Strengthen Data Safeguards with Simplified, Systematic, End-to-End Security

Earn customer trust and defend your brand with a holistic approach to data breach protection, detection and correction

Eight months after a 2013 major brand data breach:

“I don’t see how they’re getting out of this for under a billion, over time. It’s going to take them a long time to build the trust of the shopper and get them to where they were prior to December 2013.”

- John Kindervag
  Vice President, Forrester Research

Data Insecurity: The New Retail Reality

During a 2013 major brand data breach, the personal or credit card information of more than 100 million customers was compromised. The retailer subsequently spent hundreds of millions of dollars on breach-related costs.¹

Recent press accounts bring home the point: even for established, trusted retailers, one major security breach can inflict substantial damage in the form of short-term costs, revenue loss and longer-term damage to brand and customer relationships. But as the store environment evolves, the task of protecting data is becoming increasingly challenging to do well. Once, a one-dimensional strategy focused on protecting credit card data at fixed points of sale (POS) could suffice—but no longer. Now, retailers must also secure customers’ personally identifiable information—worth more than ten times the price of credit card information on the black market—and cope with a wide range of new store capabilities and new forms of payment. Meanwhile, organized cybercrime, now a multi-billion dollar shadow industry, grows ever-more sophisticated. To thrive in this evolving environment, retailers need a holistic approach to data security.

As retailers shift to unified commerce—the effort to connect all channels in real time to optimize the consumer experience—shoppers are interacting with data more often and in different ways than ever before. New capabilities, such as self-service checkout using the shopper’s personal device, click & collect, endless aisle, multi-channel returns, last-mile services, and mobile POS, appeal to consumers but raise the risk of data exposure. These capabilities demand a wide range of transaction devices—both fixed and mobile. As a result, they pose a significant challenge for retailers working to address privacy and security concerns.

As the number of transaction surfaces grows, Payment Card Industry (PCI) compliance is no longer sufficient to secure retail data and protect the brand. Addressing these challenges requires a systematic, end-to-end approach for data breach protection, detection and correction. Recognizing this, retailers are investing in enterprise-wide security architectures that reduce both data breach risk and complexity from POS devices all the way to the data center.

¹ According to John Kindervag, Vice President, Forrester Research.
The Benefits of an End-to-End Approach to Security

Adopting a holistic approach to data security offers significant advantages for retailers:

- Provides a silicon-based policy engine that operates on all transaction end points—fixed or mobile—that can encrypt the data retailers want to protect and keep that data out of the POS—or can do this for all data, according to the needs of the brand.
- Enables connected, proactive awareness, containment of threats and remediation.
- Allows retailers to strengthen ID protection with a combination of hardened identity factors that are right for the specific business.
- Simplifies scaling and extending the system so adding data centers, managers, and new functions is easily done.
- Makes it easier for advanced analytics tools to run complex queries on massive amounts of data to uncover patterns that provide insight into potential threats.

Digital Transformation and Business Innovation

New end-to-end data protection technologies allow brands to contend more successfully with the security challenges inherent in today’s complex retail environment by reducing data breach risk at three levels:

- **Protection** against data breach attempts—by reducing exposure or by detecting and blocking via deployed countermeasures so that an attack does not become a formal breach.
- **Detection** of in-process attacks—through an iterative process of finding attacks that were not prevented.
- **Quick correction** should an attack succeed—by rapidly remediating, restoring to normal operations and reporting the impact, followed by adapting countermeasures to prevent similar attacks in the future.

Enabling Transformation

Innovative solutions from Intel and its collaborators give brands the tools to meet customer needs more securely in an always-on, mobile, increasingly self-service retail environment. Solutions built with Intel security products and Intel® vPro™ technology help protect critical retail data and enable more secure, remote management of devices throughout the store—from fixed POS to interactive kiosks, sales associate mobile devices, self-service lanes, payment terminals, vending machines, interactive shopper tabletops and more. Intel® Data Protection Technology for Transactions, for example, is designed to help secure both credit/debit and personal data from the moment a transaction is initiated all the way through the storage of encrypted information on retailer and bank server networks.

Solution Summary

In the era of unified commerce—when the boundaries between physical store and online presence are collapsing and channels of engagement are multiplying—hardware and software systems in retail environments are deeply interconnected. Left unprotected, they are vulnerable to breach. This creates new opportunities for organized crime, and it means that retailers need comprehensive, easy-to-implement strategies that go beyond PCI compliance. The new, holistic approach taken by Intel and its technology collaborators addresses these challenges with components that help protect all retail data at every point along the shopper journey.

Intel Technology Foundation

- Intel Data Protection Technology for Transactions
- Intel Data Protection Technology w/ Intel® AES New Instructions (Intel® AES-NI) and Intel® Secure Key
- Intel® Authenticate Technology
- Intel® Trusted Execution Technology (Intel® TXT)
- Intel® Core™ vPro™ Processor-based Platforms
- Intel® Xeon® Processors
- Intel® Solid State Drives (Intel® SSD)
- Intel® Virtualization Technology
- Intel® IoT Platform
- Intel® Cloud Integrity Technology
- Open Network Insight Software

Where to Get More Information

For more information about security solutions from Intel and its collaborators, please visit [http://intel.com/retail/transactionsecurity](http://intel.com/retail/transactionsecurity).