Solution Brief

Edge-Native Security Solution for Utilities

intel®

AI-Driven Substation Protection, Built on the Intel® Tiber™ Edge Platform

Threat Sense at the Edge is a cloud-to-edge platform from SAP and Intel that brings new levels of security and operational insights to utility substations.

Key benefits for utilities

Accelerate time to insights
Speed data processing locally with services and tools that extend from cloud to edge.

Create new business value and streamline migration
Integrate easily on standard hardware, and run applications from whichever location delivers the most business value, with edge and hybrid implementations possible using best-in-class software from SAP partners, built on the Intel® Tiber™ Edge Platform.

Deliver flexible execution with security and compliance
Gain extensibility and manageability without compromising security or compliance.

Take advantage of AI optimizations
OpenVINO™ toolkit accelerates AI inference to maximize the application and AI accuracy, speed, and energy efficiency.

Streamline life-cycle management
Easily update application deployment based on policies, which can be adapted depending on geography and new rules (e.g., a new threat type or employee safety guideline).

The US electrical grid depends on uninterrupted operation of more than 79,000 substations.[1] The substations are typically located in remote areas hours away from maintenance crews, with access restricted to authorized personnel. On top of ongoing operational concerns, the facilities are subject to a growing variety of security threats, including physical attacks and cyberattacks that can result in lasting outages and damage to critical infrastructure.

Threat Sense at the Edge, an as-a-service solution from SAP and Intel, uses artificial intelligence (AI) to give energy and utility companies new levels of substation security and operational insights. Leveraging SAP's Digital Core and the edge-native software infrastructure of the Intel® Tiber™ Edge Platform, the cloud-to-edge platform rapidly sorts through masses of data to identify threats, provide context, and suggest the appropriate level of response—while also helping businesses meet their financial objectives and comply with evolving customer policies.

Accelerated AI processing on a proven platform

The Intel Tiber Edge Platform enables and speeds data processing at the edge, bringing applications like Threat Sense closer to the endpoints where data is generated. Proximity to the edge accelerates time to insights while reducing refactoring costs, and it gives utilities the flexibility and cost control they need, without compromising security or compliance. The cloud-to-edge architecture runs on standard hardware and handles tasks including networking and telemetry, with a focus on enabling the application of AI.

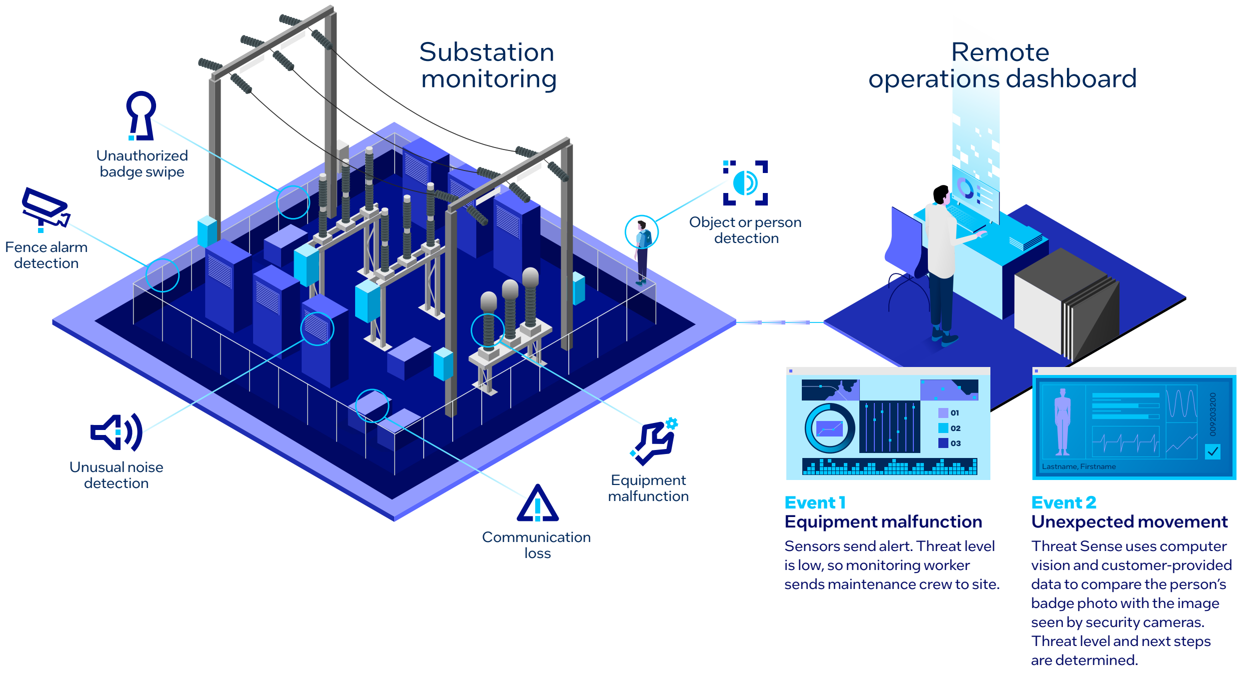
Using a layer of familiar SAP tools, utilities can integrate the Intel Tiber Edge Platform with S/4 HANA, SAP's advanced enterprise resource planning (ERP) suite that leverages in-memory computing to deliver real-time data processing and analytics. Some S/4 HANA capabilities can be deployed directly to the node for performance, while others can be hosted in the cloud for aggregation and logic services. Utilities can also customize the platform by adding solution services that are orchestrated to the node based on specific needs.

Enhance substation security with Threat Sense

Substation operations teams are awash in data. The challenge is to make sense of the constant flow of incoming information—moving quickly from recognizing that one or more events are happening at a substation to understanding the complexity of the events, the level and type of threat they pose, and the appropriate response.

Threat Sense delivers the rapid, AI-driven analysis teams need to separate relentless chatter from more-consequential events. This collaborative solution from SAP, Intel, and Alert Enterprise brings together IoT data, utility data, and signals from cameras and other physical environments. The combined information gives the system the context necessary to recognize complex issues as they happen and recommend the appropriate level and type of response.

How it works



Event 1
Equipment malfunction
Sensors send alert. Threat level is low, so monitoring worker sends maintenance crew to site.

Event 2
Unexpected movement
Threat Sense uses computer vision and customer-provided data to compare the person's badge photo with the image seen by security cameras. Threat level and next steps are determined.

With the reliability and extensibility of SAP's Digital Core and the Intel Tiber Edge Platform, Threat Sense is ready to deploy today using familiar SAP tools and standard hardware. This common usage example highlights how Threat Sense builds on existing layered security solutions:

On a dashboard at a remote operations center, a worker receives a notification about a live event at a restricted access area. In this case, a substation transformer has malfunctioned. Using Threat Sense, the worker drills down for insight into the event.

Threat Sense provides a color-coded indication of the threat level, based on parameters customized by the utility for each substation. The threat level in this instance is initially low because there are no adjoining events. The worker's suggested action is to send a maintenance crew.

If a second event—in this case, unexpected site movement—is detected at the same substation as the equipment malfunction, the threat level and response depend on the identity of the person who has swiped their badge to enter the facility. Threat Sense uses computer vision and customer-provided data to compare the person's badge photo with the image seen by security cameras, returning confidence of the match. Using rules defined by the utility, Threat Sense determines whether the person is authorized to be in the facility or if the threat level should be increased, providing workers with next-step instructions based on customer policy.

Advantages of Threat Sense at the Edge

Faster insights

AI-enabled edge technology automatically sifts through masses of data to deliver insights into events as they happen.

Intelligent analysis

Computer vision converts visual data into structured information that the system combines with utility and IoT data to rapidly identify a wide range of threats.

Customizable parameters

Automate categorization of threat types and levels by substation to ensure teams deliver the appropriate response.

Protect substations in near-real time

Threat Sense gives energy and utility companies the AI-enabled technology needed for enhanced substation security and operations in and from any location. The cloud-to-edge application is cost efficient and extensible, and it can be customized to meet business needs and requirements, even as new policies and regulations emerge.

Learn more

Speak to your Intel representative to schedule a free assessment workshop to review your substation security and operations challenges and to develop a road map for deploying Threat Sense.

intel. tiber.
Edge Platform

SAP

[1] "Sector Spotlight: Electricity Substation Physical Security, Cybersecurity & Infrastructure Security Agency," accessed February 15, 2024, cisa.gov/sites/default/files/2023-02/Sector%20Spotlight%20Electricity%20Substation%20Physical%20Security_508.pdf.

Notices and disclaimers

Intel is committed to respecting human rights and avoiding complicity in human rights abuses. See Intel Global Human Rights Principles and Approach. Intel® products and software are intended only to be used in applications that do not cause or contribute to a violation of an internationally recognized human right.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Intel® technologies may require enabled hardware, software, or service activation. No product or component can be absolutely secure. Your costs and results may vary.

0524/VM/CMD/PDF