ENERGY THEFT DETECTION PLAYBOOK

Identifying and Eliminating Non-Technical Losses Through AMI Data Analytics

bidgely

Globally, non-technical losses (NTL) are a growing financial concern for electricity utilities. It is estimated that $80 to $100 billion is lost globally to energy theft each year.

Beyond the economic impact, theft threatens grid reliability by manipulating local area supply, thereby causing transformer overloading that can result in blackouts, damage to utility assets, poor customer experience and safety vulnerabilities.

Historically, theft countermeasures have relied largely upon labor-intensive premises inspections and account auditing — even for tamper alerts originating from meter hardware. For example, an energy provider might measure the amount of power traveling through low voltage transformers at the neighborhood level and subtract the combined energy usage for all customers served by that transformer to identify a subset of customers — perhaps 200 homes — within which theft might be occurring. However, there has been no consistently accurate means to pinpoint exactly which of those 200 customers are bad actors. Enforcement could potentially cost more than the theft losses.

Today, applying AI-powered analytics to smart meter data allows a much more effective bottom-up approach. Rather than pursue theft only at the transformer level (or the occasional tamper alert), analysis is focused home-by-home at the appliance level. Anomalies in appliance-level consumption patterns accurately reveal customer-specific partial or complete meter bypassing, meter tampering, tariff misuse and more.

AI-enabled data science can, like a detective, provide a clear, data-driven picture of exactly what is happening in a given household to empower utilities with better intelligence on which to act.

The goal of this playbook is to help utilities leverage AMI data to more successfully mitigate theft-related and other NTL losses.

- **Step 1:** Ingest and Analyze Data
- **Step 2:** Accurately Detect Instances of NTL
- **Step 3:** Strategically Target Bad Actors

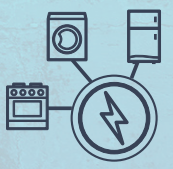
STEP 1: INGEST AND ANALYZE DATA

AI-powered data science is capable of processing huge volumes of energy use and other customer data to detect patterns and generate insights that enable more successful long-term NTL mitigation. Realizing the potential of this data-driven approach requires an investment in building a data lake that contains all the essential inputs for theft analysis, and then in leveraging AI to derive actionable insights from that rich data set.

ACTION STEPS

Deploy advanced metering infrastructure

Compile granular smart meter and other relevant customer data



Disaggregate energy consumption by appliance type

GETTING STARTED

DEPLOY ADVANCED METERING INFRASTRUCTURE (IF YOU HAVEN'T DONE SO ALREADY)

In many parts of the world, the most compelling business case for advanced metering infrastructure (AMI) deployment is revenue protection. While improving collections is typically top of mind, electricity theft detection offers an equally significant economic value proposition.

For example, electricity theft is a critical pain-point with Indian utilities. The country's ongoing massive smart meter rollout includes a variety of smart meter types capable of generating a wide range of essential analytics for theft detection and many other use cases. These meters include single phase whole current energy meters, three phase whole current trivector energy meters, three phase LT CT meters, three phase LT CT DTR meters, HT meters and feeder meters.

If you have already deployed AMI, you're well on your way already. Skip ahead to learn more about how to best compile your data sources.

For those utilities that have not yet invested in AMI infrastructure, consider a proof of concept roll out through which smart meters are installed on a limited number of homes — possibly 500 to 5000 — in order to demonstrate that the revenues recovered through analytics-driven theft detection are sufficient to justify a broader AMI rollout.

COMPILE GRANULAR SMART METER DATA AND OTHER RELEVANT CUSTOMER DATA

A sophisticated AI-based approach to identifying theft and other energy use anomalies requires a baseline understanding of the energy use behavior in every household. The foundation for that understanding is a broad set of granular data inputs.

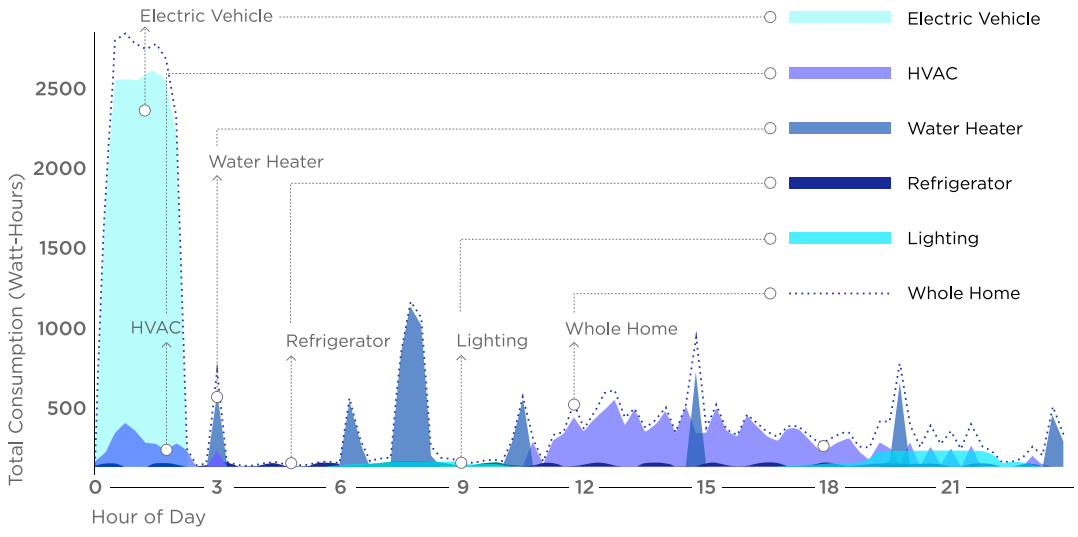
Relevant utility-provided smart meter intelligence includes consumption, current, voltage, meter events, power factor, and MDI. External data sources include weather/ambient temperature, geography, demographic, lifestyle and other available community intelligence.

These data inputs are combined to serve as the basis for creating a 360° energy use profile for every customer.

DISAGGREGATE ENERGY CONSUMPTION BY APPLIANCE TYPE

The more granular the data analytics capability, the more targeted, precise and successful non-technical loss prevention can be.

Advanced AMI data disaggregation algorithms break down total energy consumption data into identifiable appliance-specific usage patterns on a daily, weekly, monthly or bill cycle frequency. These appliance insights create a household energy use profile that includes what appliances are in use, when, and how much energy they are consuming. The energy usage patterns that emerge are key to accurate theft detection.

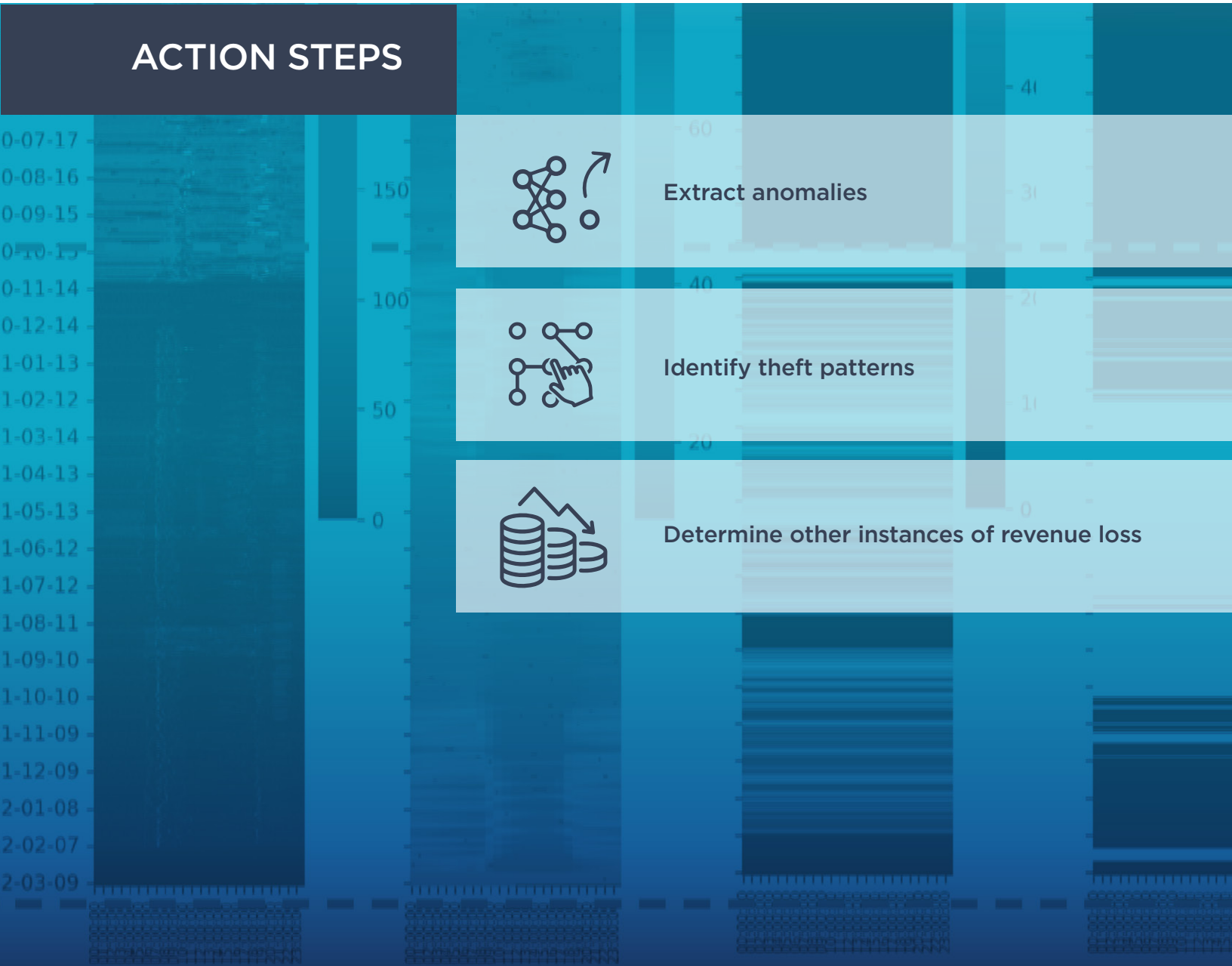


STEP 2: ACCURATELY DETECT AND CATEGORIZE INSTANCES OF NTL

AI-powered data science is able to model expected daily appliance consumption on a household-by-household basis during each season of the year. Deviations from expected behavior can then be isolated and categorized as energy usage anomalies. AI-powered algorithms are able to analyze and quantify these anomalies to uncover instances of theft, other revenue leakage and certain electrical safety anomalies in a number of important categories, including:

- **Meter tampering**
- **Direct theft through meter bypass of all or certain loads**
- **Tariff misuse**
- **Sanctioned load violations**
- **Poor power factor & earth leakage current detection**

ACTION STEPS



GETTING STARTED

EXTRACT ANOMALIES

By analyzing historical AMI data — for example, several months of 15-, 30- or 60-minute interval data — and correlating it with external factors like weather and AI-derived occupancy, and appliance/lifestyle profiling, it is possible to identify consumption-related anomalies. Similarly, by analyzing electrical AMI data and corresponding meter events, technical anomalies also can be identified.

The most precise theft indicator is the disparity between actual and expected energy consumption. Each anomaly can then be assigned a weighted theft signature.

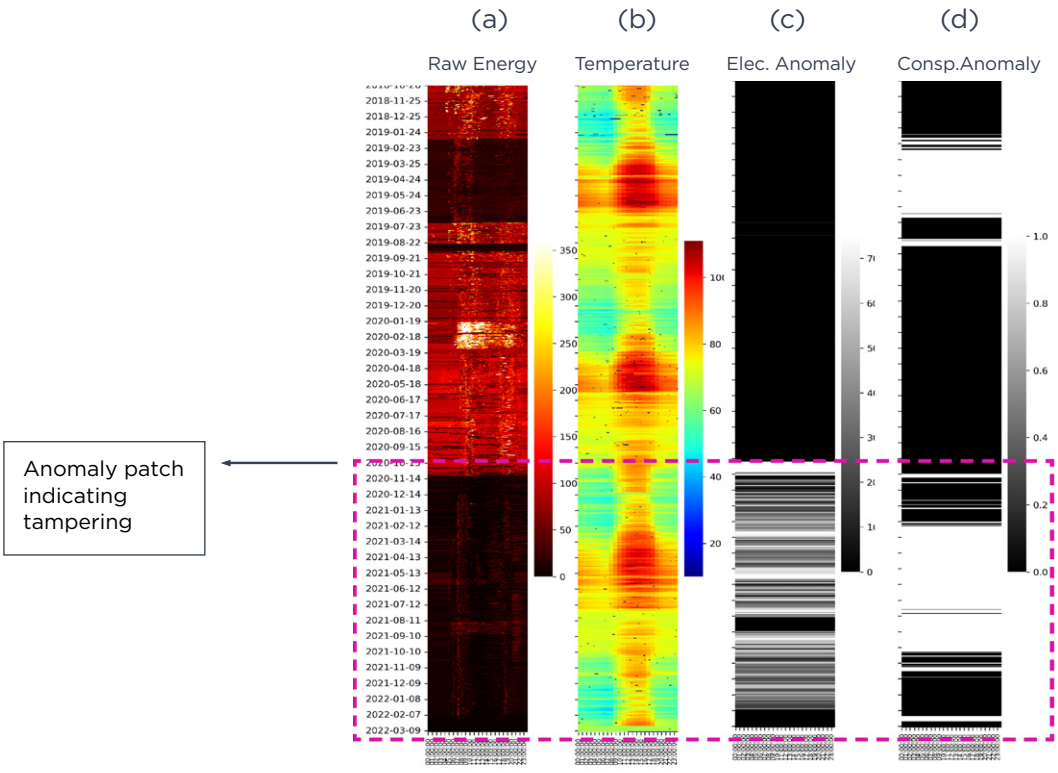
IDENTIFY THEFT PATTERNS

Meter Tampering

Electricity thieves use a number of electric meter tampering methods to prevent energy consumption from being recorded. Most of those methods are not reliably caught by meter hardware tamper alerts, which can also send false positives. AI-powered algorithms leverage energy consumption patterns, technical parameters of phase currents, neutral currents, voltages, power factors and available smart meter events to identify where and how meter tampering is most likely to have taken place, including:

- **Installing a shunt within the meter to "jump" the connection between grid supply and premises wiring**
- **Changing the sequence of terminal wiring**
- **Changing the current transformer ratio to reduce the recorded consumption**
- **Phase-to-phase short circuit**
- **Using alternate neutral lines**

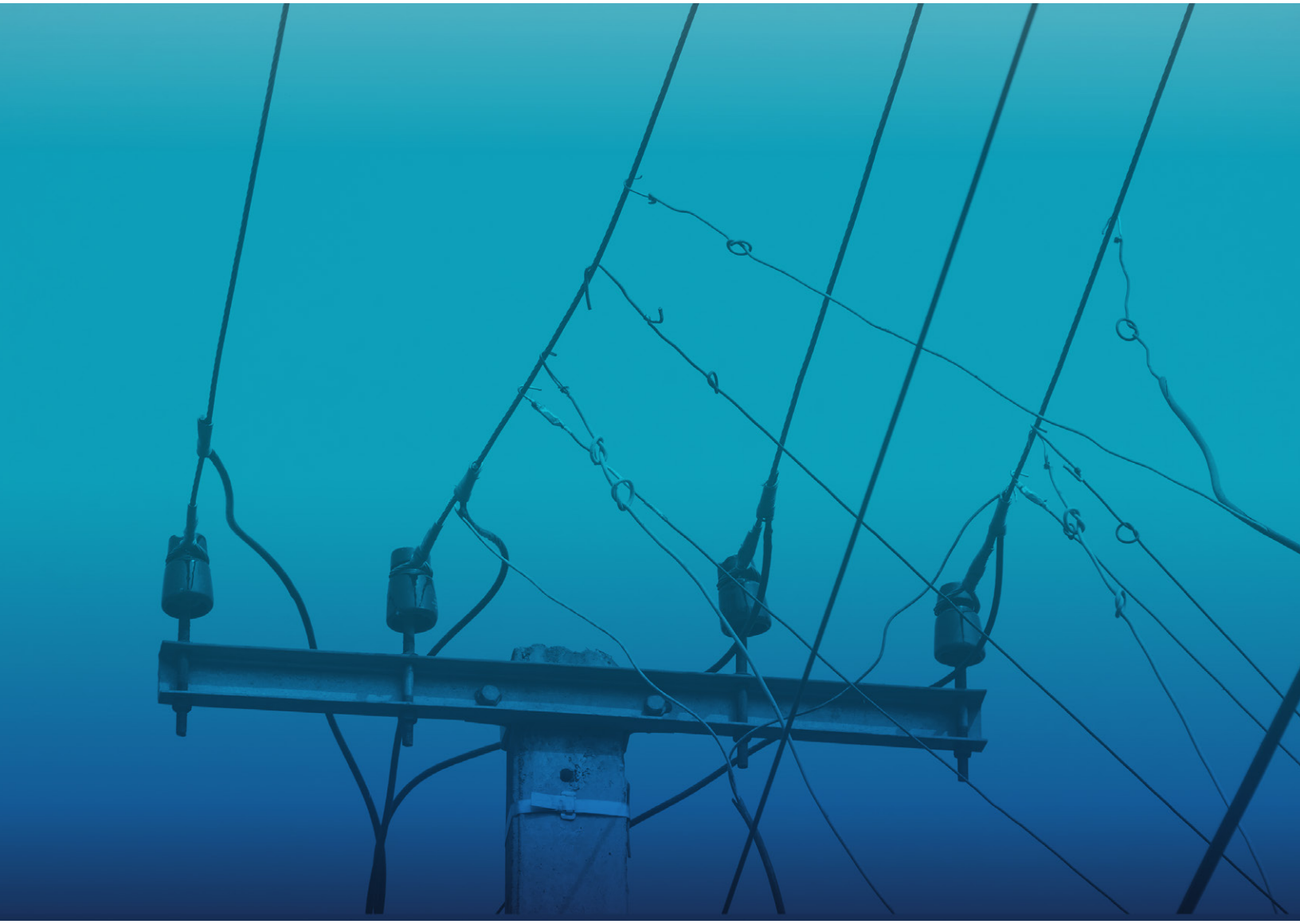
Tampering patterns include notable drops in consumption with corresponding electric anomalies.



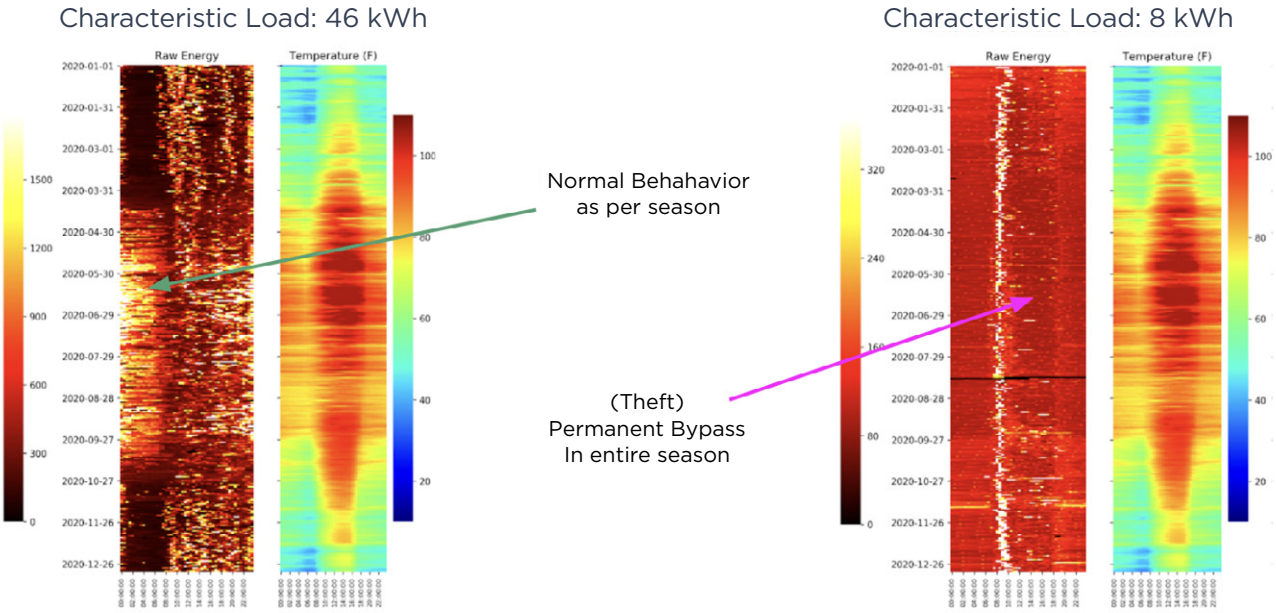
Direct Theft

Advanced data science can also determine when a consumer partially or completely bypasses the meter using an illegal connection mechanism on a permanent or intermittent basis to power some or all appliances.

For example, consumers may “hook” distribution lines through wires, cables, transformers, or a switch in order to place the meter in or out of circuit so that actual consumption is not recorded.



Direct theft patterns might include instances where past data confirms the presence of high consumption appliance followed by a period in which the appliance is no longer observed, even though there is occupancy in the premise and all other appliances show normal usage, or when there is a change in outside temperature but no corresponding change in electrical use — such as when a heat wave occurs but there is no increase in cooling-related electrical use. Analysis also looks at characteristic energy use for all homes with similar sanctioned/connected loads to identify significant outlier homes.



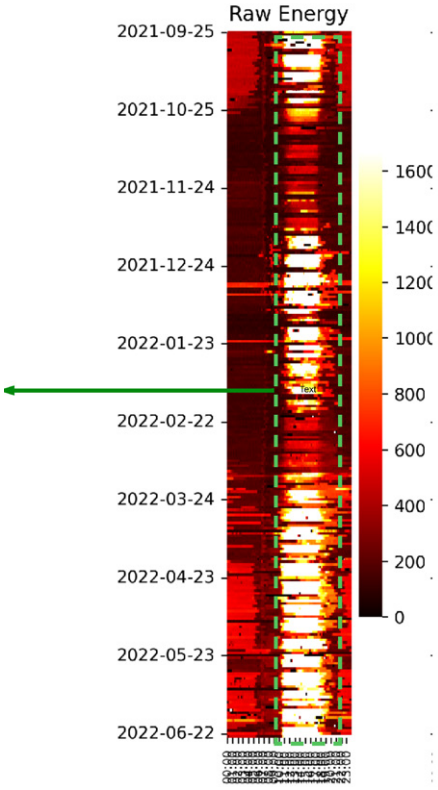
Tariff Misuse

Because smart meter data analytics isolate appliance-level signatures, it is possible to accurately distinguish between residential appliance behavior and commercial appliance behavior and determine when a customer's electricity use type is mischaracterized. Algorithms reveal patterns indicative of commercial activity on a residential tariff, including more challenging situations where there is mixed use.

Patterns that reveal likely tariff misuse might include significant activity during working hours, no activity on weekends or holidays, or non-residential appliance signatures.

Illustrative Example

Meter Number	XXYYXX
Open Time	8 am
Close Time	6 pm
AC	Present
SMB Probability	0.87
Rate Plan	Residential
Inspection	Check premise for commercial activity between 8am-6pm on Mon-Fri

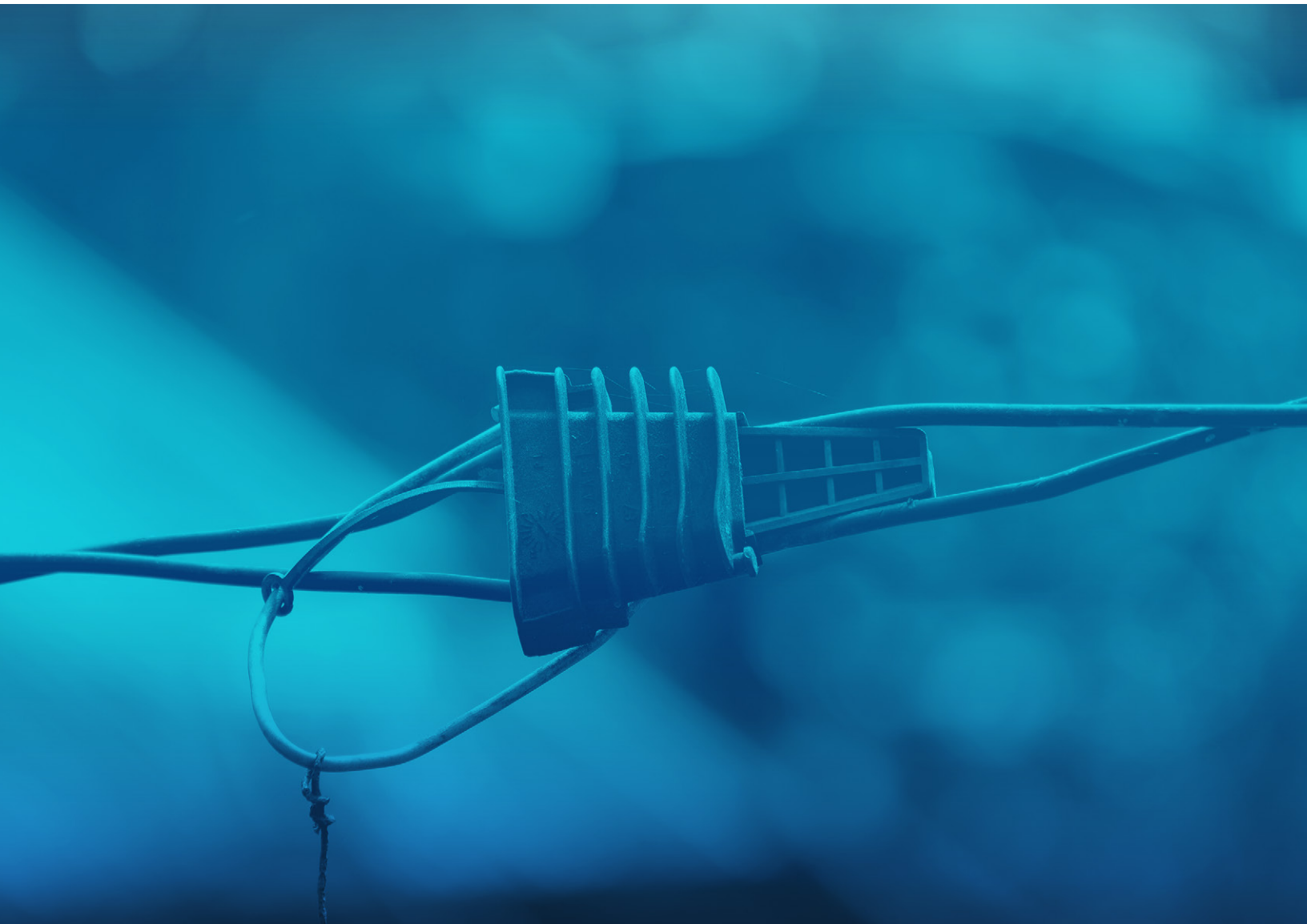


Poor Power Factor and Earth Leakage Current Detection

A high power factor is always desirable in a power delivery system to reduce losses and improve voltage regulation at the consumer-level. Power suppliers penalize consumers who operate at power factors below the specified threshold. The most sophisticated smart meter disaggregation can provide appliance usage information at the data sampling level to produce targeted insights for the energy provider as well the consumer on measures to improve the power factor values. For example, "Power factor is dropping because of air conditioner usage. Appliance and its wiring needs to be investigated." Similarly, it is possible for energy providers to identify earth leakage currents leading to unsafe wiring, and notify the consumer proactively as a safety measure.

Sanctioned Load Violations

Sanctioned load is the maximum amount of allocated power the consumer can draw from the grid at any particular interval. The higher the sanctioned load, the higher the customer's fixed charges. Advanced AMI data analytics can identify the frequency and the duration of instances when a customer violates the sanctioned load limit or violates sanctioned load by more than allowable limits. By identifying which customers are exceeding sanctioned load, energy providers are able to assess them for a higher fixed charge to recoup losses, and correct the behavior to avoid grid disruptions.



STEP 3: STRATEGICALLY TARGET BAD ACTORS

GETTING STARTED

PRIORITIZE THEFT INCIDENTS

Beyond smart theft detection, advanced data science is able to categorize theft incidents and bad actors as high, medium or low probability. The probability score is assigned based on the severity of the observed anomalies and how frequently they occur, as well as customer intelligence such as having previously engaged in theft-like behaviors such as unsafe wiring.

QUANTIFY LOSSES

In addition to the probability of theft, analytics also estimate how much energy loss occurred during an anomaly period. Consumption behavior modeling helps identify energy loss as a measure of the deviation from normal customer consumption.

Analytics also reveal the duration of theft activity and how many times the behavior was repeated — information a theft inspector cannot determine in a visit to a tampering site.

This loss estimation enables energy providers to focus mitigation efforts on the most significant violators to derive greater return on investment.

TARGET ENFORCEMENT

High probability and/or high value cases can be prioritized for immediate action, while medium and low probability cases can be closely monitored or issued warnings.

Energy providers are able to proceed with greater confidence before engaging with customers over a potential theft claim. Enforcement becomes more effective when it is based on actionable insights and a more strategic approach to on-ground inspections that yield higher conversions and lower turn-around times.

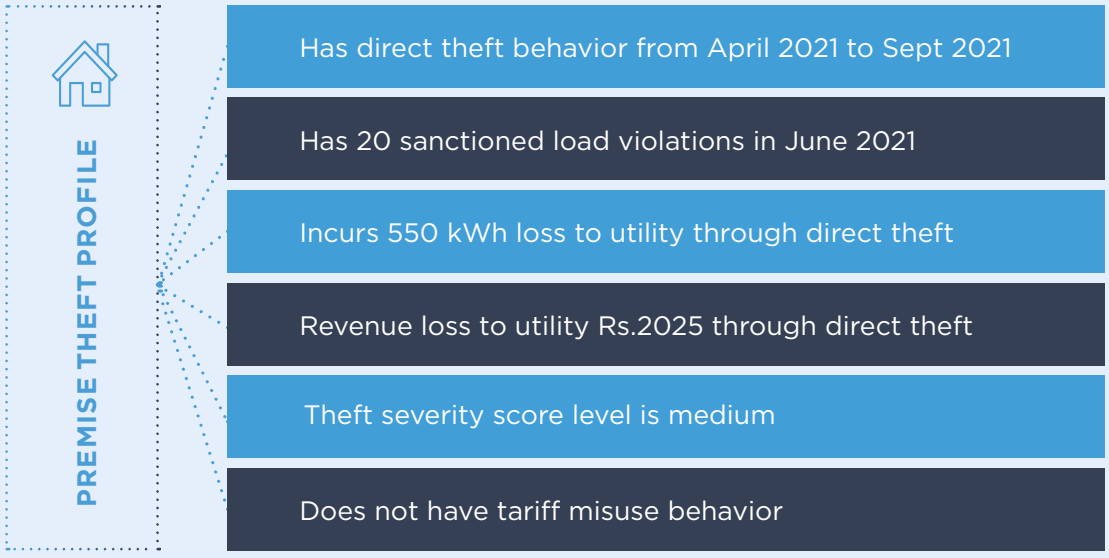
Further, AMI data provides evidence for case prosecution.

POST-INTERVENTION TRACKING

Track the behavior of bad actors that were either identified, inspected or booked for theft to ensure that they do not repeat the behavior using other methods. These actors would be placed on a “watchlist” and tracked for a longer period of, for example, 1-2 years. This approach is particularly useful for keeping suspected bad actors under observation who for some reason could not be booked on first inspection. Similarly, in the case of individuals who were booked, it is possible to track the impact of the action to establish improvement in kWh consumption in order to validate and confirm the action taken and to allow supervisory control.

In cases with ‘moderate probability,’ which may be too numerous to allow inspection, the utility may choose to simply send an advisory communication to the probable bad actors as a low-cost intervention. It is also possible to track the impact of this strategy.

Each account flagged for potential theft is given a profile based on these results.



GETTING STARTED

This playbook started with a look at the revenue impact of theft on utility performance, but the impact of theft is much greater.

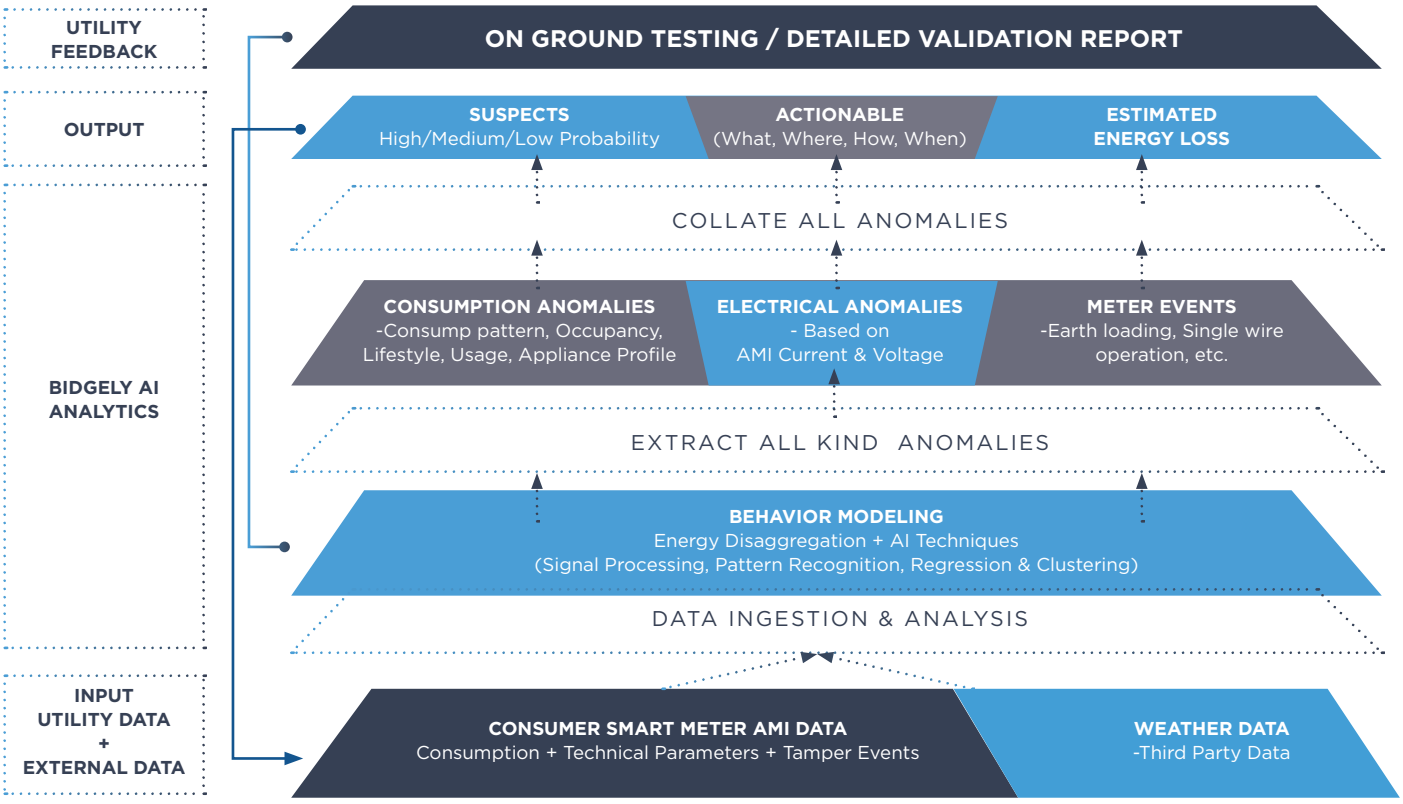
As utilities address a number of issues in a transforming energy future — decarbonization, transportation electrification, stricter regulatory requirements on efficiency, DER proliferation and more — theft is a common threat to the successful execution and performance of all such programs.

With so much on the line, the essential step all energy providers must take is THE NEXT STEP. If you don't have a theft strategy, start building one. If your theft remediation processes are not effective, get help rethinking them. If your data is in disarray, start organizing it in a data lake. If you've got smart meters, start using the behind-the-meter data available to you.

Bidgely is helping utilities solve the theft challenge.

Bidgely's UtilityAI™ Energy Theft Detection solution helps energy providers look behind the meter to determine exactly what appliance-level energy usage is occurring in every home, and equips them with precise tools to discover, understand, and remedy theft quickly.

BIDGELY APPROACH



To learn more about how Bidgely's Energy Theft Detection Solution can help you more successfully combat theft, visit

www.bidgely.com/solutions/energy-theft-detection

bidgely