On the Radar: Cynet Autonomous Breach Protection automates core functionalities for breach protection

Continuous monitoring protects, streamlines, and detects threats, then speeds response

Publication Date: 19 Sep 2019 | Product code: INT005-000033

Rik Turner

Summary

Catalyst

Cynet offers a single platform that consolidates and automates the core functionalities required by organizations for timely breach protection.

Key messages

- Threats and breaches stretch most organizations' ability to respond.
- The proliferation of new security tools, which are often poorly integrated and operating in silos, to address this is not helping.
- Cynet monitors all endpoint, user, and network activity across the entire environment to prevent and detect all main commoditized and advanced attack vectors. It simplifies threat protection by integrating the capabilities of various products in a single platform.
- Cynet's value proposition applies to security-savvy organizations, seeking to simplify and optimize their security operations, and to resource-constrained organizations without an in-house security team or a multi-product security stack.

Ovum view

Too many products, too much complexity in their deployment, lack of integration, and a shortage of in-house skills and resources to fix the problem mean that most midsize organizations are struggling with a plethora of disjointed and complicated security tools that fail to deliver the protection expected. Cynet aims to address this challenge, and bears consideration, particularly from companies in its target segment of midsize enterprises and above.

Recommendations for enterprises

Why put Cynet 360 on your radar?

While no single solution can fix all cybersecurity requirements, most organizations do not have the resources to integrate or even effectively configure many of the tools available. Cynet 360 is an out-of-the-box platform with many of the breach protection capabilities an organization requires. It performs network discovery to streamline deployment and can begin delivering value within 24 hours, with a level of autonomous breach protection that can be set to fit with available human cybersecurity resources and SOC-as-a-service bundled into the price.

Highlights

While the number of products has grown to address different types of threat, there are diminishing returns. Additional cybersecurity all too often fails to provide additional protection, because disparate products are operating in their own silos, adding deployment and configuration complexity but leaving gaps and only partial threat coverage. Few organizations have the skills, or can put in place the necessary resources, for the manual integration required.

Cynet challenges the perception that cybersecurity needs to be complicated, by starting with the principal of maximum visibility and monitoring. From its inception, threat detection though monitoring multiple sources and activities in files, processes, memory, network, and user accounts has been vital for building a picture of the true context of actions to determine whether or not they are malicious.

The company’s Cynet 360 product aims to deliver a wide set of breach protection functionality in a single platform. At its heart is the company’s Sensor Fusion technology, which continuously aggregates and analyzes all endpoint, user, and network activity data across the protected environment to decipher the exact context of file executions, network traffic, and user behavior, and determine if and what risk it introduces.

Agents deployed on all endpoint devices (currently Windows, Linus, and Mac, physical and virtual) gather information on activities on files, processes, networks, and user accounts. Cynet says endpoints do more than protect themselves, and a local element of the Sensor Fusion engine (within the agent) determines the nature of context, which is then collated for total visibility by the Sensor Fusion engine in a server. With context intelligence, actions can be undertaken autonomously when malicious activities are detected, with response orchestrated through automated playbooks. The level of automation can be adjusted to allow for human intervention, which means customers can start at a low level and increase it as they grow more comfortable with the concept of automated response.

Cynet acknowledges that technology alone is not enough to provide full protection, and it therefore bundles SOC services operated 24/7 by CyOps, its team of dedicated threat analysts and security researchers, with its Cynet 360 offering. The CyOps team complements Cynet 360 by providing threat hunting, in-depth investigation, and attack reports.

Deployment can be initiated remotely and automatically, reaching up to 5,000 hosts in an hour, with automatic deployment on new hosts as they are detected. Monitoring is typically in place in around seven hours, with full prevention, detection, and response orchestration within 24 hours.

The fast deployment model is a particular benefit for incident response handling coupled with the CyOps SOC services. This is of value to two audiences. First are the incident response providers that use Cynet 360 for visibility into new environments and faster response using the vendor’s automated threat detection and remediation actions. Second are the managed service providers (MSPs) that do not have their own incident response service, but can offer it by deploying Cynet 360 and taking advantage of both the situational visibility and the SOC service without charge.

Background

Cynet was founded in 2015 by its president, Eyal Gruner. Gruner also co-founded cyber-consultancy BugSec, where he served as CEO, as well as founding and leading Versafe, an antifraud, anti-phishing, and anti-malware vendor acquired by F5 in 2013.

Cynet has raised its market profile in part through its cyber discoveries alongside BugSec. These include major flaws such as the “SNAP” smartphone vulnerability and the TCP handshake vulnerability in next-gen firewalls. BugSec provides offensive and defensive security consulting services, complementing Cynet’s emerging threat detection and response platform.

The company raised financing in February 2016 through a $7m investment from Lazarus, a US-based hedge fund. It raised a further $13m in Series B funding in June 2018, led by Norwest Venture Partners, serial cyber investor Shlomo Kramer, and returning investor Ibex Investors. Kramer is a network security expert and serial entrepreneur, having co-founded SD-WAN service provider Cato Networks, firewall heavyweight Check Point Software, and data and application security vendor Imperva. He is currently CEO of Cato.

Current position

Cynet numbers its customers in the few hundreds spread across multiple countries, with a particular concentration in Europe and North America. As for its target market, the company says its customers are varied in size and industry.

It is a challenge to define precisely the category in which Cynet 360 sits. It certainly builds on endpoint detection and response (EDR) technology but moves beyond it to analyze a wider range of data that may be relevant, so Ovum's xDR categorization may be a more appropriate term. Other industry vendors are also moving toward this approach, and xDR as a category is becoming a more established class of product in its own right.

Looking forward, Cynet plans to extend agents to mobile devices and in time to containers and serverless environments. Its agent footprint is already quite light at between 25kB and 50kB, with just 3% to 4% CPU cycle utilization, so this seems realistic at some point.

In the meantime, Cynet 360 co-exists comfortably alongside the deployment of other systems, and beyond its own agent-generated data, it can also ingest firewall proxy logs and Active Directory user data. For companies not currently using or having a security specialist to gain value from a security information and event management (SIEM) system, Cynet can act as a compensating control, aggregating the functionality a SIEM would deliver, but also orchestrating incident response.

It is therefore an example of how the security management market is in a state of flux, with some SIEMs adding functionality to remain relevant, while new players are entering the fray with platforms that can complement or supplant a SIEM.

Data sheet

Key facts

Table 1: Data sheet: Cynet

Product name	Cyner 360	**Product classification**	Breach protection platform
Version number	3.7	**Release date**	September 2019
Industries covered	All verticals, retail	**Geographies covered**	Europe, US
Relevant company sizes	Midsize to large enterprise	**Licensing options**	Per endpoint monitored
URL	www.cynet.com	**Routes to market**	Europe: channel; US: channel and direct sales
Company headquarters	Tel Aviv, Israel	**Number of employees**	100+

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

Trend Micro starts to flesh out its XDR story, INT005-000026 (August 2019)

Palo Alto Networks Cortex XDR spans endpoint, network, and the cloud for detection and response, INT003-000351 (April 2019)

2019 Trends to Watch: Cybersecurity, INT003-000295 (December 2018)

The Evolution of Endpoint Detection and Response, INT003-000022 (December 2017)

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@ovum.com

Rob Bamforth, Associate Analyst

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

The contents of this product are protected by international copyright laws, database rights and other intellectual property rights. The owner of these rights is Informa Telecoms and Media Limited, our affiliates or other third party licensors. All product and company names and logos contained within or appearing on this product are the trademarks, service marks or trading names of their respective owners, including Informa Telecoms and Media Limited. This product may not be copied, reproduced, distributed or transmitted in any form or by any means without the prior permission of Informa Telecoms and Media Limited.

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

CONTACT US

ovum.informa.com

askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Boston
Chicago
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
Paris
San Francisco
Sao Paulo
Shanghai
Singapore
Sydney
Tokyo