How a U.S.-Based MSP Transformed into an Advanced Cybersecurity Provider with Seceon



Executive Summary:

A leading Managed Service Provider (MSP) in the United States faced increasing customer demand for advanced cybersecurity services while also needing to enhance its own security posture across the managed IT infrastructure of hundreds of customers. The MSP struggled to scale its security operations due to:

- High cost and complexity of building a 24x7 Security Operations Center (SOC)
- Inefficiencies from using multiple disjointed security tools
- Growing cyber threats targeting MSPs as prime attack vectors
- Regulatory compliance challenges across multiple industries





By adopting Seceon's AI-driven Open Threat Management (OTM) platform, the MSP:

- Transformed into an advanced cybersecurity provider
- Achieved triple-digit revenue growth Year-over-Year (YoY)
- Improved gross margins to 60-70% within one year
- Reduced security risk across all customer environments
- Strengthened its own cybersecurity posture to prevent MSP-targeted attacks
- Implemented multi-tenancy for regulatory compliance management

With Seceon, the MSP was able to compete with top MSSPs, attract new customers, and significantly scale its cybersecurity business while also ensuring its own IT infrastructure remained resilient against modern threats.

The Challenge: Scaling Cybersecurity While Reducing Its Own Risk

1. **Growing Demand for Advanced Cybersecurity**

The MSP had a strong customer base across SMBs, healthcare, finance, manufacturing, and government organizations. However, customers increasingly required proactive, AI-driven cybersecurity solutions to combat rising threats like:

- Ransomware & phishing attacks – Especially targeting MSPs and their customers.
- Regulatory compliance pressures – Meeting HIPAA, PCI-DSS, CMMC, and NIST standards.
- Advanced Persistent Threats (APTs) – Zero-day exploits and sophisticated adversaries.



2. **The MSP Itself Became a Prime Target for Cybercriminals**

MSPs are attractive attack vectors because they manage the IT infrastructure of multiple businesses. A single breach could compromise all their customers.

The MSP faced:

- Growing threats targeting MSPs via supply chain attacks
- Increased risk of lateral movement across customer networks
- Limited visibility into real-time threats affecting customer environments
- Difficulty managing compliance across multiple industries

3. **Inefficiencies from Managing Multiple Security Tools**

The MSP used multiple disjointed security tools for SIEM, endpoint protection, firewalls, and vulnerability management. These tools:

- Generated overwhelming alerts, leading to alert fatigue.
- Had no unified correlation, making it difficult to detect real threats.
- Required extensive manual intervention, slowing response time.
- Were expensive, cutting into profit margins.

To stay competitive, scale security services, and protect itself from MSP-targeted threats, the company needed a single, AI-driven platform that could detect, prevent, and respond to threats in real time across all customers.

The Solution: Seceon's AI-Driven Open Threat Management (OTM) Platform

The MSP adopted Seceon's OTM platform to replace multiple security tools, enabling:

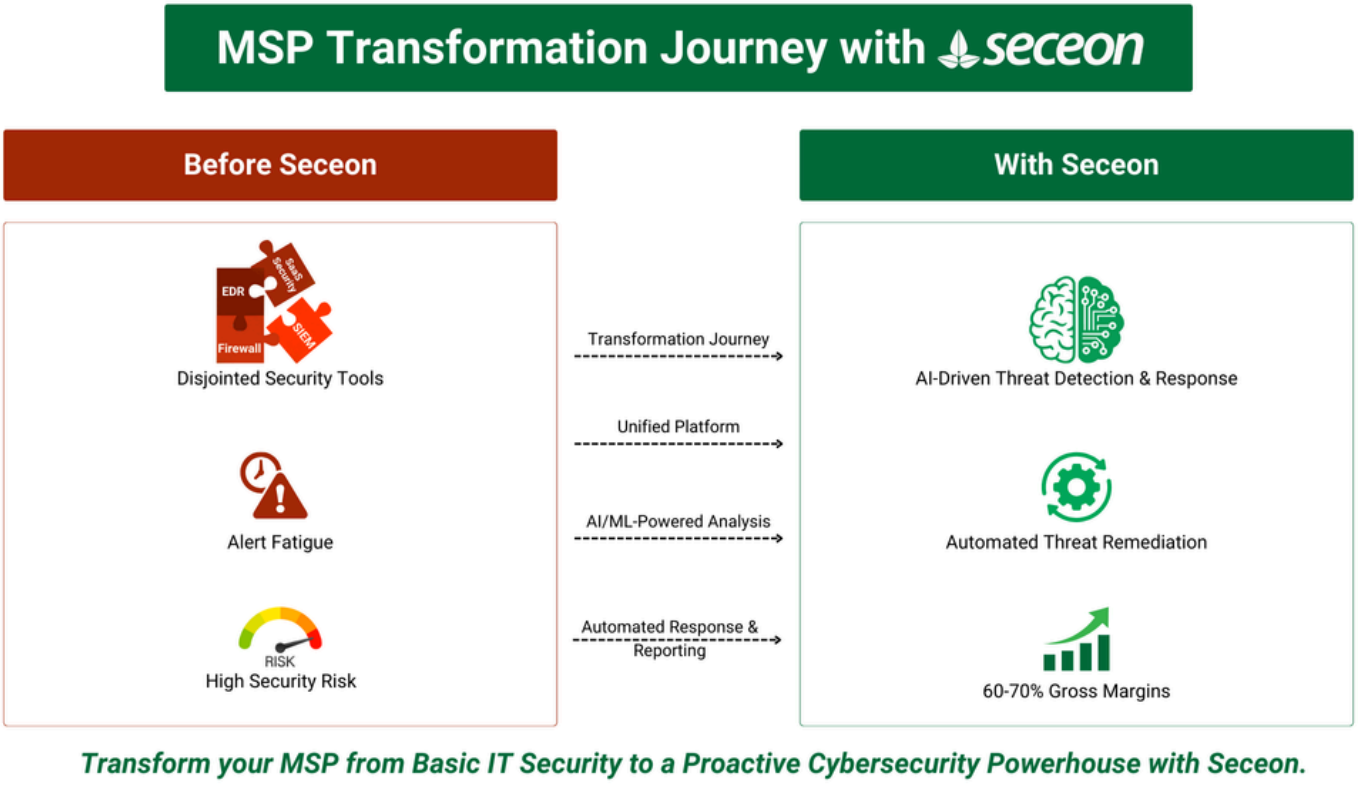
- AI-driven threat detection & automated response
- Multi-tenancy to manage cybersecurity across multiple customers securely
- Continuous compliance management for audit readiness
- Improved MSP security posture with real-time visibility & automated protection

1. **AI-Driven Threat Detection & Automated Response**
   - AI-driven behavioral analytics detected threats in real time.
   - Automated response mechanisms immediately contained and neutralized cyberattacks before they could spread.
   - Stopped ransomware, insider threats, and APTs across customer environments within seconds.

2. **Multi-Tenancy for Secure, Scalable Cybersecurity Services**
   - Seceon's multi-tenant architecture enabled the MSP to provide advanced security services across multiple customers while ensuring strict data separation.
   - Customers could access custom security dashboards while the MSP maintained centralized control.

3. **Securing the MSP's Own IT Infrastructure**
   - Protected the MSP from supply chain attacks targeting IT service providers.
   - Enhanced internal cybersecurity monitoring across the MSP's own operations.
   - Reduced the risk of a single breach affecting all customers.

4. **Replacing Multiple Security Tools with a Unified AI-Driven Platform**
   - Eliminated redundant security tools, cutting operational costs by 50%.
   - Unified threat detection, monitoring, and compliance tracking into a single platform.
   - Reduced the need for additional security analysts, improving operational efficiency.



Transform your MSP from Basic IT Security to a Proactive Cybersecurity Powerhouse with Seceon.

Implementation: A Fast & Smooth Transition

Phase 1: Initial Risk Assessment & Planning

- Evaluated security risks across customer environments and the MSP's internal infrastructure.
- Identified gaps in current security tools and mapped compliance requirements.

Phase 2: Seceon OTM Deployment & Integration

- Deployed Seceon's platform across all customer environments within weeks.
- Configured automated threat detection & response policies based on each customer's risk profile.
- Provided hands-on training for security analysts on using AI-driven threat monitoring.

Phase 3: Expanding Advanced Cybersecurity Services

- Introduced Managed Detection & Response (MDR) and Extended Detection & Response (XDR) services.
- Automated compliance tracking for HIPAA, PCI-DSS, NIST, CMMC, and ISO 27001.
- Integrated Seceon's threat intelligence feeds for proactive defense.

Phase 4: Reducing MSP's Risk While Scaling Cybersecurity Business

- Strengthened its own cybersecurity defenses to prevent MSP-targeted attacks.
- Gained real-time visibility into threats across all managed environments.
- Doubled customer acquisition by offering cutting-edge security services.

The Results: A Profitable, Secure, and Scalable Cybersecurity Business

1. Triple-Digit Revenue Growth YoY

- New cybersecurity services became the MSP's fastest-growing business unit.
- Increased customer base by 150% in the first year.

2. Achieved 60-70% Gross Margins

- Reduced operational costs by 50% by eliminating redundant security tools.
- Fewer security analysts are required, improving efficiency and profitability.

3. Strengthened Security Across Customers & the MSP Itself

- Blocked multiple ransomware attacks before execution.
- Eliminated lateral movement risks across customer environments.
- Improved internal SOC capabilities to defend against supply chain attacks.

4. Continuous Compliance & Audit Readiness

- Automated compliance for HIPAA, PCI-DSS, CMMC, and more.
- Reduced customer audit preparation time by 80%.

5. Competitive Advantage & Industry Leadership

- Successfully competed with major MSSPs by offering enterprise-grade security at a fraction of the cost.
- Became a trusted cybersecurity provider for critical industries.

Customer Testimonials

CEO, The MSP:
"Seceon's platform transformed our business. We went from offering basic IT security to becoming a high-margin cybersecurity powerhouse with triple-digit revenue growth. It's a game-changer!"

CISO, Financial Services Customer:
"With our MSP using Seceon, we now have real-time threat detection, automated response, and continuous compliance monitoring—all without increasing costs."

Director of IT, Healthcare Client:
"Cybersecurity was a major concern for us. Our MSP's transition to Seceon means we now have 24x7 AI-driven protection, ensuring patient data is secure."

Conclusion: Future-Proofing the MSP's Business and Security

By adopting Seceon's AI-driven OTM platform, the MSP:

- Scaled its cybersecurity services profitably
- Strengthened its own security posture against MSP-targeted threats
- Eliminated inefficient security tools, reducing costs
- Ensured continuous compliance for highly regulated industries

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 464 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/

© 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.