

AI-NATIVE ENERGY RUNTIME SECURITY AND SECURE REMOTE ACCESS FOR ENERGY OT

SECURING THE FUTURE OF ENERGY

Growing Security Risks for Energy OT/IoT Environments

Distributed energy sites - BESS, solar PV, substations, smart meters, wind turbines, and more - are geographically dispersed, cloud-managed, and run on energy-specific protocols like Modbus TCP, IEC 61850, DNP3, and MQTT that traditional security tools don't understand. They're also opened up daily to remote access from technicians and vendors - often over static VPNs and shared credentials that leave standing, unaudited pathways into critical infrastructure.

- A successful attack can mean manipulated power output, falsified meter readings, disrupted grid services, unauthorized remote access, or cascading failures - with safety, revenue, and regulatory fallout.
- Your SOC sees network anomalies without energy context; your power operations team sees operational issues without security visibility; and remote sessions leave little record of what was actually done.

SaiFlow is purpose-built for energy and utility operators, and energy-intensive environments like data centers, stadiums, and industrial facilities - where energy infrastructure is business-critical and a high-value attack surface.

The SaiFlow Energy Runtime Cybersecurity Platform & Secure Remote Access

SaiFlow bridges network security and power operations - combining an on-site software agent with cloud analytics, and brokered secure remote access, to deliver:

- **Contextual Threat Detection** - real-time identification of malicious and anomalous energy operations by correlating network and power data.
- **Full Energy IoT Visibility** - asset discovery and vulnerability management that continuously reduces the attack surface.
- **AI-Powered Investigations** - faster forensics and incident response, cutting Mean Time to Investigate and Respond (MTTI/MTTR).
- **Regulatory Compliance Scoring** - real-time scoring across NERC-CIP, NIS2, EU CRA, and more, so operators stay audit-ready.
- **Secure Remote Access** - zero-standing-privilege, just-in-time sessions for technicians and vendors, brokered end-to-end with Palo Alto Networks Idira and Prisma Access, fully recorded and cross-checked against live energy telemetry.

WHY SAIFLOW

Secure Remote Access (with PANW)

- **Zero Standing Risk** - Just-in-time, task-scoped sessions replace persistent credentials and shared logins - nothing left behind for attackers to find.
- **One Console, Every Site** - Request, scope, and audit every remote session across a multi-vendor, global fleet - no more sprawling VPNs.
- **Context the Grid-Edge Understands** - Every session is encrypted, fully recorded, and cross-checked against live site and device telemetry - closing the gap between login and action.

Energy Runtime Security

- **See the Attack Before It's an Incident** - Correlates network and power data in real time to catch malicious and anomalous energy operations as they happen.
- **Full Visibility, Zero Blind Spots** - Continuous IoT asset discovery, vulnerability management, and zero-trust policy enforcement across every energy protocol - Modbus TCP, IEC 61850, DNP3, MQTT.
- **Audit-Ready, Always** - Real-time compliance scoring across NERC-CIP, NIS2, EU CRA, IEC 62443, and more, with the forensics to cut MTTI/MTTR when it counts.

BETTER TOGETHER - OUR PARTNERS

