

How Retail Can Build a Security-First Data Architecture



Retail loves data. While tech companies get all the press when it comes to data and innovation, retail is quietly (and sometimes not so quietly) ramping up data collection and analytics to pursue the ideal customer 360 model. It has become essential to the industry's operations and provides personalization as a competitive differentiator.

Cybersecurity issues have also grown in proportion. As data collection shifts away from cookies, retailers must find a way to protect the data they gather while freeing it from silos that prevent personalization at the scale that customers crave. Luckily, a data operating system provides the answer to this balance.

Driving the need for a new type of data management in retail.

The retail data picture has become increasingly complex. Brands manage their own data, partners, and data acquired through buyouts and mergers. They're under increased pressure to accomplish competing goals like balancing privacy with personalization. The current climate, especially post-pandemic, will require a complete overhaul of how data management works. Here is what retailers are balancing.

Winning consumers with personalization

The vast majority of consumers want—and expect—personalization from retailers. They want their preferred brands to get to know them, enable frictionless experiences no matter where they're engaging, and offer continued value.

This is a significant differentiator that retailers don't want to give up. However, it opens them up to considerable

cybersecurity risks as they unlock the data they need. And it only takes one wrong turn to lose the trust of consumers everywhere.

Consumers typically feel better about brands that remember their past activities and behaviors on apps and websites but they also fear the amount of monitoring that companies do with their data. Consumers are very concerned with what companies are doing with customer data, and many also believe respecting buyer anonymity should be a higher priority.



So how do retailers manage these very different ideas? Consumers want both personalization and anonymity. Moving the needle in either direction means sacrificing one of these goals—traditionally.

Managing supply chains and inventory

Customers demand personalization, but behind the scenes, another significant driver for a revolution in data management waits. Retail operates on thin margins, and companies need real-time data analysis to help manage inventory.

Retail is embracing big data to help make data-driven decisions about inventory, prevent out-of-stock statuses that send customers to competitors, and better predict what goods will be where (and when). The ideal pipeline ensures retail has a grasp on even the most complex supply chain, but data silos from partners and within the retail organization itself can prevent these insights.

Breaches can cost companies millions

Data breaches can lose customers, but companies can face more far-reaching consequences than a hit to their brand. Companies lose revenue if sites go down. They pay the soft costs of failing to contain the breach in a timely manner.

According to Accenture, the average IT budget for security is 11% of the overall IT total. The cybersecurity market is growing, adding new tools every day to help companies manage their security and prevent these costly breaches.

While cybersecurity tools are a necessary part of data management, companies can also rethink governance and security in general by creating granular governance controls from the start. Thanks to the operational layer of a data operating system, this is now possible at scale.

Balancing security and personalization with a data operating system

A data operating system starts at the beginning. It allows companies to assign attribute-based administrative controls to data—no matter the source—so that each stakeholder has access to needed data. Administration can set granular governance controls from a single dashboard, see how data is used, and manage even legacy systems at scale.

Companies can bring data from anywhere—legacy lakes and warehouses, acquired data, third party data—and leverage these tag-based controls to free up data while ensuring compliance with regulations like GDPR. For international retail, this is a significant driver in scaling operations.

DataOS shifts retail data management to an access-based system. The company owns its data and grants access to individuals and departments based on these tags. Thanks to automatic profiling and validation, retail has everything it needs to succeed in the post-Covid normal without abandoning customer 360 dreams.

Curious about how DataOS—the world's first data operating system—is revolutionizing retail analytics?

BY E. WALLACE

[Learn more about our latest paper – The Latest Look in Retail →](#)



How Retail Can Build a Security-First Data Architecture

© 2022 The Modern Data Company. All trademarks are properties of their respective owners.

The Modern Data Company
306 Cambridge Ave
Palo Alto, CA 94306

[TheModernDataCompany.com](https://www.themoderndatacompany.com)
info@TMDC.io