IDC Innovators

IDC Innovators: Artificial Intelligence–Infused Security Solutions, 2018

Cathy Huang Rijo George Thomas Christina Richmond

IDC INNOVATORS IN AI-INFUSED SECURITY

With the proliferation of digital technologies, enterprises are striving to stay ahead of the increasing number and complexity of threats across multiple vectors. To safeguard against critical breaches, it is pivotal that enterprises identify and respond to cyberattacks in real time. The influx of artificial intelligence (AI) and deep learning technologies is changing the dynamics of how enterprises respond to threats and helping them stay ahead of the threats for once. These new "intelligent" security solutions from vendors and providers are not just improving the effectiveness of enterprises' cyberdefense controls but also transforming the entire cyberdefense life cycle for business customers by shifting the value propositions and metrics of their security programs. This IDC Innovators study profiles three start-up vendors in the AI-infused security solution market for business customers to consider Cybereason, Deep Instinct, and Vectra AI (see Figures 1–4).

FIGURE 1

IDC Innovators in AI-Infused Security, 2018

IDC Innovators are emerging vendors with annual revenue <US$100 million that have an innovative new technology or a groundbreaking business model.

AI-Infused Security Solution, 2018

Company Name:	Founded:	Headquarters:
Cybereason	2012	Boston, Massachusetts
Deep Instinct	2014	New York City, New York
Vectra AI	2010	San Jose, California

Source: IDC, 2018

October 2018, IDC #AP42610618

FIGURE 2

Cybereason

Why Cybereason Was Chosen as an IDC Innovator

Cybereason is an endpoint detection and response technology as well as managed detection and response provider which promises to provide deep visibility into endpoint, behavioral, and system data across the entire enterprise. Its current customer base spans across financial services, manufacturing, healthcare, professional services, and so forth.

Company Name		
Founded 2012	**Number of Employees** 350-500	**Headquarters** Boston, Massachusetts
Product Name Deep detect and respond	**Founders** Yonatan Amit, Yossi Naar, Lior Div	
Profiled Product/Service Deep detect and respond Deep prevent Deep investigate	**Funding** Total funding amount estimated - US$188 million, total of four rounds of funding. Series D (2017) - US$100 million	

IDC Innovator Assessment

- Cybereason specializes in endpoint detection and response to security breaches, with a proprietary AI platform, a multilayered defense platform that does behavioral analytics and analysis on all digital action and interaction happening enterprisewide via the endpoint.
- Cybereason's AI-based solution requires minimal training and can identify potential threats immediately upon deployment. Its Malop feature can reveal malicious activity, including contextual awareness of threats, leading to insights into impacts to endpoints and the enterprise, including root cause analysis.
- Cybereason has categorically separated the different elements of its detection, response, and forensic capabilities into products called deep detect and response, deep prevent, and deep investigate.

Key Differentiator

Cybereason's custom-built in-memory graph is the heart of its malicious behavior identification and hunting engine. Apart from detection, Cybereason also provides forensics, which is enabled by the pre-categorization of raw data that has been flagged as suspicious; this helps the analysts immediately dive into the data and make actionable use. The solution is not kernel-based, extremely lightweight for an endpoint.

Challenges

Cybereason needs to improve its capabilities around monitoring cloud events. Additionally, automated risk prioritization is an essential component of AI bases threat platforms. Cybereason needs to effectively elevate the use of automation in its risk prioritization capabilities to reduce the dependence of analysts.

Source: IDC, 2018

FIGURE 3

Deep Instinct

Why Deep Instinct Was Chosen as an IDC Innovator

Deep Instinct is one of the pioneers in applying deep learning technology (e.g., behavioral analysis plus unsupervised algorithms) to safeguard mainly enterprises against cyberthreats across multiple vectors. The vendor emphasizes its unique focus on deep learning techniques, which its neural network is trained on 100% raw data.

Company Name		
Founded 2014	**Number of Employees** 100	**Headquarters** New York City, New York
Product Name Deep Instinct Omni-Cybersecurity	**Founders** Eli David, Guy Caspi, Nadav Maman	
Profiled Product/Service Deep Instinct for Endpoint/Servers Deep Instinct for Mobile Devices (Android and iOS)	**Funding** Total funding amount: Estimated Series B - US$37 million in total, with estimated two rounds of funding.	

IDC Innovator Assessment

- Deep Instinct solutions work in complement with all the leading antivirus solutions and offer a lightweight agent which requires low memory and CPU usage that can be easily deployed (i.e., runs on any CPU).
- Deep Instinct solution is able to use a correlated risk model to offer contextualization and predict if it's a threat (e.g., malware, fileless attack) by scanning raw data and traffic across the enterprise environment. If it's a threat, the solution can initiate automated remediation, such as quarantine the files, sandboxing, file delete, and so forth.
- Deep Instinct also offers automated analysis and malware classification without any human expert involvement.

Key Differentiator

Deep Instinct emphasizes its unique focus on deep learning techniques which the algorithm is trained on 100% raw data (i.e., not human-curated data). The data set which its neural network is trained on consists of almost 1 billion files from different public sources, including dark/deep web, open source data, and also "homegrown" malware and mutated malware. This training process is unique and based on its proprietary deep learning algorithms, which can protect a wide range of devices, platforms, files, and different scenarios like online or offline against cyberthreats.

Challenges

The solution does not seem to mention a capability for encrypted traffic. The vendor claimed to offer the lowest false-positive rates and highest detection accuracy rates in the industry. The claimed accuracy level will be better positioned if it is based on third-party verified results.

Source: IDC, 2018

FIGURE 4

Vectra AI

Why Vectra AI Was Chosen as an IDC Innovator

Vectra AI is a cyberattack detection and threat hunting solutions provider based in San Jose, California, United States. It leverages AI to detect attackers in real time and enrich threat investigations in the event of a breach. The solution from Vectra is currently deployed across organizations in retail, education, and healthcare in the United States and Europe.

Company Name		
Founded 2010	**Number of Employees** 100-250	**Headquarters** San Jose, California
Product Name Vectra Cognito platform	**Founders** James Harlacher, Mark Abene	
Profiled Product/Service Cognito platform - AI-infused cyberattack detection and threat hunting solutions The Cognito platform consists of Cognito Detect and Cognito Recall.	**Funding** Total funding amount estimated - US$122.5 million Series D (2018) - US$36 million Series C (2015) - US$35 million	

IDC Innovator Assessment

- Vectra AI spearheads its detection and hunting solutions with its AI-powered flagship product called the Cognito platform. The platform promises real-time detection and response capabilities to neutralize enterprise cyberthreats across network and endpoints.
- The automated and self-learning algorithms powering the Cognito platform require minimal human intervention to effectively identify hidden attackers within the enterprise ecosystem. At the core of the Vectra Cognito platform are a set of behavioral detection algorithms that can detect from the metadata captured from the enterprise network traffic, end users, cloud events, and endpoints.
- Additionally, the Cognito platform can automatically score every detection and host in terms of the threat severity and certainty using the Cognito Threat Certainty Index.

Key Differentiator

Vectra puts a special emphasis on the integration of its AI-powered security capabilities into other parts of the enterprise security defenses, which include security in virtualized environment, EDR, SIEM, firewalls, and so forth, to provide automated detection and containment of threats. The vendor is focused on core steps in the cyber kill chain with high accuracy of detection and ability to provide a high-fidelity signal.

Challenges

Vectra needs to elaborate on the training and updates its behavioral algorithms get. Timely updates are a key component in ensuring the algorithm is able to decrease false positives and increase its accuracy when it comes to threat and malware detection.

Source: IDC, 2018

TECHNOLOGY DEFINITION

This IDC Innovators study examines three start-up vendors that provide AI-infused security products or services, or both. The AI-infused security solution is defined as a core security solution that primarily leverages on artificial intelligence technologies, including deep learning, machine learning, knowledge graphs, and so forth, to quickly detect, prevent, and respond to cyberthreats.

IDC INNOVATORS INCLUSION CRITERIA

An "IDC Innovators" document recognizes emerging vendors chosen by an IDC analyst because they offer an innovative new technology or a groundbreaking business model, or both, and were approved by the IDC Innovators Review Panel. It is not an exhaustive evaluation of all companies in a segment or a comparative ranking of the companies.

An IDC Innovators document highlights vendors that meet the following criteria:

- In IDC's opinion, the company exhibits innovative technology or a new business model.
- The company has annual revenue under US$100 million at the time of selection.
- Customers are currently using the company's products and services (i.e., the products and services are not conceptual or in the process of being released).
- The product, service, or business model must solve or help alleviate an IT buyer challenge.

In addition, vendors in the process of being acquired by a larger company may be included, provided the acquisition is not finalized at the time of publication of the document. Vendors funded by venture capital firms may also be included even if the venture capital firm has a financial stake in the vendor's company.

LEARN MORE

Related Research

- *IDC FutureScape: Worldwide Security Product and Services 2019 Predictions* (forthcoming)
- *Market Analysis Perspective: Worldwide Cybersecurity AIRO, 2018 – Harden, Detect, Respond, and Repeat* (IDC #US44282118, September 2018)
- *IDC Survey Spotlight: Compliance Spending – How Much Is Too Much?* (IDC #AP42610118, September 2018)
- *IDC MarketScape: Asia/Pacific Threat Lifecycle Services 2018 Vendor Assessment* (IDC #AP43699718, July 2018)

SYNOPSIS

IDC Innovators are emerging vendors with revenue of <US$100 million that have demonstrated either a groundbreaking business model or an innovative new technology, or both. This IDC Innovators study profiles three emerging vendors in the artificial intelligence (AI)-infused security solution market for business organizations: Cybereason, Deep Instinct, and Vectra AI.

"Feeling the pinch to effectively combat the ever-increasing cyberattacks, organizations have turned to AI-infused security solutions that have changed the dynamics of how enterprises identify, prevent, and respond to threats, helping them improving the cyber resilience level and effectiveness of enterprises' entire cyberdefense life cycle by shifting the value propositions and metrics of their security programs," says Cathy Huang, program lead, IDC Asia/Pacific Security Services.

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.

IDC Asia/Pacific Headquarters (Singapore)

80 Anson Road, #38-00
Singapore 079907
65.6226.0330
Twitter: @IDC
idc-community.com
www.idc.com