Ovum
TMT intelligence | informa

On the Radar: Seceon provides advanced threat detection services

Analytics, machine learning, and adaptive detection algorithms are used to identify cyber-threats

Publication Date: 13 Apr 2016 | Product code: IT0022-000673

Andrew Kellett

Summary

Catalyst

Seceon helps its enterprise clients identify and stop known and unknown (zero-day) threats when they happen. Its Open Threat Management (OTM) platform uses a combination of advanced analytics, machine learning, and adaptive detection algorithms to block and eliminate cyber-threats and defend organizations against malicious attackers.

Key messages

- The Seceon OTM platform makes use of predictive analytics to detect threats that range from traditional off-the-shelf cyber threats to the latest generation of APTs.
- Behavioral analysis techniques are used to highlight insider threats as well as threats from external users.
- Seceon combines the use of data collection and analysis techniques, machine learning, and behavioral analytics to identify and block an ever-growing range of cyber threats.
- Seceon will need to highlight its fast-to-market, out-of-the-box detection, and alert prioritization capabilities to make it stand out from the crowd.

Ovum view

Too many organizations continue to be breached by security threats that should be detected. Once a break-in has taken place, detection and remediation times at an average of around 200 days remain far too high. More effort is needed to improve threat identification rates and remediation timelines. Two issues are important in achieving these objectives: the ability to deal with a higher percentage of cyber-attacks as they occur, and the contextual knowledge to prioritize workloads to deal with the threats that are likely to cause the most damage to a business and its customers.

Recommendations for enterprises

Why put the Seceon Open Threat Management platform on your radar?

Security vendors and service providers that can make significant improvements to cyber-threat detection rates and reduce the time taken to find and fix security breaches have an important role to play. Seceon's approach to these issues is driven by its combined use of analytics, machine learning, and adaptive detection algorithms to identify and block cyber-attacks, improve detection rates, and prioritize remediation activity.

Highlights

The Seceon OTM platform uses data collection and analysis, machine learning, and behavioral analytics to identify, block, and report on cyber threats. Its threat visualization capabilities are intended

to help security managers see all threats, drill down into the details, and take corrective action. The goals are to prioritize and deal with the threats that matter and need immediate attention, and find all compromised users, devices, and systems, then deal with the containment issues by addressing the business impact.

Functionally, the OTM platform comprises two major components:the Seceon Control and Collection Engine (CCE) and the Seceon Analytics and Policy Engine (APE).

The Seceon Control and Collection Engine (CCE) gathers threat information from all available network and business sources. This includes metadata from the corporate network, and log and traffic flow information coming from devices, applications, processes, and systems. Relevant security event information is automatically passed to the Seceon Analytics and Policy Engine.

The Seceon Analytics and Policy Engine (APE) provides the platform's central processing power. CCE information is used to generate a range of analytical files that are used to predict and detect threat activity. It also provides information about how users, devices, and applications interact, and makes this information available when the customer is setting acceptable usage policies. From this, threat and policy violations can be highlighted and reported. APE reporting facilities are also responsible for providing prioritized threat alerts and remediation recommendations for security managers.

The automated components of the OTM platform make use of machine learning and algorithmic processes to deliver its predictive security/threat analytics. Information on everything from basic to advanced persistent threats (APTs) is analyzed and maintained. There is also a strong focus on usage issues surrounding both insider threats and external behavior patterns. This includes identifying compromised credentials and associated security threats before they can cause damage.

The OTM's policy management features provide an overview of how users, devices, applications, and systems interact. They are supported by policy enforcement tools that are used to block unwanted connectivity to specific external geographies, domains, sites, or URLs, and whitelisting facilities that control connectivity between individuals as well as internal and external groups.

The OTM platform incorporates a fast and easy to deploy risk mitigation approach. Deployment is said to be achievable in an hour, with initial out-of-the-box threat detection starting immediately. The platform is available for use by organizations of all sizes, and can be deployed as a standalone solution or as part of a larger integrated enterprise security strategy.

Background

Seceon was founded in 2014 by an experienced team of business leaders and software developers, senior managers, and technologists with particular strengths in application development and big data systems. The Westford, Massachusetts-based company is a self-funded start-up and has been in revenue since December 2015.

The senior management team comprises its founder and CEO Chandra Pandey, an expert in data center and scalable network solutions, and a former general manager and VP of platform solutions at BTI Systems. The other co-founders are Naveen Rohatgi, the company's engineering lead and chief architect with over 20 years industry experience who has also held similar engineering positions at BTI Systems; CSO, Gary Southwell, who has over 25 years of strategic business and product planning experience and was BTI Systems CTO; Sunil Kotagiri, who leads the architecture, development of the company's big data security platform, and with over 20 years of experience in

software development was previously VP of software engineering at IneoQuest; and Smit Kadakia, who leads Seceon's data science and machine learning team, and before joining Seceon held a senior executive position at Tradepoint Systems.

Current position

Seceon is still a relatively new entrant to the security protection market. Initial interest in its threat surfacing, prioritization, and remediation platform has come mainly from medium-to-large enterprise organizations in North America. Future growth is targeted at the global market, where there is already growing interest. This can be partly attributed to the company's per user/device pricing strategy, which helps to keep the product set within the reach and expectations of medium-sized organizations and is also seen as attractive to larger enterprises, and partly attributed to its fast-to-deploy and out-of-the box usage opportunity.

Data sheet

Key facts

Table 1: Data sheet: Seceon, Inc.

Product name	Seceon Open Threat Management platform	**Product classification**	Cyber threat management
Version number	2.3	**Release date**	December 2015
Industries covered	All	**Geographies covered**	Worldwide
Relevant company sizes	Companies with between 1,000 and 5,000 users	**Licensing options**	Subscription, term, and SaaS on a per device and month basis
URL	www.seceon.com	**Routes to market**	Direct and through channel partners and OEMs
Company headquarters	Westford, MA, US	**Number of employees**	50

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

On the Radar: Observable Networks offers an analytical approach to threat detection, IT0022-000592 (January 2016)

"Microsoft Windows Defender begins to address advanced threat protection requirements", IT0022-000650 (March 2016)

Author

Andrew Kellett, Principal Analyst, Infrastructure Solutions

Andrew.kellett@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum

TMT intelligence | informa

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo