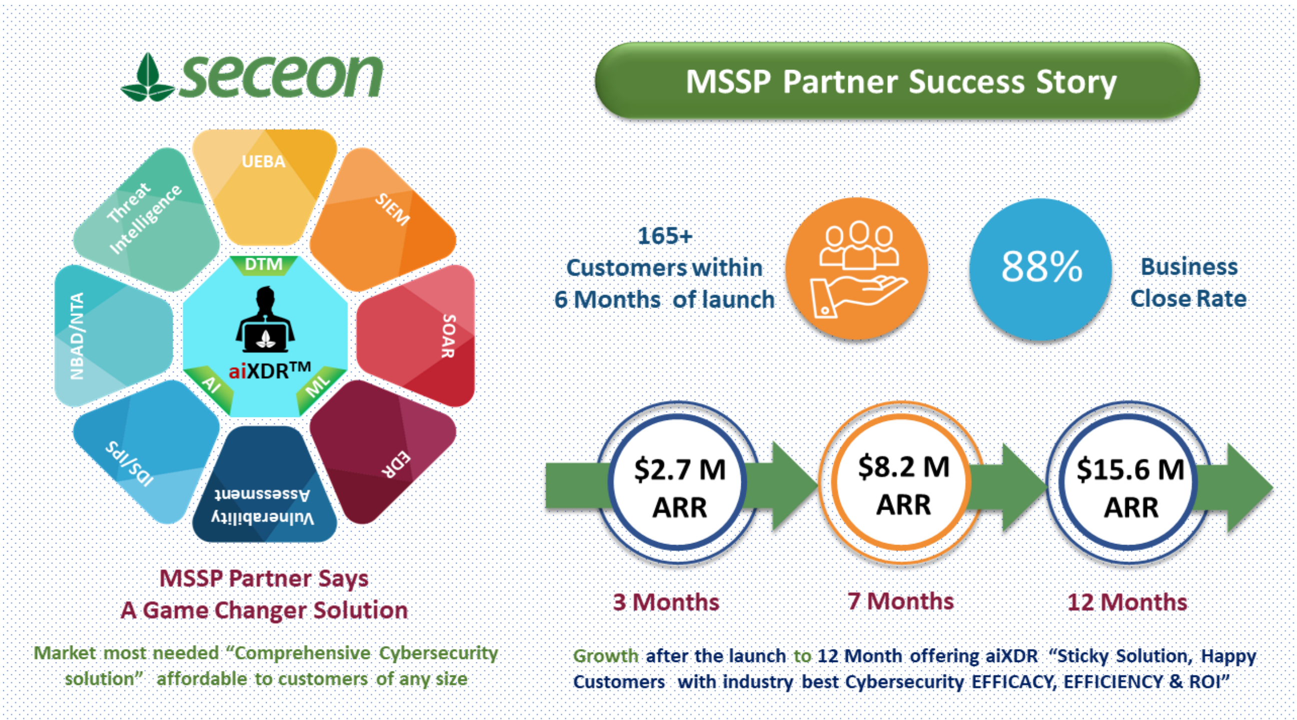
Sector: MSSP



MSSP Partner Success Story

165+ Customers within 6 Months of launch

88% Business Close Rate

$2.7 M ARR — 3 Months

$8.2 M ARR — 7 Months

$15.6 M ARR — 12 Months

MSSP Partner Says
A Game Changer Solution

Market most needed "Comprehensive Cybersecurity solution" affordable to customers of any size

Growth after the launch to 12 Month offering aiXDR "Sticky Solution, Happy Customers with industry best Cybersecurity EFFICACY, EFFICIENCY & ROI"

With nearly 20 years in business, this MSSP headquartered in Midwest US, set their eyes on cybersecurity from get go. They realized long back that existing security services were too expensive and required dedicated staffing for ongoing operations and maintenance. Hence, the company built its managed security service offerings around vendor specific solutions fulfilling the needs of managing Firewall, Email Security, Endpoint Security, Security Assessment, Wireless Network Security, Compliance and Extended Detection and Response (XDR). This MSSP with 550 customers (as of mid-2021) was recently acquired by a Managed Service Provider in Northeast USA with wide ranging services, particularly based on the value they serve in cybersecurity.

It is interesting to note that the MSSP has white-labeled Seceon's aiXDR platform to deliver XDR with their SOC-as-a-Service offering rolled out to customers in wide range of sectors – Healthcare, Retail, Hospitality, Financial Services and Government.

What approach did the MSSP take in segmenting and targeting customers?

Segmentation policy followed by the MSSP was based on value acknowledgment and service impact. Hence, existing customer base of 100 to 500 employees each, was targeted in the 1st wave of value positioning – a segment that was benefitted from the MSSP's existing services.

Next, in target were net new clients, most of whom were Manufacturing clients ($100M - $1B in yearly revenue) and small-medium Insurance and Financial Services clients (100 – 1000 knowledge workers). The focus then shifted to industries with a need for heavy compliance. For example, PCI-DSS applied to Retail/Restaurant, HIPPA applied to Health Care Services (Hospital/Senior Living) and NIST 800-53 applied to SLED – Universities, Large K-12, Cities and Counties, especially those with responsibilities in Power/ Waste/ Critical infrastructure.

Finally, it made sense to revisit clients who were lagging in their adoption of aiXDR.

How are the customers (sectors) benefiting from Seceon aiXDR?

1. Seceon aiXDR offered a credible chance for cybersecurity tool consolidation through the composite features covering SIEM, SOAR, UEBA, NBAD, IDS/IPS, EDR, Threat Intelligence and Vulnerability Scan. In addition to reduced Capex and Opex, Technical Debt was considerably lowered.
2. Faced with overtaxed staffing, Seceon aiXDR's automated threat detection and remediation allowed for ample free time that was utilized to accomplish a few goals, acquire skills that were lacking and refocus staff on core IT functions (digital transformation).
3. By virtue of the elevated security posture operationalized by Seceon aiXDR, it has been easier to meet industry compliance requirements:
   a) Technical audience – completeness of the tool for ease of use and power of the integrated AI based solution
   b) Business audience – ROI derived from a single solution tracking compliance in various forms (NIST, GDPR, PCI, HIPAA)

while offering protection against Ransomware, Brute-Force, Trojan/ Worms, DDoS and many other attacks with direct consequences to reputation or IP.

What are some of the key features/functions enabling customers to derive considerable value?

While there are many tools and platforms that offer security monitoring and flag suspicious activities, a comprehensive set of analysis and evidence (threat indicators) tied to a threat model (Brute Force, Ransomware, Volumetric DDoS etc) is absent. Seceon aiXDR, however, offers a different experience by leveraging Dynamic Threat Models that bring a purpose to individual pieces of evidence (threat indicators).

1. Visualization and Reporting: Summarized information and visualization (graphical) with user and asset centric views, makes it both powerful, yet easy for the Security Analyst, IT Security Director and CISO to grasp the nature (type of attack), extent (users and assets impacted) and level (severity/impact). Also, reports are generated continuously so that customers can stay compliant with regulatory requirements 24x7 and assess their security posture.
2. Network Policies: From IT Governance standpoint, Seceon offers the ability to apply network segmentation and segregation through inclusive and exclusive rules that enable implementation of policies associated with Zero-Trust. Customers have found the Policy Violation Alerts to be very effective in preserving compliance while improving security posture.
3. Custom Alerts: Any event of interest can be defined through a customized alerting feature with wizard-based navigation called "User Defined Alerts". These alerts can be flagged for notification to the SOC Analyst. In particular, customers find UDAs to be very effective in tracking and alerting unauthorized user access to critical assets (databases and business apps), operations on a database, changes to an AD user account and even simple notifications related to emails blocked by firewall policies.

How does Seceon's solution reduce Capital Expenses and/or improve Operating Margins?

❑ Seceon's aiXDR has considerably reduced cost (70–80%) with comprehensive capabilities covering SIEM, UEBA, SOAR, Network Behavioral Detection, IDS/IPS, EDR, Threat Intelligence and Vulnerability Scan. There is no need to incur expense on separate tools/platforms with additive costs, overlapping features and integration challenges.

❑ With automation (AI and ML), built-in correlation, analytics and dynamic threat models at the helm of Seceon aiXDR, SOC Analysts can address alerts and incidents with considerable ease, freeing up 80% time per customer compared with other SIEM/XDR solutions. This makes for a compelling reduction in MSSP's Operating Cost.

❑ Seceon's aiMSSP platform design remarkably facilitates growth and scale. In addition to multi-tenancy with unlimited tenants at scale, the platform boosts improvement in Operating Margin through Multi-Tier Multi-Tenancy (MtMt) feature, allowing easy transformation of the MSSP into Master MSSP with growth aspirations.

Managed Security Service Provider can be onboarded on Seceon aiMSSP in less than an hour and tenants (customers) can be created in minutes. Information of security relevance from customer environment (On-Prem and Cloud assets) can be aggregated, analyzed and correlated within minutes of deployment, such that onboarding, threat detection and remediation for a new customer can be initiated within a day.