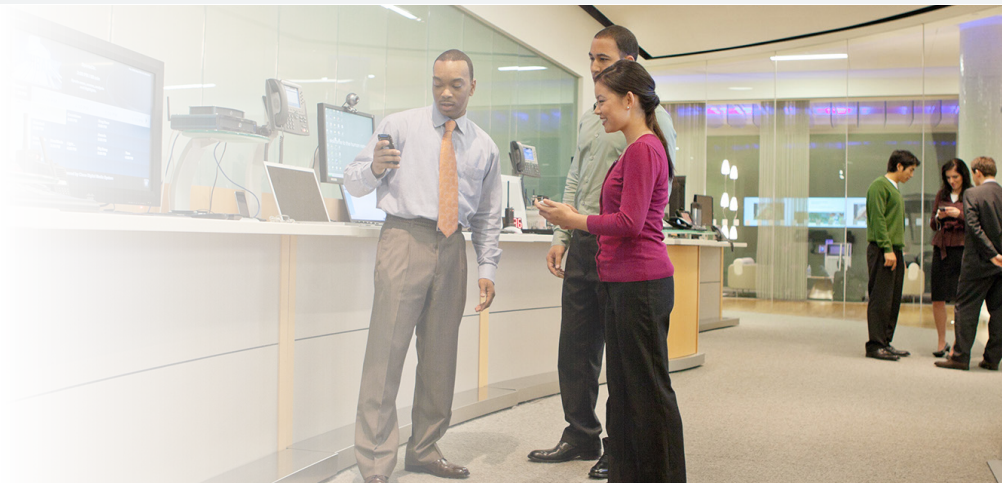
# Protect and Enhance Brand Value

## Cisco Risk Management for Retail



## Benefits

- Gain end-to-end protection, tailored for retail
- Safeguard customer, employee, and credit card data across multiple channels
- Secure the physical store, customers, associates, and assets
- Protect your brand and assets before, during, and after a cyber attack
- Reduce management complexity

### Customer Loyalty Begins with Security

The combination of mobile devices, distributed services, increased customer expectations, virtual systems, and changing business goals creates vulnerability for your retail brand. In fact, nearly 90 percent of consumers expect stores they shop at to stay up to date with the latest financial safety technologies.[1]

Weak security can profoundly damage brand loyalty and can also critically affect customers' trust.

Innovative retailers have recognized that risk management is a customer experience and revenue opportunity, not just a way to mitigate risks. They are finding ways to turn cybersecurity preparedness into a competitive advantage rather than a cost.

For instance, retailers that have a security breach may find shoppers less comfortable sharing personal information. As a result, they won't be able to offer the analytics-driven, personalized experiences that in-store and online that shoppers expect. Those customers will switch to a retailer that can provide better customer experiences supported by secure data.

### Mitigate Theft and Fraud

Retail shrinkage is a nagging and persistent challenge that infects any retail organization. Some shrinkage is from customers and others inside the store. Analytics enabled through video surveillance can provide a first-level defense across both types of threats. Video that tracks real-time movement of customers, associates, and assets can assess anomalies where threats may occur.

[1] PSFK Labs/MasterCard

> "Our biggest concern with cybersecurity breaches is not as much the direct financial impact...What would it do to us from a reputational standpoint? What if customers decide that we're not worthy of their trust and stay away?"
>
> – Greg Kleffner
> CFO, Stein Mart


## Secure Physical and Information (Data) Assets

Controlling access to high-value areas through access control can help protect against physical threats. But the greater threat arises from digital—m-commerce, e-commerce, and in-store payments—and these dwarf what physical intruders can gather. For example, retailers in the UK reportedly lost more than $850 million to hackers in 2013.[2] By implementing an end-to-end security architecture, you can mitigate both physical and virtual breaches and the associated costs of brand erosion.

## Simplify Regulatory and Process Compliance

In an industry immersed in compliance risk, retail organizations need to design strategies to sense internal and external compliance risks in order to thrive and create competitive advantage. For instance, payment card industry (PCI) mandates have put you at the forefront of data protection by absorbing the risk for noncompliance. Cisco® solutions and services simplify PCI compliance through a network segmentation approach.

Cisco Risk Management for Retail provides capabilities that are flexible and configurable, and you don't have to throw out existing solutions to see immediate benefits. It allows all your shoppers, associates, channels, and applications to use one highly secure, consolidated platform that protects their data and your business.

## Begin Protecting Your Customers Today

Let us help you draft an end-to-end risk management plan. For more information, visit Cisco Risk Management for Retail.

[2] Intel



C45-737262-00 02/17