How an MSSP Transformed Onboarding and Scaled Global Security Operations with Seceon



Executive Summary:

A leading Managed Security Services Provider (MSSP) struggled to onboard customers efficiently due to operational complexity, tool sprawl, and integration challenges. With over 10 different security tools, their security stack was fragmented, leading to:

- Prolonged onboarding times – Some customers remained partially onboarded for over four months.
- High operational costs – Multiple tools required separate licensing, management, and expertise.
- Inefficient security operations – Lack of a unified view made threat detection and response slow and inconsistent.
- Limited scalability – The MSSP was unable to expand its services effectively to MSP partners and international customers.





By transitioning to Seceon's AI-driven Open Threat Management (OTM) platform, the MSSP achieved:

- Full onboarding of most customers within days
- Successful onboarding of its largest customer in just 4 days (compared to 4+ months of failed efforts previously)
- A unified platform replacing 10+ security tools, drastically reducing operational complexity and costs
- The ability to act as a Master MSSP, delivering cybersecurity services to multiple MSPs and businesses across various countries
- Continuous security posture improvement with automated threat detection and response
- Compliance management to ensure audit readiness for multiple regulatory frameworks

With Seceon, the MSSP transformed its security business, enabling rapid customer expansion, reduced risk, and a scalable cybersecurity service offering at an affordable price point.

The Challenge: Slow Customer Onboarding & Inefficiencies from Multiple Security Tools

1. **Struggles with Onboarding Customers Efficiently**

• Onboarding delays of over four months for some customers, leading to frustration.
• The largest customer, with a complex IT environment, remained incompletely onboarded despite multiple efforts.
• Multiple teams had to be involved in configuring different tools, leading to resource drain.

2. **Managing 10+ Disjointed Security Tools**

The MSSP relied on a complex stack of security tools, including:
• Traditional SIEM solutions
• Endpoint Detection & Response (EDR)
• Threat Intelligence Platforms
• Vulnerability Management Tools
• Network Detection & Response (NDR)
• Firewall and Intrusion Detection Systems (IDS/IPS)

Each tool required separate integration, monitoring, and alert triage, creating:

- High costs for licensing and operations
- Fragmented threat visibility
- Inefficient security incident response

3. **Limited Scalability for MSSP & MSP Partners**

The MSSP wanted to expand globally by working with MSPs as a Master MSSP, but:
• The complex security stack made it difficult to manage security across multiple partners.
• High operational costs prevented competitive pricing for MSP partners and customers.
• Regulatory compliance requirements varied by country, making security operations more complex.

4. **Customers at Increased Risk Due to Slow Deployment**

Without complete onboarding, some customers were operating with blind spots, leaving them vulnerable to:

- Advanced cyber threats (ransomware, insider threats, APTs, and zero-day attacks)
- Compliance violations due to lack of security monitoring and reporting
- Inconsistent security policies across assets and geographies

A Critical Need for a Unified, AI-Driven Cybersecurity Platform

The MSSP needed a single, AI-powered cybersecurity platform capable of automating threat detection, response, and compliance tracking to simplify operations, accelerate customer onboarding, and scale globally.

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

1. Rapid, Seamless Customer Onboarding

- Most customers are onboarded within days instead of months.
- The largest customer (which was stuck in onboarding for 4+ months) was fully operational in just 4 days.
- All assets and security controls were integrated automatically, providing immediate threat visibility.

💡 **Why It Worked:**

- Automated asset discovery ensured all endpoints, network devices, cloud workloads, and applications were protected.
- AI-driven analytics instantly identified vulnerabilities and security gaps.
- Zero-touch deployment eliminated manual configuration issues that delayed onboarding.

2. **Replacing 10+ Security Tools with a Unified AI-Driven Platform**

- SIEM + EDR + NDR + SOAR functionalities in one
- AI-driven threat detection & response across endpoints, networks, and cloud
- Eliminated integration issues, streamlining security operations
- Lower operational costs and reduced staffing requirements

> *"We're hyper-focused on building best-of-breed cybersecurity solutions for our customers and Seceon is core to that strategy. Built on the aiSIEM platform, our award-winning solution, XDR, offers proactive defense monitoring and alerting to safeguard our clients from various attacks and downtime-causing incidents."*
> *-CTO, MSSP*

💡 **Why It Worked**:

- Real-time correlation of threats across all attack vectors (endpoint, network, user, and cloud).
- Automated response actions, reducing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).
- Fewer tools meant lower costs and simpler management.

3. Master MSSP Enablement for MSP Partners & Global Expansion

- Multi-tenancy allowed secure segmentation of MSP partners & customers
- Affordably priced security services enabled global growth
- Compliance management tailored for different industries & geographies

💡 **Why It Worked:**

- Multi-tenant architecture enabled seamless management of multiple MSPs and customers under a single pane of glass.
- Each MSP partner could have their own security dashboard, while the MSSP maintained centralized visibility.
- Automated compliance tracking ensured audit readiness for regulations like GDPR, HIPAA, PCI-DSS, and NIST.

4. **Improved Cyber Resilience and Security Posture**

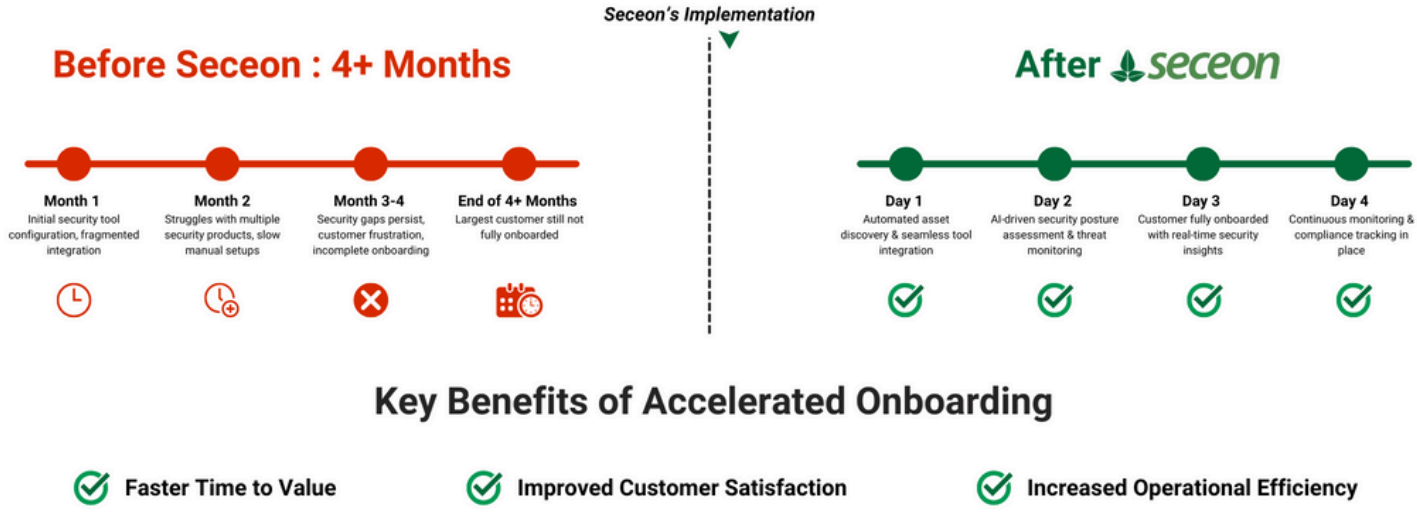
- Real-time AI-driven detection and mitigation of cyber threats
- Proactive security controls reducing attack surfaces
- Continuous security posture improvement with automated assessments

💡 **Why It Worked:**

- Seceon's AI detected threats before they escalated, unlike legacy SIEM solutions that relied on logs alone.
- Proactive vulnerability assessments enabled remediation before cybercriminals could exploit weaknesses.
- Continuous monitoring and adaptive threat models ensured resilience.

MSSP Growth Timeline: Onboarding Acceleration

From 4+ Months to Just 4 Days with Seceon



Key Benefits of Accelerated Onboarding

- **Faster Time to Value**
- **Improved Customer Satisfaction**
- **Increased Operational Efficiency**

Implementation: A Smooth and Efficient Transition

Phase 1: Risk Assessment & Strategy Development

- Evaluated existing security gaps across all customers and MSP partners.
- Mapped business objectives with security needs.

Phase 2: Seceon Platform Deployment & Integration

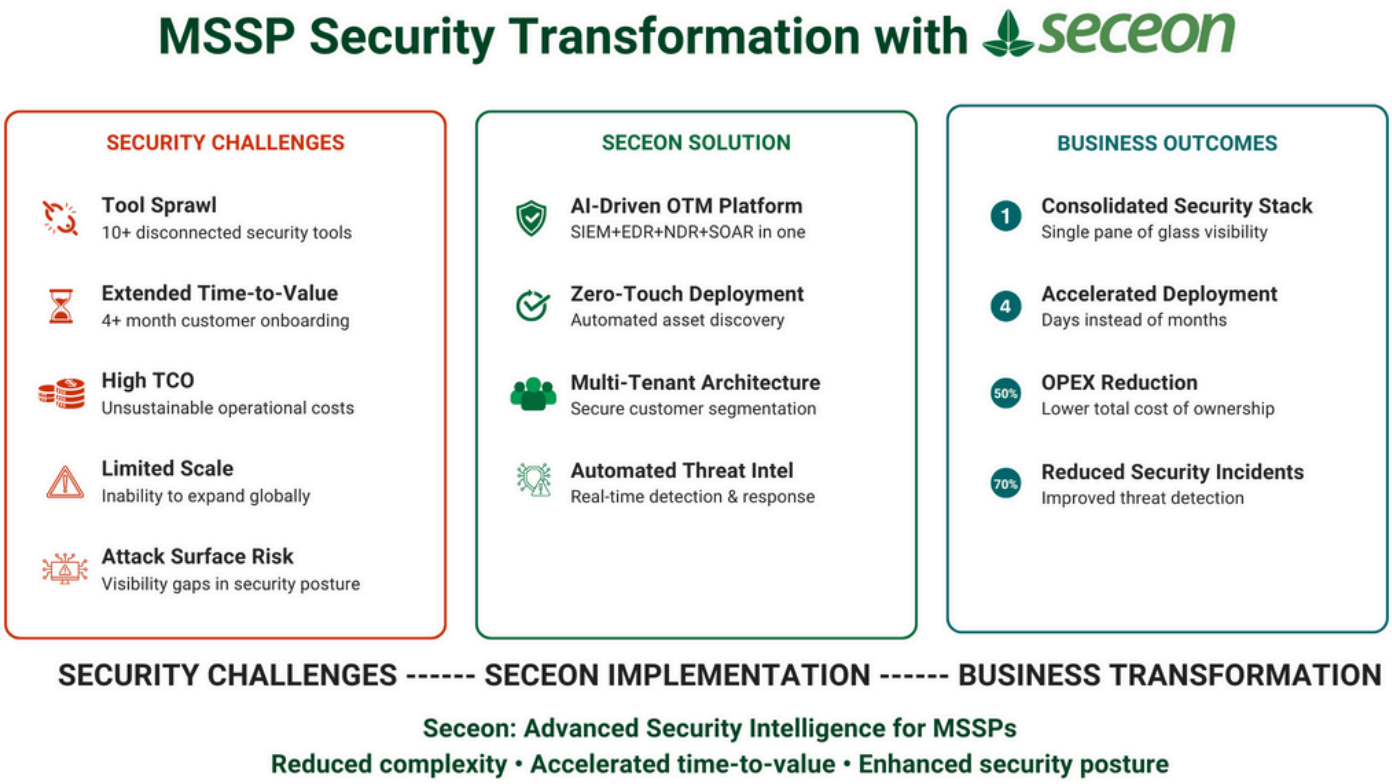
- Automated discovery of all customer assets and security controls.
- Configured threat detection & response policies based on individual customer risk profiles.

Phase 3: Large-Scale Onboarding & Security Optimization

- Most customers onboarded within days, eliminating previous delays.
- The largest customer was fully onboarded in just 4 days.
- Multi-tenancy enabled secure, scalable security management for MSP partners.

Phase 4: Scaling Operations as a Master MSSP

- Expanded services to multiple countries, supporting diverse compliance needs.
- Provided affordable pricing, increasing MSP partner adoption.
- Implemented continuous compliance tracking, reducing audit preparation time by 80%.



The Results: A High-Growth, Efficient, and Scalable MSSP

1. **Faster Customer Onboarding & Increased Satisfaction**
   - Most customers fully onboarded within days instead of months.
   - Largest customer fully operational in 4 days, compared to over 4 months previously.
   - Higher customer retention & satisfaction scores.

2. **Significant Cost Reduction & Improved Efficiency**
   - Eliminated 10+ security tools, reducing software licensing and staffing costs.
   - 50%+ operational cost savings by consolidating security functions.

3. **Master MSSP Enablement for MSP Partners & Global Reach**
   - Multi-tenancy enabled secure, scalable cybersecurity services across multiple countries.
   - Affordable pricing attracted more MSP partners & customers.

4. **Enhanced Cyber Resilience & Continuous Compliance**
   - AI-driven automated threat detection & response reduced security incidents by 70%.
   - Continuous compliance monitoring ensured audit readiness at all times.

Conclusion: A Scalable, Future-Proof Cybersecurity Business

By transitioning to Seceon's AI-driven OTM platform, the MSSP:

- Accelerated onboarding from months to days
- Eliminated tool sprawl, improving efficiency and cost savings
- Enabled a scalable, global Master MSSP business model
- Reduced risk and enhanced customer security postures

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/



© 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.