



Beyond Surveillance:

Analytics for Self-Checkouts

Agilence Analytics Identifies Self-Checkout Abuse

Go beyond traditional surveillance methods to proactively identify patterns of theft and fraud in self-checkout lanes, ensuring a seamless and secure shopping experience. Agilence identifies specific instances and trends of abuse, such as:

- Low-Priced High-Value Items: Identify transactions
 where high-value items are scanned at unusually
 low prices, which could indicate label tampering or
 collusion with employees.
- Multiple Similar Items: Alert on transactions with an unusually high number of identical low-cost items, like multiple banana SKUs, which may be an attempt to disguise expensive items with cheaper items' barcodes.
- Payment Anomalies: Identify transactions with a high percentage paid by compromised methods, such as certain benefits cards.

- Repackaging: Report on transaction data to flag instances where the weight or quantity of a scanned item doesn't match typical purchasing patterns, suggesting possible repacking.
- Employee-Assisted Fraud: Alert on unusual activity by checkout attendants, including excessive price overrides, to identify collusion between employees and shoppers.
- Coupon and Price Overrides: Identify employees
 with a high volume of coupons or manual price
 overrides as this can be indicative of fraudulent
 activities.

Case Management Links Investigations

With the power of AI, Agilence Case Management's "Case Linking" feature connects incidents, making it easier to spot and stop self-checkout.

Use Case Linking to:

- **Find Patterns:** Identify common characteristics of incidents across stores.
- **Discover Connections:** Reveal links between incidents that weren't apparent before, like similar vehicles or suspect tattoos.
- Target Chronic Thieves: Automate the detection process and pinpoint chronic self-checkout abusers.



Self-Checkout fraud is committed by **1 in 7 customers**. How are you tackling it?