ENTERPRISE SECURITY TRANSFORMATION & ZERO TRUST RECOVERY

A Modernization Success Story Powered by IOSecure

CLIENT OVERVIEW

Industry:	Retail & Gaming
Footprint:	30+ Locations
Scale:	13,000+ Retail Gaming Terminals
Digital:	Integrated Online Gaming Platform
Annual Revenue:	~$3 Billion

THE CHALLENGE

The client faced a rising level of operational and compliance risk. Their security posture was **fragmented across five independent technology teams,** each managing tools, policies, and processes without coordination.

KEY ISSUES

- Conflicting and outdated security tools and standards
- Complex, expensive and unmanageable security operations
- Legacy tools increasing risk and operational friction
- Increased exposure to configuration errors, breaches, and compliance violations
- Falling behind in security operational best practices - needed new architecture to go faster

At the same time, the client was attempting to deploy a Zero Trust security platform, but the initiative – led by a global consulting firm – had stalled due to over-complication, lack of agility, missed timelines, and runaway costs.

LEADING THE SECURITY MODERNIZATION PROGRAM

IOSecure was engaged to bring **leadership, structure, and technical expertise** to drive enterprise-wide security modernization and rescue the Zero Trust project.

IOSECURE'S MODERNIZATION APPROACH

A large Canadian retail and gaming enterprise with extensive physical and digital operations was grappling with escalating operational and compliance risks stemming from a fragmented security posture across multiple independent technology teams, each handling disparate tools, policies, and processes without alignment.

This disarray not only amplified vulnerabilities to breaches and configuration errors but also hindered the deployment of a Zero Trust security platform, which had stalled under prior consulting efforts due to excessive complexity, missed deadlines, and escalating costs.

First Steps: Strategic Consulting & Technology Advisory

IOSecure was engaged to provide leadership, structure, and technical expertise in steering an enterprise-wide security modernization and recovering the stalled Zero Trust initiative. The process began with a comprehensive root-cause assessment of the existing security landscape, identifying issues such as over-complication, lack of accountability, and unclear architecture across the five technology teams. Drawing on these findings, IOSecure developed a streamlined roadmap that included centralized governance policies, scalable change management processes, and a right-sized deployment approach aligned with Zero Trust best practices and the client's operational needs.

Implementation: Enterprise Security Transformation & Zero Trust Recovery

IOSecure unified the security operating model by establishing clear standards, roles, responsibilities, and authorities, while simplifying processes to eliminate conflicts and enhance coordination among teams. Modern controls were implemented enterprise-wide, incorporating manufacturer and Zero Trust best practices to reduce complexity and ensure consistent policy enforcement, full visibility, and audit readiness. Structured decision-making and accountability models were introduced to accelerate delivery, bringing the Zero Trust rollout back on schedule and within budget without compromising quality or security.

Tracking Client Results

The outcome was a resilient, unified security framework that minimized operational friction, configuration errors, and compliance risks, fostering a predictable environment conducive to innovation and growth. By aligning technology with business priorities, IOSecure transformed the client's security operations into a strategic asset that enhances agility, efficiency, and long-term adaptability while supporting regulatory adherence and overall enterprise stability.

MEASURED RESULTS

OPERATIONAL EFFICIENCY

- Developed and implemented centralized security governance policies
- Introduced scalable change management processes for future growth
- Created clear and enforceable security standards, roles, responsibilities, and authorities
- Simplified and aligned the security operating model across all 5 technology teams

PERFORMANCE, RESILIENCE & PRODUCTIVITY

- 5 Teams Consolidated into a Single Security Operating Model
- Simplified Security Operations. Reduced risk of misconfiguration, errors, and non-compliance

ZERO TRUST PROGRAM RECOVERY

- Took over architecture of a stalled Zero Trust deployment previously run by a global consulting firm
- Conducted root-cause assessment: complexity, lack of accountability, and unclear architecture
- Delivered a right-sized, streamlined deployment approach aligned with Zero Trust best practices
- Re-established timelines, scope, and execution structure

LONG-TERM PREDICTABILITY & CONTROL

- Introduced structured decision-making and accountability models
- Improved delivery velocity without sacrificing quality or security
- Brought the Zero Trust rollout back on schedule and back on budget
- Delivered a successful enterprise deployment previously at risk of failure

> **Program restarted within 60 days** of IOSecure engagement

> **Delivery timeline accelerated by ~40%** versus prior plan

> Clear milestones and ownership established for 100% of Zero Trust components

> **Improved mean time to detect** (MTTD) and investigate security events

IOSECURE

STRATEGIZE + SIMPLIFY + OPTIMIZE =

TECHNOLOGY EMPOWERING PEOPLE, DRIVING INNOVATION

We work with clients to build a clear strategy, scope just the hardware and software required and optimize the technology so your IT stack delivers dependable and secure business results.

604 945 6324 contact@iosecure.com

IOSECURE.COM