be applied at the packet level extremely quickly but cannot discern the operational state of the DER equipment. Stateful detection solves that problem by retaining operational information and detecting bad operations over longer timeframes. Digital twins go a step further and capture the complex interactions of multiple grid-support functions with the grid- and DC-power source states. Power simulation, updated with out-of-band and DER-control data, is run in parallel with the physical system to detect maloperations of the DER by tracking significant measurement deviations with the physical equipment. Finally, machine learning is used to classify DER measurements and control data using an offline learning methodology to capture attacks that are not detected using the previous techniques.



- Runs per-packet
- Applies rules very quickly
- Acts as firewall by holding each packet in queue before routing traffic

- Greater threat coverage
- Retains historical DER/grid control state to apply additional rules
- Tracks freshness of data to discard old system states after expiration time

- Runs a DER power simulation in parallel with the physical device to find deviations in expected behavior/ measurements
- Requires detailed information about the system design

- Autoencoders decrease parameter space
- Offline training used to preload basic DER operational characteristics
- Recurrent training learns unique DER behaviors based on location, system composition, etc.

Implementation DERSec Detective technology is deployed, in cloud environments or as an on-premises solution using rackmount or other industrial-grade computer hardware, as discrete IDS- and SOAR virtual machines that capture, parse, and analyze network traffic for malicious content to respond to threats. DERSec Sentry is deployed on field-hardened hardware or is containerized to run on Linux-based DER gateways or power electronics products. When network connectivity is paramount, connecting the DERSec Sentry to a mirror or SPAN port at the site provides fail-safe operations while alerting operators to threats that target field assets. Field alerts are routed to the DERSec Security Information and Event Management (SIEM) system at the network- or security operations center via syslog or database formats, emailed to security personnel, or otherwise transferred to security teams as appropriate. DERSec's groundbreaking technology sets a new, high bar for protecting and defending critical energy infrastructure.

References DERSec technology is built on patented, R&D100 Award-winning research conducted at Sandia National Laboratories to detect and mitigate cybersecurity threats to DER systems. Technical details are here:

- J. Johnson, et al., "SOAR4DER: Security Orchestration, Automation, and Response for Distributed Energy Resources" in Power Systems Cybersecurity. Power Systems. Springer, Cham. 2023.
- A. Chavez, et al., "Hybrid Intrusion Detection System Design for Distributed Energy Resource Systems," IEEE CyberPELS Workshop 2019, Knoxville, TN, April 29–May 1, 2019.
- S. Hossain-McKenzie, et al., "Proactive Intrusion Detection and Mitigation System: Case Study on Packet Replay Attacks in Distributed Energy Resource Systems", IEEE Power and Energy Conference at Illinois (PECI), pp.1-6, 2021.
- C. Birk Jones, et al., "Unsupervised Online Anomaly Detection to Identify Cyber-Attacks on Internet Connected Photovoltaic System Inverters", 2021 IEEE Power and Energy Conference at Illinois (PECI), pp.1-7, 2021.