

Case Study: Optimizing Cybersecurity Efficiency for a Global Software Company



**CISO and SVP,
Information Technology**



ORNA's expertise noticeably transformed how we view and approach cybersecurity across our portfolio, reducing costs while enhancing our security coverage. Their comprehensive assessment streamlined our tool stack, alleviated team workload, and delivered immense value to our operations. We're now more secure, efficient, and well-positioned to address pressing cybersecurity challenges and will continue to use ORNA to support our 2025 initiatives.

About ORNA



ORNA is a boutique Canadian cybersecurity company headquartered in Toronto, Ontario, pioneering proprietary hybrid SASE cybersecurity posture orchestration, compliance, and cross-functional incident response automation in zero-trust environments. ORNA's AI cloud security products and advisory services benefit over 450+ organizations in 11 countries.

The Client

The client, a 3,500-employee company, specializes in acquiring, managing, and building industry-specific software companies worldwide. With operations in 30 countries, covering over 40 vertical markets, and managing more than 150 subsidiary organizations, the company is tasked with complex software procurement and cybersecurity management across a vast and diverse portfolio.

Challenges

The company faced significant challenges in its software procurement and cybersecurity functions:

- 1 Balancing Budget Pressures with Security Needs**
The client's C-suite applied increasing pressure to control escalating cybersecurity budgets, without compromising the integrity of their infrastructure or leaving their subsidiary organizations vulnerable.
- 2 Justifying Essential Cybersecurity Investments**
The company experienced delays in justifying essential technology and security purchases needed to safeguard their subsidiaries, resulting in potential gaps in coverage and inefficiencies in the procurement process.
- 3 Managing Complexity Across Multiple Products**
With over 70 separate security products deployed, the company struggled to maintain transparency, command, and cost-efficiency over its cybersecurity investments. The overlap between tools created redundancies, while the sheer number of solutions placed undue strain on the cybersecurity and IT teams, increasing the risk of burnout.

Solution

The company hired ORNA to help analyze and optimize its cybersecurity tool stack, aiming to balance cost efficiency, tool management workload, and comprehensive security coverage.

The project was designed to assess the company's existing cybersecurity solutions across multi-cloud and on-premises infrastructure environments (including hybrid HQ/Data Centers, SaaS applications, endpoints, FWaaS, CASB, and more), identify redundancies, and provide a strategy for reducing costs while improving or maintaining cybersecurity standards.

Case Study: Optimizing Cybersecurity Efficiency for a Global Software Company

Project Approach

ORNA undertook a comprehensive cybersecurity solutions gap and coverage assessment, including:

Analysis of over 300 tools and technologies deployed across the company's multi-cloud and on-premises environments.

Conversations with 12 client stakeholders from various business units to understand their specific cybersecurity needs and concerns.

Review of over 40 internal documentation articles and compliance frameworks to ensure alignment with corporate and regulatory standards.

ORNA's focus was on identifying consolidation opportunities, eliminating redundancies, and confirming or adjusting the robustness of the configuration of the resulting cybersecurity stack for optimal efficiency.

Key Findings

Throughout this 3-month engagement, ORNA uncovered several critical insights:

11 cybersecurity products with unused licenses were found across the portfolio, contributing to unnecessary expenditures.

60% in vendor price variability was identified, showing significant opportunities for cost negotiation or replacement.

Consolidation or replacement of 8 security tools was recommended, allowing for streamlined management while improving coverage.

Results

The project led to remarkable improvements in both cost savings and security effectiveness:



38% reduction in annual cybersecurity spend was achieved through tool consolidation and vendor renegotiations.



The company's **cybersecurity coverage was increased or maintained** with fewer tools and vendors, ensuring that security wasn't compromised while trimming excess costs.



Reduced burnout and overwhelm among the cybersecurity and IT teams, who previously had to manage the complexity of dozens of tools, by simplifying the stack and improving visibility across security functions.

ORNA's comprehensive assessment and optimization project not only delivered significant cost savings but also enhanced the client's cybersecurity posture. By consolidating tools, eliminating redundancies, and streamlining vendor relationships, ORNA helped the company strike a balance between budget efficiency and robust cybersecurity. This enabled the client to protect its extensive global operations with fewer resources while maintaining high security standards across its diverse portfolio of subsidiaries.