Artificial Intelligence (AI)-based Security Industry Guide, 2019

The Need for AI-enhanced and Automated Security Solutions for Better Threat Prevention, Detection and Response

Cybersecurity Research and Practice Team at Frost & Sullivan

PA74-74

September 2019

FROST & SULLIVAN

Executive Summary

Return to contents

Key Findings

- Owing to the multifaceted benefits that Artificial intelligence (AI) and machine learning (ML) bring, they have been adopted across industries, chiefly, healthcare, education, information and communication technologies (ICT), logistics, maritime, aviation, aerospace and defense, entertainment, and gaming.
- Despite their many benefits, AI and ML in the cybersecurity space caused much damage; AI-engineered attacks have increased in number, scale, and frequency, in the last few years. Therefore, security professionals are now required to employ advances, smart, and automated technologies to combat automated attacks.
- AI and ML have been used in all stages of cybersecurity to enable a smarter, more proactive, and automated approach to cyber defense—right from threat prevention or threat protection; threat detection or threat hunting; or threat response to predictive security strategy.
- Security startup companies are the most proactive about employing AI-security technologies.
- Large, traditional security companies have also beefed up their cybersecurity strategies to keep up with the trend of integrating AI/ML into their existing security solutions. In a bid to strengthen portfolios and capabilities, traditional security companies are increasingly acquiring start-up companies.

Source: Frost & Sullivan

AI-based Security Solution Profiles

Return to contents

The Market Landscape

AI/ML has been increasingly developed by security companies to strengthen their competitiveness. Most of them are now in the midst of developing their own AI/ML algorithm for some or all of their product lines. For example, Cisco Systems is developing its AI/ML to empower its intent-based networking and datacenter security solutions. Fortinet has integrated AI/ML into its Fortiweb solution to fight against web-based application threats. Symantec has recently added AI/ML capabilities to enhance its endpoint security protection with its AI-powered Targeted Attack Analytics (TAA) for incident response.

While most of the security giants are just now embedding AI/ML into some certain security products, we have seen an increasing number of companies develop AI-/ML-driven security products that have gained greater traction in the market. There are hundreds of such companies with different capabilities and focus areas, from application-centric protection or AEDR, to security analytics platform. In this study, we profile those AI-/ML-driven and AI-/ML-centric cybersecurity companies.

Balbix®

CROWDSTRIKE

DARKTRACE

安恒信息
DAS-security 安全中国

eSENTIRE®

PALADION
BETTER SECURITY OUTCOMES

REAQTA

seceon

SHAPE
SECURITY

In the next update, we would like to include more companies that have AI/ML-driven products which have seen widespread adoption.

Source: Frost & Sullivan

Balbix

Country of Origin	Solution Name	Solution Type	Security Category	Commercial Form Factor
US	Balbix BreachControl™	Breach risk and cybersecurity posture management	Cybersecurity posture assessment and improvement	SaaS/Hybrid

Solution Overview

- Balbix BreachControl™ is a converged cybersecurity platform which uses deep learning and other advanced AI algorithms to continuously discover and analyze the enterprise attack surface and provide real-time visibility into cybersecurity posture and breach risk.
- The assessment is provided as risk heat maps and dashboards and enables enterprises to prioritize mitigation actions that are necessary to proactively avoid data breaches.
- To initiate the BreachControl™ platform, Balbix sensors and collectors must first be deployed on premises and in cloud, to automatically and continuously monitor the extended enterprise network.
- The collected internal security posture data together with external threat information from various sources is further processed by the Balbix Brain (SaaS hosted) which applies an ensemble of AI algorithms to evaluate cyber risk for each and every entity on the network and for the enterprise as a whole.

Key Features

- **Asset Discovery and Inventory:** The system helps with automatic discovery and monitoring of a full range of coverage of network assets, such as devices, applications and users, on premises, in the cloud, or mobile, including unmanaged assets and IoT.
- **Breach Risk Assessment:** The Balbix platform helps users visualize breach risk using real-time dashboards and understand the potential impact to business from different breach scenarios.
- **Prioritized Actions to Avoid Breaches:** The system prioritizes the necessary mitigatory actions that would fix the most urgent cybersecurity posture issues efficiently.

Source: Balbix; Frost & Sullivan

Balbix (continued)

Key Differentiators

- Balbix's sensors analyze a broad range of applications, devices, and users, both on-premises and in the cloud, to continuously monitor the extended enterprise network. This addresses challenges that arise from the proliferation of assets which increase the complexity and difficulty for security team to monitor and manage risk comprehensively.
- With a massive volume of monitored security posture data and the external threat intelligence data, the BreachControl™ Platform adopts 24 advanced AI algorithms to examine and address different aspects of breach risk. AI-enabled capability also prioritizes actionable mitigation plans for the security team.
- Apart from visualization of breach risk and potential business impact, based on the analyzed results, the platform also provides natural language processing (NLP) search. Users can easily search and explore potential security and risk issues through human-like conversation for example: "Which devices in the network are most vulnerable?".
- The platform is also capable of continuous verification of security compliance, such as PCI-DSS, HIPAA, GDPR, etc.
- Balbix integrates with other security tools to enable the implementation of enterprise security workflows to proactively fix cybersecurity posture issues.

Business Overview

- Founded in 2015, Balbix positions itself as an AI-powered cybersecurity posture transformation company. The company's founder and management team have deep entrepreneurship and technology backgrounds which earned Balbix great attention in the market.
- In 2018, the company completed a second round of funding led by Singtel Innov8, with investors, such as Mubadala Ventures, Mayfield, and John Chambers' (ex-Cisco CEO) JC2 Ventures.
- Balbix's customers include Global 2,000 companies based in the US, Canada, Europe, and Japan.

Source: Balbix; Frost & Sullivan

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Our customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for customers' internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

For information regarding permission, write to:

Frost & Sullivan

3211 Scott Blvd, Suite 203
Santa Clara, CA 95054