Scaling Trust in Digital Commerce: How a Leading Online Retailer Fortified Its E-Commerce Ecosystem with Invinsense

About the Customer

This omnichannel retail company is part of one of India's largest and most trusted business groups. It offers a curated and premium online shopping experience across fashion, electronics, home essentials, and luxury goods through its e-commerce platform. With a robust digital footprint, integrations with third-party sellers, and an expanding logistics and warehousing network, the business prioritizes customer trust, transaction security, and digital resilience.

Industry	E-Commerce & Retail
Challenge	Securing online shopping infrastructure, customer data, and regulatory compliance at scale
Solutions Used	Invinsense XDR, XDR+, OXDR, GSOS

The Challenge

The company's growing e-commerce presence introduced new threat surfaces across applications, APIs, vendors, and data centers:

Frequent fraud attempts during checkout and refund processes	Exposed APIs connecting mobile apps, payment gateways, logistics platforms, and warehouse systems	Credential stuffing targeting customer accounts and loyalty programs
Pressure to comply with PCI-DSS, CERT-IN directives, and consumer protection regulations	Third-party integrations introduced blind spots in inventory sync and payment validation	Slow exposure validation, causing patching delays across multiple agile dev teams

The Invinsense Solution

To secure its high-volume transaction environment and ensure compliance, the retailer implemented a comprehensive cybersecurity program using the Invinsense platform.

Invinsense XDR: Unified Detection Across Shopping and Transaction Workflows

Invinsense XDR integrated with their front-end web apps, mobile apps, ERP systems, and payment APIs to detect and respond to threats across the transaction lifecycle.

Key Results:

- 62% drop in fraudulent checkout attempts (fake cards, test payments)
- 3.2-minute average detection time for credential stuffing
- 71% reduction in alert noise via ML-powered behavioral detection
- Improved incident triage across security, dev, and fraud teams

Invinsense OXDR + CTEM: Securing APIs, Inventory Systems, and Vendor Integrations

A Continuous Threat Exposure Management (CTEM) program was established to help the e-commerce platform move from reactive patching to proactive risk reduction.

Scoping	• Mapped 5,600+ digital assets, including product APIs, vendor onboarding portals, and fulfillment system links • 22% of exposed surfaces were shadow APIs used during festive sale launches
Discovery	• Discovered 190+ high-risk exposures including unauthenticated SKU endpoints and weakly encrypted payment webhooks • Found expired authentication tokens used by dormant vendors
Prioritization	• Focused on risks involving price manipulation, cart injection, and customer PII • Applied threat modeling based on live attack simulations and business impact
Validation	• Simulated inventory-based fraud attempts and discount abuse scenarios • Replayed known threat actor patterns against returns management systems
Mobilization	• Achieved 76% closure of validated risks within the first 30 days • Integrated auto-remediation playbooks into CI/CD pipelines for API fixes and inventory syncing

Invinsense XDR+: Deception for Shopping Cart Traps and Loyalty Abuse Detection

Deception strategies were deployed using fake checkout flows, unused coupon generators, and decoy seller onboarding dashboards.

Results:

5.8x higher attacker detection via decoy discount flows	Exposed two fraud groups targeting loyalty redemptions with automated scripts	Identified a pattern of pricing crawler bots imitating legitimate user agents	Reduced false positives in abuse detection by 68% through deception correlation

Key Result

- 69% faster detection of anomalous activity across digital portals
- 3.7x improvement in vulnerability validation cycles
- 91% coverage of required financial sector cybersecurity controls
- 5.3x increase in early threat identification using deception technology

Executive Insight

"Invinsense helped us move from transactional cybersecurity to strategic risk reduction. It's not just about detecting threats — it's about eliminating them before they disrupt the business."

CTEM Outcomes:

- 4.4x faster vulnerability validation
- 3.6x improvement in patch success rate across dev pods
- 52% reduction in exposed shadow APIs within two sprints

Invinsense GSOS: Streamlining Regulatory and Payment Compliance

GSOS helped the team standardize and report on security controls required by:

PCI-DSS for secure card handling and storage	CERT-IN reporting mandates for digital platforms	Consumer data protection under India's Digital Personal Data Protection (DPDP) Act	Internal IT policies for vendor access and fraud analytics

Compliance Outcomes:

91% alignment with regulatory control objectives	Audit preparation time reduced from 21 to 6 days	Compliance dashboard integrated with internal GRC workflows and partner contracts	Full mapping of security controls to 11 third-party systems

Quantifiable Impact

Category	Improvement
Fraudulent Transaction Attempts	↓ 62%
Time to Detect Credential Attacks	↓ to 3.2 minutes
Vulnerability Validation Speed	↑ 4.4x
Deception-Based Attacker Detection	↑ 5.8x
Regulatory Control Alignment	↑ 91%
Audit Readiness Cycle	↓ from 21 to 6 days

Conclusion

For online retailers navigating high transaction volumes, seasonal traffic spikes, and stringent compliance standards, digital trust is essential. This e-commerce leader used Invinsense to transform its security from reactive response to proactive exposure management, protecting customers, partners, and revenue — even during the busiest sales days.

Infopercept | INVINSENSE

About Infopercept - Infopercept is one of the fastest growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint

Contact
sos@infopercept.com
www.infopercept.com/knowledge/casestudy