

## Retail Case Study

# Secure AI at Scale

Transforming Customer Experience and Supply Chain Operations



## The Challenge

To safely operationalize LLMs at scale, the client needed to:

- Identify and eliminate vulnerabilities across customer-facing and backend systems
- Secure payment flows, customer data, and proprietary algorithms
- Ensure compliance with industry-specific standards without disrupting service

## Our Solution: AI Security Built for Retail

We delivered a retail-optimized AI security architecture that balanced performance, compliance, and trust.

## What We Did

- Applied the OWASP Top 10 for LLM Applications and the MITRE ATLAS framework, tailored to e-commerce environments
- Deployed secure API gateways to protect inventory systems and ensure controlled access
- Enabled end-to-end encryption for payment channels and sensitive data flows
- Strengthened authentication and token security with JWT and frontend protections
- Used tools like Microsoft Edge Developer Console to proactively monitor and secure interfaces



## The Business Impact

- ✓ **60% reduction** in AI-related security incidents
- ✓ **99.9% uptime** across core e-commerce systems
- ✓ Full PCI-DSS **compliance** with no disruption to service
- ✓ Increased protection of **customer trust** and brand reputation
- ✓ **Future-ready architecture** to scale secure AI use across operations



## Key Takeaway

This engagement shows how security and innovation can co-exist—with the right architecture, frameworks, and controls in place. By partnering early in their AI journey, we enabled the client to confidently unlock the benefits of LLMs while protecting what matters most: their customers, their data, and their business.