



Industry:
Retail

Use cases

- Tool consolidation
- Edge visibility
- Operational efficiency

Case study

Fortune 50 retailer consolidates security stack and saves \$10M with virtual NDR

Background: Securing the retail edge

This Fortune 50 retailer operates a massive distributed network of data centers and more than 2,000 individual store locations. Securing the “retail edge” is critical, as modern stores use connected devices, from point-of-sale (POS) systems to smart inventory scanners.

Challenge: The cost of visibility at scale

The customer faced a significant visibility gap. While data centers were monitored, the stores relied on a fragmented mix of open-source tools and expensive legacy NDR vendors. This created data silos and operational headaches.

Furthermore, deploying physical security appliances to 2,000+ locations was financially and logistically impossible, representing a potential capital expenditure of more than \$10 million. They needed a way to gain deep East-West visibility inside stores without the hardware price tag.

Solution: Virtual sensors and automation

The retailer deployed Corelight’s Open NDR Platform using Virtual Sensors running on existing store servers. This approach utilized available compute power without requiring new hardware.

To manage this massive fleet, Corelight resident engineers developed custom automation scripts interfacing with the Corelight Fleet Manager API. These scripts allowed the customer to schedule updates in granular “waves” (e.g., “Update these 50 specific stores at 3:00 AM”), bypassing bandwidth limitations and adhering to strict corporate change management rules.

Results: Unified data and massive savings

- **Hardware savings:** Saved an estimated \$5M–\$10M by utilizing virtual sensors instead of physical appliances
- **Operational efficiency:** The entire global deployment of 2,000+ sensors is managed by just two engineers
- **Tool consolidation:** Replaced legacy network security and performance monitoring solutions, unifying data formats across the enterprise for consistent threat hunting and visibility.
- **Data optimization:** Implemented custom filtering at the sensor level to reduce data volume by ~70%, preventing massive storage cost increases in their data lake

Why Corelight: Scalability and flexibility

Corelight was the only vendor capable of delivering high-fidelity data at the retail edge without a prohibitive hardware footprint. The flexibility of Corelight's Open NDR Platform allowed the customer to automate management at a scale that legacy vendors could not support.

Why it matters

Retail environments are increasingly "smart," creating a larger attack surface that includes unmanaged IoT devices. This customer proved that enterprise-grade visibility is achievable at the edge without breaking the bank, provided the solution supports virtualization and rigorous automation.



To see how Corelight helps retailers and high-tech security teams accelerate incident response and expand visibility, request a demo at

[**https://corelight.com/contact**](https://corelight.com/contact)

info@corelight.com | 888-547-9497