Insight

SECDO Private Vendor Watchlist Profile: Preemptive Forensics to Reduce Incident Response Time

Dan Yachin Petra Kacer

IDC OPINION

Dealing with the vast amount of alerts, events, and logs generated by security information and event management (SIEM) and other security systems is one of the biggest challenges faced by cybersecurity teams. While this raw data contains valuable information, the sheer volume makes it practically impossible to effectively investigate each and every alert. As a result, obtaining the forensic evidence is becoming a complex, time-consuming, and error-prone task that requires the involvement of highly skilled security analysts.

Founded by a team of experienced security analysts and incident responders, SECDO aims to tackle this problem by continuously collecting and analyzing all host (endpoints and servers) events and storing them for forensics and later analysis. The recorded data is correlated to create event chains that describe the forensic history of alerts back to their root causes, enabling security analysts prioritize alerts and investigate and respond to incidents in a more accurate and timely manner.

We believe SECDO is a company to watch because:

- SECDO's solution improves the efficiency of incident response by automating key stages of the threat analysis process and reducing false positives.
- SECDO provides remote visibility into hosts down to the thread level, enabling security and IT teams to query in natural language to address a broad range of issues.
- SECDO focuses on managed security service providers (MSSPs) as one of its main target audiences, enabling them to offer high-value services such as host visibility, advanced threat protection, incident response, and forensics.

January 2017, IDC #US42245517

IN THIS INSIGHT

Overall Score: 16/20

16

This IDC Insight analyzes SECDO, a company playing in the forensics and incident investigation segment of the security management market, and reviews key success factors: market potential, products and services, competitive edge, customers, and corporate strategy. Detailed subquestions make up each of the five success factors, which are assigned a value from 1 (weak) to 4 (strong). Leveraging IDC's expert understanding of the competitive landscape and future outlook, this document provides insight into private companies based on IDC's unique watch score system:

- **Market potential:** Market growth potential, strength of competition, and current stage of market (early adopters versus late majority)
- **Products and services:** Level of differentiation, disruptive capability, and scalability
- **Competitive edge:** Competitive landscape and peer assessment
- **Customers:** Number of existing customers, quality of existing customer base, geographic reach, and size of addressable market in the coming years, given the vendor's current capabilities
- **Corporate strategy:** Go-to-market strategy, management pedigree, and financial status (running on venture capital with insignificant revenue versus self-sustaining and not seeking additional rounds of funding)

SITUATION OVERVIEW

I. Market Potential

Score: 3/4

3

Market

SECDO plays in the forensics and incident investigation (FII) segment of the security and vulnerability management (SVM) market, which encompasses two separate but symbiotic markets — security management and vulnerability assessment. These two markets can stand alone, but they have considerable overlap. FII solutions are part of the security management market. They provide organizations with the ability to create security policy that drives other security initiatives, allow for measurement and reporting of the security posture and, ultimately, provide methods of correcting security shortcomings.

FII solutions capture and store real-time network and device data and identify how business assets are affected by network exploits, internal data theft, and security or HR policy violations. Products in this category also include those that can do historical recreations to find how an event occurred. The submarket also includes malware forensics tools used by researchers to deconstruct targeted and stealthy malware. Finally, this category includes products that can be used by law enforcement to gather evidence associated with criminal activity.

According to *Worldwide Security and Vulnerability Management Forecast, 2016-2020: Enterprises Continue Focus on Security Operations* (IDC #US41943616, December 2016), security information and event management is the biggest segment of the security management market and is expected to grow from $1.9 billion in 2015 to $2.8 billion in 2020 at a CAGR of 8.4%. The FII segment is projected to grow at a CAGR of 11.8%, reaching $786.4 million in 2020. IDC continues to see an increase in the need for enterprises to have forensic capabilities, driving spending on both SIEM and FII solutions. The FII segment is also expected to continue to gain traction as enterprises are being held more accountable for not just reporting a response but also disclosing specifics around exactly what data was compromised in a breach.

SECDO plans to capitalize on the FII market opportunity by focusing on managed security service providers. According to IDC's research, as in-house security solutions are expensive and challenging to maintain in the face of a rapidly evolving threat landscape and formidable adversaries, enterprises increasingly are considering MSSPs. As a result, MSSPs are required to collect and analyze ever-growing amounts of security data and still enable their customers to act upon threats in a timely manner to prevent escalation. Furthermore, in light of the growing competition, MSSPs are increasingly challenged with differentiating their offerings. SECDO looks to tap into this opportunity by enabling MSSPs to offer high-value services such as advanced threat protection, incident response, and forensics. SECDO also sells directly to enterprises, including large organizations with security operation centers (SOCs) or internal teams of security analysts.

II. Products and Services

Score: 4/4

4

SECDO Incident Response Platform

SECDO's Incident Response Platform automates the processes of validating and investigating security alerts. The company's solution continuously records all events and activities from all endpoints and servers, down to the thread level, and stores it on a centralized server (in the cloud or on-premise). Utilizing proprietary algorithms, event chains are automatically created to provide a contextual view for each alert. The data is then correlated with alerts from SIEM and other third-party detection systems to build the forensic profile of an attack. As most of the data is continuously collected and preprocessed, investigation time is significantly reduced. SECDO also provides visual interface and query tools to facilitate the threat validation and investigation process and shorten incident response time.

Once a threat is detected, SECDO's Incident Response Platform enables security and IT teams to take actions such as freezing a process in memory or isolating an affected machine from the network while keeping it available for remote remediation. IT personnel can also run commands and code interactively (using Python, Power Shell, etc.) on any host and build complex response scripts or scenarios without the need to install Python on the endpoint. Furthermore, by providing continuous visibility into corporate endpoints, SECDO's Incident Response Platform can be used to monitor the IT environment and conduct investigations that are relevant to IT support.

III. Competitive Edge

Score: 3/4

3

Competitive Landscape

SECDO competes with other emerging FII companies such as CyberSponse, Demisto, Hexadite, and Syncurity, which are also focused on automating incident response processes. Among the major security management vendors, RSA, IBM (Resilient Systems), HPE, Symantec, Splunk, and others are working to incorporate more security analytics into their forensics and SIEM offerings to improve their incident response capabilities.

In addition, SECDO can be considered as competing to some extent in the endpoint segment of the specialized threat analysis and protection (STAP) market, which consists of solutions that put behavioral detection methods above signature-based approaches. The endpoint STAP segment is led by FireEye, followed by Cylance, CrowdStrike, Carbon Black, and Palo Alto Networks. Other players in this space include well-funded VC-backed companies such as Bromium, Cylance, Invincea, CounterTack, and SentinelOne. Among the endpoint STAP vendors, SECDO competes most closely with Carbon Black (and specifically, the company's Cb Response solution), which is similarly offering incident response capabilities empowered by advanced analytics. Following the acquisition of Confer Technologies in July 2016 (for $100 million), Carbon Black now also has a strong MSSP offering that supports multitenancy.

Partners

SECDO is targeting VARs and MSSPs in the United States, India, Europe, and Israel. The company focuses on both a channel-based sales strategy and direct sales to large enterprises.

IV. Customers

Score: 3/4

3

- **Key vertical markets and company sizes:** Security service providers, enterprises with a mature SOC or incident response operations in industries including finance, insurance, telecommunications, and retail (SECDO already serves dozens of customers worldwide and has established sales operations in the United States and Israel, as well as signed partnership agreements with established MSSPs in the United States.)
- **Geographic reach (currently and planned):** Worldwide

V. Corporate Strategy

Score: 3/4

3

Leadership

Shai Morag, SECDO's CEO and cofounder, was previously the founder and CEO of Integrity Project, a software company that is specialized in connectivity, low-level development, real-time applications and security, which was acquired by Mellanox in 2014. Prior to that, he served for 10 years as an officer in the IDF Intelligence Corps' Unit 8200.

Gil Barak, SECDO's CTO and cofounder, was previously a software architect at Apple and served as a private security consultant for Texas Instruments, Elbit Systems, and Israel's Ministry of Defense. Prior to that, Barak served for five years in the IDF Intelligence Corps' Unit 8200.

Key Acquisitions

SECDO has not made any acquisitions.

Current Investors

SECDO raised more than $11 million in two funding rounds to support the development of its product to enterprises, MSSPs, and other security service providers.

Company Overview

TABLE 1

SECDO Company Snapshot

Category	Details
Functional and secondary markets	Security vulnerability and management; forensics and incident investigation
Founding year	2014
Number of employees	45
Number of customers	25
Company location	New York City, New York; Ra'anana, Israel
Website	**www.sec.do**
Revenue estimate	$1 million to $10 million

Source: IDC, 2017

TABLE 2

SECDO Funding History

Round	Date	Amount	Investors
Seed	2014	$3 million	Angel investors and industry veterans including Marius Nacht (chairman of Check Point Software), Ariel Maislos, Ofir Shalvi, and Ehud Weinstein
A	2016	$8 million	Seed investors and Rafael Development Corporation (RDC)

Source: IDC, 2017

TABLE 3

SECDO Peers

Company Name	Revenue Estimate	Investors
Carbon Black	$43.0 million (STAP revenue, 2015)	Sequoia Capital, Paramount Pictures, Kleiner Perkins Caufield & Byers, Highland Capital Partners, Blackstone, Evolution Equity Partners, Founders Circle Capital, .406 Ventures, and Atlas Venture
Cylance	$58.5 million (STAP revenue, 2015)	Blackstone, Capital One Growth Ventures, Dell Ventures, DFJ Growth, Draper Nexus Ventures, Khosla Ventures, Fairhaven Capital, Insight Venture Partners, KKR & Co., TenEleven Ventures, Thomvest Ventures, and private investors
Hexadite	NA	Hewlett Packard Ventures, TenEleven Ventures, YL Ventures, and private investors

Source: IDC, 2017

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com