When Static Tools Fall Short: How a Global Firm Rebuilt Cybersecurity with Seceon



Executive Summary:

An enterprise struggling with legacy cybersecurity tools and fragmented vendor solutions faced persistent security gaps and slow response times. With attackers adapting daily, their 3-5 year security contracts left them exposed to outdated technologies. By adopting a unified, adaptive security platform, the organization gained full telemetry, contextual visibility, and continuous innovation, closing gaps, reducing risk, and eliminating dependency on stitched-together products that failed to evolve with threats.





Key Cybersecurity Risks

- **Advanced Threats:** The organization faced a growing volume of ransomware, phishing, and supply chain attacks, some leveraging living-off-the-land techniques.
- **Fragmented Security Stack:** With over a dozen disparate tools, including separate SIEM, EDR, NDR, CSPM, and DLP products, integration gaps and blind spots were routine.
- **Detection Delays**: The average time to detect and respond stretched into weeks, giving adversaries ample time to persist and exfiltrate.
- **Compliance Burden:** Manual processes for SEBI, PCI-DSS, and GDPR audits required weeks of effort across teams.

The Challenge: Legacy Tools and Contract Lock-in

The organization’s security model was based on legacy assumptions: that a collection of "best-of-breed" tools would provide the strongest defense. In practice, it resulted in integration chaos. The firm used different vendors for SIEM, EDR, NDR, DLP, vulnerability management, and cloud security posture management, among others.

Each department or regional subsidiary had chosen its own tools over time, further splintering the security stack. Most tools were tied to long-term contracts, locking the firm into rigid solutions even as threats evolved. These limitations became evident when attackers exploited integration gaps to breach systems that were, on paper, "protected."

Manual investigation and correlation meant that key signals were missed or dismissed. An internal breach investigation showed a pattern of ignored alerts spanning 35 days—alerts which, had they been connected in real-time, could have led to early intervention. Instead, the delayed response cost over $47 million in damages.

The Turning Point: Realizing the Innovation Gap

A detailed MITRE ATT&CK analysis revealed that the firm’s detections occurred primarily in the later stages of an attack—often during lateral movement or data exfiltration. Their existing tools lacked the telemetry breadth and context to flag early-stage activity.

Despite significant investments, threat actors were outpacing the firm’s defense. SOC analysts were managing 23,000 alerts daily, with an estimated 90% false positive rate. Security teams were overwhelmed and unable to prioritize real threats over noise.

The board and executive leadership realized their multi-year contract strategy was outdated and counterproductive. They needed a platform that could evolve with the threat landscape, not one that expired before it became useful. The search began for a unified security platform with measurable, demonstrable ROI.

Requirements for a Modern Security Platform

To regain control and efficiency, the firm required a solution that could:

- Replace multiple security tools with a unified platform to simplify operations
- Leverage AI and ML for behavior-based threat detection
- Provide a real-time automated response to reduce the mean time to containment
- Ensure continuous compliance and generate real-time audit reports
- Offer centralized visibility across multiple business units and subsidiaries
- Support multi-tenancy to enable federated but unified security operations

The Solution: Seceon's Unified Security Platform

Seceon delivered a complete transformation. Its AI-driven Open Threat Management (OTM) platform replaced fragmented security products with a tightly integrated solution that:

- Ingested and correlated telemetry from endpoints, network, cloud, users, and applications
- Delivered behavioral analytics and anomaly detection using AI/ML
- Executed automated playbooks for threat containment and policy enforcement
- Supported multi-tenancy, giving business units localized control under a centralized platform
- Enabled real-time compliance monitoring across SEC, PCI-DSS, GDPR, and NIST



Unlike traditional SIEMs, Seceon's unified codebase meant no custom integrations or patchwork fixes were needed. Within days of deployment, Seceon's AI identified a phishing campaign targeting executives and prevented an insider threat from escalating into a breach.

Implementation & Deployment

Phase 1: **Security Assessment & Gap Analysis**
Seceon's team conducted a full risk and infrastructure assessment, identifying blind spots, false-positive hotspots, and high-risk assets.

Phase 2: **Platform Integration**
The Seceon platform was deployed across cloud (AWS, Azure), endpoint, and network environments. Despite the scale, integration was completed in under two weeks with zero operational downtime.

Phase 3: **Threat Monitoring & Automation Activation**
AI-powered threat detection was activated across all telemetry sources. Automated responses were enabled to isolate endpoints, block IPs, and enforce policies. Dashboards for compliance, risk scoring, and SOC metrics went live.

Measurable Results

Metric	Before (Multi-Vendor)	After (Seceon Platform)
Alert Volume	23,000/day	1,400/day
False Positives	73%	8%
MTTR	12 days	47 minutes
MTTD	89 days	3.2 days
Analyst Productivity	67 alerts/day	340 alerts/day
Annual Breach Cost	$67M	$2.1M
Annual Licensing	$4.2M	$1.2M
Integration Cost	$1.8M	$0.3M

Strategic Outcomes

- **90% Faster Threat Detection:** Seceon's AI enabled early-stage detection, stopping threats before impact.
- **Unified Visibility:** All business entities reported into a central security dashboard while maintaining local autonomy.
- **Proactive Compliance:** Real-time compliance dashboards replaced manual audits, cutting audit prep time by 90%.
- **Operational Efficiency:** SOC workloads dropped 50%; analyst productivity rose over 400%.
- **Economic Impact:** By replacing 14 vendors, the firm saved 64% in annual licensing and reduced breach losses by 97%.

Why Seceon

Seceon's Open Threat Management platform stands out by offering:

- AI-driven behavioral detection across all vectors (network, endpoint, cloud)
- Integrated SIEM, XDR, SOAR, UEBA, TI, and VA on a single codebase
- Multi-tenant security for federated environments
- Real-time automation with transparent, explainable alerts
- Compliance-ready reporting for regulated industries

Conclusion

The firm's adoption of Seceon represented a strategic shift from reactive, siloed security to an intelligence-led, unified cybersecurity approach. No longer constrained by integration gaps or long-term vendor lock-ins, the enterprise gained the freedom to evolve, adapt, and scale its defenses in real time.

Seceon not only unified over 20 specialized security tools into one operational framework—it replaced complexity with clarity, manual effort with automation, and lagging compliance with real-time audit readiness. The measurable improvements in risk reduction, SOC productivity, and cost savings demonstrate what modern cybersecurity should deliver: business resilience. In an era where the velocity and sophistication of cyberattacks are only accelerating, Seceon proved that staying ahead isn't about adding more tools—it's about using the right platform to make faster, smarter decisions.

With Seceon, the firm turned cybersecurity into a strategic advantage and set a new standard for future-ready security operations.

Learn more about Seceon aiXDR and

Schedule a Demo www.seceon.com/contact/



© 2025 Seceon Inc. All rights reserved. aiSIEM, aiXDR, aiMSSP are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.