A 100-Year-Old Financial Services Firm Modernizes Cybersecurity with Seceon

Executive Summary:

A leading financial services firm with over 140 years of history, $1.4 trillion in assets under management, and 14,000 employees worldwide faced growing cybersecurity challenges. The firm managed multiple subsidiaries, partners, and financial entities, requiring a multi-tenant security approach to protect its diverse operations while ensuring continuous compliance with SEC, FINRA, PCI-DSS, and GDPR regulations.

The firm relied on multiple disparate security tools—traditional SIEMs, endpoint security, compliance tracking, and threat intelligence platforms—which created visibility gaps, operational inefficiencies, and high costs. To modernize its security posture, Seceon's AI-driven Open Threat Management (OTM) platform replaced these tools, providing:

- Multi-tenancy support to secure multiple business entities
- 90% faster threat detection and response
- 60% cost reduction by consolidating security tools
- Real-time compliance monitoring and automated audit readiness
- Significant reduction in cyber risk across global financial operations

The Challenge: Managing Security Across Multiple Financial Entities

Key Cybersecurity Risks

As a large financial institution with multiple subsidiaries, affiliates, and partner entities, the firm faced several cybersecurity challenges:

- **Sophisticated Cyber Threats** – The firm experienced a growing number of ransomware, phishing, supply chain attacks, and insider threats.
- **Multiple Isolated Security Tools** – Managing different security platforms across multiple business units led to high costs, inefficiencies, and gaps in visibility.
- **Slow Incident Detection & Response** – The legacy SIEM was too slow and reactive, creating delays in identifying and mitigating threats.
- **Compliance Complexity** – The firm had to meet SEC, FINRA, GDPR, and PCI-DSS regulations across multiple jurisdictions, making compliance tracking a manual and time-consuming process.

Challenges with the Existing Security Stack

The firm had invested in multiple cybersecurity solutions, but they were:

- **Siloed and Fragmented** – Different subsidiaries used separate security tools, making it difficult to correlate threats.
- **High Operational Costs** – Licensing, maintenance, and integration of multiple security tools increased overall costs.
- **Lack of Real-Time Compliance Management –** Preparing for audits required weeks of manual work, increasing regulatory risk.
- **No Multi-Tenancy Support** – The existing security infrastructure could not effectively manage cybersecurity across multiple business units from a central platform.

Requirements for a Modern Security Platform

The firm needed a solution that could:

- Replace multiple security tools with a single, unified platform
- Leverage AI and automation to detect and respond to threats in real time
- Provide multi-tenancy support for subsidiaries and financial partners
- Ensure continuous compliance with financial regulations and reduce audit costs
- Enhance security visibility while reducing operational complexity and costs

The Solution: Seceon's AI-Driven Multi-Tenant OTM Platform

To overcome these challenges, the firm implemented Seceon's Open Threat Management (OTM) platform, replacing multiple security tools with a single, AI-powered solution that delivered:

1. **AI-Driven Threat Detection & Automated Response**

- Behavioral AI & Machine Learning analyzed financial transactions, network traffic, and endpoint activity to detect:
  - Insider threats
  - Advanced persistent threats (APTs)
  - Phishing and credential theft
  - Ransomware attacks
- Automated Incident Response executed security playbooks, blocking malicious IPs, isolating infected systems, and enforcing security policies in real-time.

2. **Multi-Tenant Security Across Business Units & Entities**

- Seceon's OTM platform provided a centralized security dashboard with full visibility into security events across:
  - Corporate Headquarters
  - Regional branches & subsidiaries
  - Wealth management & investment divisions
  - Third-party financial partners
- Granular Access Controls allowed each entity to maintain security autonomy while ensuring unified threat monitoring.

3. **Continuous Compliance & Automated Audit Readiness**

- Real-time compliance monitoring ensured adherence to:
  - SEC & FINRA regulations for financial transactions
  - PCI-DSS for secure payment processing
  - GDPR for global data privacy compliance
  - NIST & ISO 27001 frameworks for cybersecurity best practices
- Automated Compliance Reports eliminated manual tracking and ensured audit readiness at all times.

4. **Cost Savings & Operational Efficiency**

- Replaced multiple security tools (SIEM, threat intelligence, endpoint security, compliance management) with a single, integrated platform, reducing costs by 60%.
- SOC Workload Reduced by 50%, enabling security analysts to focus on proactive threat hunting rather than managing alerts.

Transforming Financial Cybersecurity with seceon

$1.4T Assets

140+ Year Financial Firm

14,000 Employees

Before Seceon

- Multiple Security Tools
- Slow Response
- Complex Compliance
- Complex Compliance

After Seceon

Unified Platform

- Fast Response
- AI-Powered Security
- Multi-Tenant Support

Seceon OTM Platform Impact

90%	60%	50%
Faster Detection	Cost Reduction	SOC Workload

Implementation: Seamless Migration to Seceon OTM

Phase 1: Security Assessment & Risk Analysis
Seceon's cybersecurity experts conducted a full assessment of the firm's infrastructure, identifying security gaps and compliance risks across its business entities.

Phase 2: Multi-Tenant Deployment & Integration

- Integrated Seceon OTM with existing security infrastructure, including:
  - Firewalls
  - Cloud environments (AWS, Azure, Google Cloud)
  - Endpoint protection solutions
  - Financial transaction monitoring systems
- Deployed with zero downtime, ensuring uninterrupted financial operations.

Phase 3: AI-Powered Threat Monitoring & Compliance Automation

- Within the first month, Seceon AI detected multiple suspicious insider activities and a phishing campaign targeting executive accounts.
- Automated incident response blocked attacks before they could escalate.
- Compliance dashboards enabled real-time monitoring for SEC, FINRA, and PCI-DSS adherence.

The Results: A Future-Ready Cybersecurity Strategy

1. **Significant Reduction in Cyber Risk**

- 90% faster threat detection and response, stopping attacks before impact.
- Eliminated manual security event correlation, reducing alert fatigue.
- Prevented a supply chain attack that could have compromised partner institutions.

2. **Multi-Tenancy Enabled Secure Business Operations**

- Centralized security for multiple subsidiaries, affiliates, and partners.
- Improved security visibility while allowing separate business units to maintain operational autonomy.

3. **Continuous Compliance & Cost Savings**

- Real-time compliance monitoring reduced audit preparation time from months to hours.
- Automated compliance reports ensured adherence to SEC, FINRA, GDPR, and PCI-DSS.
- Reduced cybersecurity costs by 60% by eliminating multiple security tools.

4. **Enhanced SOC Efficiency & Threat Intelligence**

- SOC workload reduced by 50%, enabling proactive threat management.
- AI-driven insights provided predictive threat detection, reducing response time from hours to seconds.

Conclusion: Seceon OTM as the Future of Financial Cybersecurity

By replacing multiple security tools with Seceon's AI-powered, multi-tenant OTM platform, the firm strengthened cybersecurity, streamlined compliance, and reduced operational costs.

Key Takeaways

- AI-Driven Threat Detection & Automated Response for real-time security.
- Multi-Tenancy for Subsidiaries & Financial Partners to meet compliance requirements.
- Automated Compliance Management for SEC, FINRA, PCI-DSS, and GDPR.
- Lower Costs, Improved SOC Efficiency, and Faster Risk Mitigation.

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 640 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 8,800 clients.

Learn more about Seceon aiXDR and

Schedule a Demo www.seceon.com/contact/