seceon

RFA Case Study

A Global Technology Provider for 600+ Clients, with $900+ Billion AUM, Increases Efficiency of Personnel and SOC team by 77% with Seceon.

As security breaches and hacks continue to lead global headlines, effective cybersecurity protections are the "new normal" for conducting business today. In addition to recently enacted regulations, with more coming in near future, it is imperative for MSPs to provide the best security solutions to its customers. Traditional solutions are no longer sufficient; tools must evolve to combat the increasing sophistication of cybercriminal techniques and technologies. Customized malware exists now that can evade and bypass many of the traditional endpoint security solutions. Traditional signature- and manual calculation-based approaches are simply not sufficient for providing security with the increasing sophistication of cyber threats. Above all, the biggest challenge was integration as these point solutions are from different manufacturers and not built to communicate with each other inherently.

Seceon OTM Platform turned out to be the one they desired and the ease of integration was superior. The platform provides a comprehensive security solution to analyze all network traffic, utilizes machine learning (ML), artificial intelligence (AI) and anomaly detection algorithm capable of processing traffic behavior and correlates events in network without a need to establish rules

One of the differentiators for Seceon is the ability for immediate remediation. Seceon OTM has the ability to contain and eliminate threats in real-time – which is equally important to compromise detection – not just detecting it but also stopping it! The majority of current security solutions provided by major market leaders can detect but not immediately remediate. An aspect of the platform that RFA relies on the most is Seceon's ability to bring together variety of seemingly unrelated threat indicators to identify potential issues due to the ease of integration. "Seceon's machine learning capability has been key to reducing noise and ensuring that critical alerts get the attention they require," said Mark Alayev, Director of Service Delivery at RFA. Another advantage of Seceon OTM is the ease of set-up. RFA was able to fully set-up and start collection data in less than a day! The major use-cases to be addressed were:

- Ability to detect reconnaissance
- Ability to detect data exfiltration
- Ability to detect various external and internal threats.

Prior to Seceon OTM, RFA used a number of traditional solutions and services from large market leaders but it was always challenging to find a solution that could detect/cover between perimeter and endpoints to the required level of sophistication. The multi-layered approaches recommended by industry experts were rendered ineffective without proper integration between security solutions.

"We have built-in security and compliance features for our cloud platform, but we need to ensure we defend our sensitive information as well as our clients," said Grigoriy Milis, Chief Technology Officer at RFA. The company was on the hunt for next-gen security solutions with a key focus on cloud security. They evaluated a number of security solutions in the market to provide their clients with the best possible selection and protection. A core requirement for RFA was a solution that delivered perimeter-to-endpoints to network security. He continued, "despite evaluating a number of security solutions, including SIEM solutions and behavioral analysis solutions, we could not find ones that can be brought together under one umbrella."

"When we did a side-by-side comparison between Seceon OTM and some of the other solutions from larger providers, Seceon was able to detect real-life security threats that the other platforms did not detect."

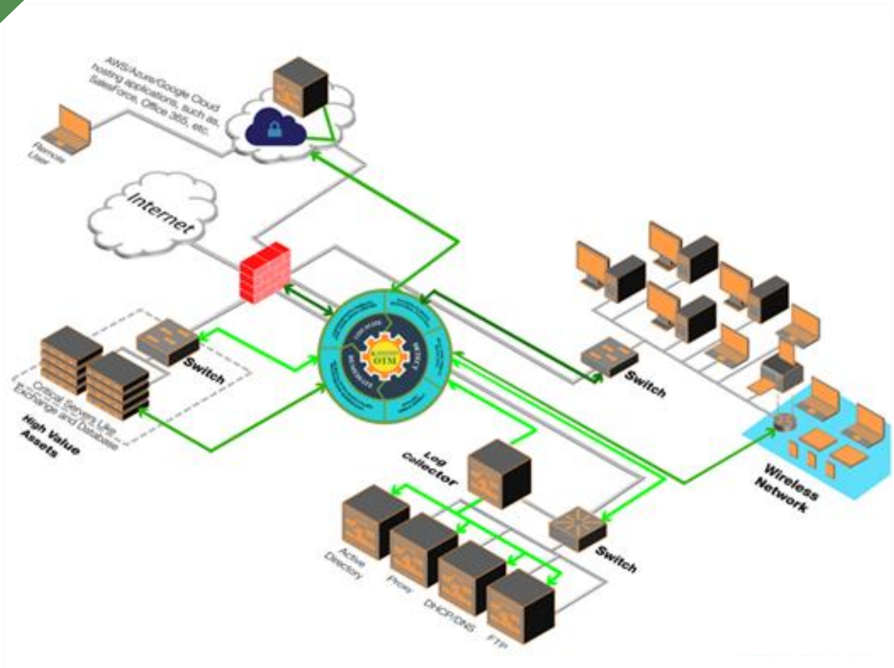
- Grigoriy Milis
CTO at RFA

Challenges:

- Traditional solutions and services from large vendors could neither combat the increasing sophistication of cyber threats nor could detect between perimeter and endpoints to the required level.

- The level of protection afforded by signature- and manual calculation-based approaches are simply not sufficient compared to the overhead costs.

- Integration is the biggest challenge as point solutions from different manufacturers are not built to communicate with each other inherently.


AWS/Azure/Google Cloud hosting applications, such as, SalesForce, Office 365, etc.
Remote User
Internet
OTM
Switch
Critical Servers Like Exchange and Database
High Value Assets
Switch
Log Collector
Active Directory
Proxy
DHCP/DNS
FTP
Switch
Wireless Network

Also, the level of protection afforded resulted in dissatisfaction when compared to the overhead cost. RFA formed an R&D group led by their CTO in order to evaluate security solutions on a variety of factors, such as, economics, multi-tenant capability, scalability, quality of detection, automated remediation, rate of false positives, and integration with various contextual data sources, and make the final selection.

> *"Seceon's machine learning capability has been key to reducing noise and ensuring that critical alerts get the attention they require."*
>
> *- Mark Alayev*
> *Director of Service Delivery*

Solution:

- Analyzes all network traffic, utilizes ML, AI and anomaly detection algorithm capable of processing traffic behavior and correlates various events in network without needing to establish rules

- Detects reconnaissance, data exfiltration, and various external and internal threats

- Provides SIEM functionality and behavioral analysis under one umbrella on a single platform

Benefits:

- Increases efficiency of personnel and SOC team by 77%

- Ease of set-up and integration is superior as it brings together variety of seemingly unrelated threat indicators to identify potential issues

- Ability to remediate (contain and eliminate) threats in real-time

The OTM Platform is very easy to set-up, and with complete set-up taking only one day, their SOC team was able to see meaningful information coming from their systems within the first week. This resulted in an immediate benefit of considerable improvement in their security posture by detecting what others may miss as now they had the ability to analyze substantially higher number of sources, events, and data. They were currently processing over more than Billions events/day with an extremely low rate of false positives. The OTM Platform enabled them to increase efficiency of personnel and SOC by 77%. According to Grigoriy, "When we did a side-by-side comparison between Seceon OTM and some of the other solutions from larger providers, Seceon was able to detect real-life security threats that the other platforms did not detect." The improvement in security posture, the ease of installation and integration, and the ability for immediate remediation have greatly improved their competitive advantage as an MSP and allows them to be able to offer innovative technology to their clients at much lower costs than their competitors.

About RFA:

Richard Fleischman & Associates is the trusted technology partner to over 600 clients globally, with more than $900 Billion in total assets under management, for nearly thirty years. Offering a full range of technology solutions with global data center operations and industry-leading service, RFA serves the IT and Technology needs across the Financial industry. It delivers scalable, reliable and secure enterprise-grade technology infrastructure. RFA is headquartered in New York City with operations in New York, Connecticut, New Jersey, Massachusetts, California, with EMEA operations headquartered in London.