

VENDOR SNAPSHOT

PRODUCTS AND SERVICES

- Seceon aiSIEM™ system detects threats in real time by continuously analyzing metadata from raw streaming data & flows from network elements, applications and end points. It then applies three approaches: dynamic threat models, machine learning and AI deep learning techniques.
- Also packages its system as a multi-tiered and multitenant “SOC-in-a-box” solution, aiMSSP™ to support managed security services provided by SI and CSP partners for the SME and SMB markets.
- System can provide value within a few hours with its predefined “common sense” rules, then extends its reach and depth of detection with machine learning.
- Administrators can set policies for auto setting of remediation policies for closed loop operations.

KEY STRATEGIES

- Provide subscription services for a multi-function software system for detecting, alerting & remediating known and day-zero security risks, with extensive compliance reporting. Its solution, plus a firewall and end-point monitoring provide a comprehensive security solution, obviating the need for tens or hundreds of specialized systems.
- Focus on being a technology provider, partnering with others who provide associated services.
- Use private, public & hybrid cloud infrastructure to provide a high-performance, extremely scalable system that can be demonstrated in an hour, implemented in a few days and fully trained in a few weeks.

4/14/2020

© Copyright 2019 ACG Research

Key Customers

- Enterprise: RFA, SUNY.
- CSP: Charter Comm, Comcast

Founded
2014

Seceon provides security software to detect and defeat cyber attacks using predictive behavioral analytics, monitoring metadata from data flows.

Ecosystem

- MSSPs: ADT, Charter, Comcast, LAC, NTT Com
- Cloud Svcs: AWS, Azure, Google Cloud

Waltham, MA



and Japan

ANALYSIS

- The 3 views of the real-time data flows (dynamic threat model, machine learning, & AI engine) and comprehensive analysis of network, application, & endpoint metadata to identify threats is very innovative and differentiates this solution in the marketplace.
- The simple pricing model of endpoints/devices, rather than data volumes, scales well, but provides an easy to understand model for customers.
- The multi-function approach is well-suited to small to medium organizations without specialists in the various security sub-specialties.