# IDC REPORT ON CYNET

## Advanced Threat Detection

Digital Pathways

**For More Information on Cynet Contact**
Digital Pathways Ltd
Harlow Enterprise Hub
Edinburgh Way
Harlow
Essex CM20 2NQ

Tel: 0844 586 0040
Email: intouch@digitalpathways.co.uk
Web: www.digpath.co.uk

Vendor Profile

# Cynet: Forging a Solution for Comprehensive, Integrated Security with the Cynet 360 Platform

Mark Child

## IDC OPINION

Information security has become a top concern for all organizations due to ever-evolving threats, complex infrastructure, and limited security teams. The market has answered with prolific innovation and the development of advanced security tools to meet specific needs. Nevertheless, this in itself has brought challenges, as companies are struggling to integrate and manage the plethora of security tools that they have incrementally deployed.

Major vendors have responded to these market developments with acquisitions of key technologies to plug gaps in their portfolios. They have integrated these acquisitions into complex security management dashboards. However, each solution seems to throw up a fresh challenge, and the market is now ripe for natively built comprehensive security platforms with seamless interoperability across components. Where natively built components are unavailable, native integration capabilities are the next best thing. Whatever the approach, the goal is to build out the most tightly integrated system — one able to monitor and analyze the properties and activities of all entities across the entire infrastructure, from users and files to endpoints and the network itself.

Here, too, is opportunity. All entities present throughout the network are sources of event and alert data. The central collection, correlation, and analysis of that information enables richer contextual insights into potentially malicious behavior on the network. The final step, then, is to facilitate a response to malicious activity and remediate any identified threats. This, more than anything, can be a considerable operational challenge in terms of the time and resources required and the skills and sensitivity to remediate without disrupting legitimate users, systems, or business operations. This has resulted in increasing demand for automated remediation capabilities. The deployment of such capabilities is not unusual in pre-compromise responses to basic alerts, but it is still a nascent field when it comes to more complex post-compromise mitigation and remediation.

## IN THIS VENDOR PROFILE

This IDC Vendor Profile provides an overview of Israel-based Cynet, which offers a comprehensive platform, Cynet 360, for the detection of common and advanced threats and automated remediation. The study examines Cynet's solution strategy, product capabilities, and complementary services, as well as its go-to-market approach, market sweet spots, and customer base. IDC assesses the drivers of demand for Cynet's platform and provides guidance that could help drive further growth for Cynet.

## SITUATION OVERVIEW

### Introduction

It is no secret that Israel has been producing many of the sharpest security start-ups for many years. Cynet exemplifies that trend, with its holistic security platform designed and built to overcome many of the key challenges that organizations face today in terms of cybersecurity and tackling both commodity and advanced threats. This is by no means a thin field: The rapidly growing next-generation antivirus (NGAV) and endpoint detection and response (EDR) markets are packed with innovative vendors and solutions attempting to solve the problem of monitoring host activity and process execution to prevent initial compromise and uncover undetected malicious presence.

Another approach is the use of network analytics tools that seek to detect active breaches by analyzing network traffic, establishing a behavioral baseline, and detecting anomalous behavior or indicators of compromise (IoCs). This type of analytical approach is integral to the fast-growing user and entity behavior analysis (UEBA) segment. Cynet's 360 platform seeks to deliver all these capabilities through a comprehensive integrated suite, with all security functionalities unified in a single interface to deliver effective, simplified operations and an optimal user experience.

## Company Overview

Cynet was founded in 2015. Its cofounders came from the field of offensive cybersecurity and have a strong awareness of the multitudes of vulnerabilities and threat vectors that hackers look to exploit. The company and its solution have rapidly grown in reputation due to a few key factors:

- Cynet built a unified solution from the ground up, unhampered by legacy code or components that create challenges for integration.
- The company focuses on delivering the fundamental capabilities that enable organizations to execute security functions rather than simply mapping development to established market categories.
- Cynet's platform, Cynet 360, enables customers to move away from siloed security products that leave blind spots within an organization's infrastructure and activity.
- Cynet's platform unifies all security functionalities through a single user interface, enabling effective security management for the security operations team.
- The platform provides granularly automated remediation for incidents even in post-compromise stages, significantly enhancing mitigation and recovery.

In 2016, the company received $7 million in start-up funding from a U.S.-based hedge fund. In 2018, it received a further $13 million in Series B round funding to help continue its rapid growth. The vendor employs around 90 people. Research, engineering, and support teams comprise around 60% of its headcount, with most of the remainder in sales and marketing.

By the end of 2017, Cynet had built up a client base of around 80 companies worldwide. As of 2019, the figure is in the hundreds. The vendor's client base spans multiple geographies, verticals, and size segments. One of the largest clients is insurer Allianz, which uses Cynet's platform to protect around 150,000 endpoints. The smallest are midmarket companies — typically, with around 400-500 endpoints. Other references include retailer Carrefour, UniCredit Bank, Catalina (a U.S shopper intelligence and personalized digital media), Flugger (a Scandinavian paint company), PLDT (a leading Philippine telecommunications provider), and ICL (international manufacturer of chemicals). The upper midmarket represents something of a sweet spot for the vendor. Such companies are more likely to look for a single security solution to cover all their needs (whereas large enterprises typically look to multiple solutions). In geographic terms, the vendor has a strong customer presence in Europe, the Philippines, the United States, and Israel.

## Company Strategy

The dynamic threat landscape, characterized by the increasing volume, variety, and sophistication of threats, has driven waves of security innovation and the emergence of new protection technologies. Although each technology has specific benefits, the result is that organizations now possess complex security stacks that often do not work well together. This, in turn, requires budget, staffing, skills, and time to manage. Cynet has responded to this operational burden with an integrated solution that addresses many security challenges facing organizations, including:

- Unattended Alerts: Manual breach protection workflows can result in unaddressed security events as alert volumes surpass the security team's alert-handling capacity.

- Security Team Size and Skills: Advanced threat detection products may require costly and hard-to-find security skills for effective operation.
- Integration Overhead: Deploying multiple disparate products, each providing partial coverage, necessitates an additional aggregation layer (e.g., a security intelligence and event management system, or SIEM) for management and consolidated threat visibility.
- Deployment and Maintenance: The need to deploy and maintain multiple products creates an operational burden that can lead to slow or partial deployment, leaving the organization exposed to attacks.

One of Cynet's guiding principles is its focus on root causes that prevent organizations from being secure from breaches. These causes include:

- Partial and siloed security products that do not cover an organization's entire environment (leaving blind spots in some areas and overlaps in others)
- Manual post-compromise protection, which leads to longer mean times to remediation and greater risk of lateral movement and data exfiltration

With their backgrounds in offensive cybersecurity, Cynet's cofounders understand well that an organization's attack surface comprises far more than endpoints. Attackers can see many other vectors — a framework of attack surfaces that includes everything from stolen credentials and privilege escalation to rootkits and memory injection. Consequently, Cynet developed its platform as a fully converged suite of security technologies, including endpoint protection, NGAV, user-behavior analysis, EDR, vulnerability management, network analysis, and deception. Cynet uses terms like EDR in its marketing, but it should be emphasized that the vendor focuses on developing the required capabilities rather than mapping technologies. Cynet aims to provide the widest possible attack-vector coverage across all attack stages from its single platform.

Cynet has scaled up rapidly. The vendor is small, flexible, and very focused. Cynet is not looking to replace inbound/outbound traffic protection, such as firewalls (although it can upload scripts to firewalls for remediation). Rather, the vendor focuses on internal environments, continuously monitoring and analyzing process execution, host behavior, user log-on activity, and network traffic. Of course, in the digital transformation (DX) era, this raises questions about mobility and remote access — an area in which Cynet is still developing. Notebook PCs outside the corporate network are protected, as most of the threat protection mechanisms operate autonomously on the agent. Cynet does not yet provide protection for mobile devices like smartphones and tablets. This is something the vendor will need to add in the future as these devices become an increasingly targeted entry point for cybercriminals seeking to penetrate the corporate perimeter. However, as noted above, being small and agile may be an advantage as the vendor seeks to develop and integrate these capabilities into its platform.

## *Key Differentiators*

Cynet emphasizes the benefits of its ground-up development approach in building a truly unified platform that effectively delivers numerous essential security capabilities through a single user interface. The vendor's platform approach brings it into competition with some well-established market leaders (e.g., McAfee, Symantec, and Microsoft), which have had many years to build out their comprehensive platforms. Nevertheless, Cynet notes that building native integrations of non-native (i.e., acquired) components is very demanding: They need to be stripped down to the core, rewritten, integrated, and rebuilt. Even then, the acquiring vendor may still end up with some relatively disparate products or modules that are only unified on the management interface. Cynet's determination to build everything from scratch has resulted in a solution with seamless integration between all its components and functionalities — a significant benefit for security professionals using the solution.

As previously noted, Cynet places considerable emphasis on post-compromise protection. The vendor is striving to be a trailblazer in the field of automated discovery and mitigation. Automated remediation in the early stages of an attack might mean simply killing a process or limiting access rights, and numerous solutions are already available on the market that can provide this level of orchestration. However, post-compromise remediation can be more complex, once hackers have progressed beyond reconnaissance into, for example, privilege escalation or lateral movement. At this stage, the organization might need to isolate a host or disable user accounts, which can have more significant implications. Consequently, many organizations tend toward the mindset that post-compromise malicious activity is best detected and addressed with manual triage, investigation, and remediation (often augmented with EDR, UEBA, and network analytics tools).

For clients, automated remediation at this stage can be daunting: They may face significant operational risks if a key system is quarantined or users are frozen out of an application. Many of Cynet's customers prefer to start with its automated remediation capabilities switched off. Once an event type has been successfully and correctly detected multiple times, then they may switch on the automated remediation for that event type. This granular addition of automation is a key benefit of Cynet's platform. Customers, for example, might aim for an 80:20 approach, whereby the goal is automated remediation for the 80% of alerts that pertain to low-value assets or have a low impact. Manual intervention is retained for the 20% of alerts and incidents that impact high-value assets. Note that, even when organizations opt for a manual response to specific types of alerts, the Cynet system still provides full context and insights regarding the scope and impact of the malicious activity, as well as guidance and tools for remediation. The degree to which automated remediation is adopted depends on many factors — company culture, vertical market, geography, and regulation — but, ultimately, the customer organization has the choice to automate as much (or as little) as it wants.

In addition to its autonomous agent-based threat prevention and detection, Cynet conducts correlation and analysis on the server layer. Each customer runs a correlation engine, either on a server deployed on premises or in the cloud. This engine collects information from the agents, including asset identifiers, activity data, and alert data. A further level of analysis runs on Cynet's private cloud-based central engine. This ingests and analyzes threat feeds, which are uploaded from the client-based correlation engines via hashes and compared against other incoming feeds to analyze events in an even broader context. Communication between the customer servers and main Cynet server takes place in one of two ways: The local servers query Cynet's server when encountering suspicious activity that they cannot validate locally; or, once a new IoC, signature, or prevention/detection mechanism is uploaded to the main Cynet server, the server pushes the new configuration to all local servers as a response.

Upon deployment at a new customer entity (which can take as little as two hours), Cynet maps the organization's entire network, devices, and dependencies. One of the benefits of this approach is that its system can even address, to some extent, endpoints where it does not have an agent. The system maps that the device exists and can establish a baseline for its behavior. If the device deviates from that baseline, it can be isolated and quarantined or an alert triggered.

For this study, Cynet demoed its platform for IDC. The interface is intuitive: After deployment of the solution and the mapping of the customer's network, security admins are presented with a comprehensive network topology overview, with the ability to view the entire network or zoom in on specific host groups. With a single click, the user can zoom in on any individual asset and get an overview of all its properties (e.g., configuration and installed software), dependencies, and activities, from the time of the initial scan to the present view time.

Cynet also provides a 360-degree alert view, which shows the threat activity status across the entire environment, including files, network, users, and hosts. Each alert is classified as either critical, high, midrange, or low, based on the level of manifested malicious presence or activity. The home screen includes a threat radar that shows high and critical alerts only, but alerts can easily be filtered manually, either from the alert screen or when zooming in on assets (files, hosts, users, and network). Again, a single click can drill down into any alert, showing the affected asset (or assets) and the activity of any compromise or attempted breach. The next level presents the security administrator or analyst with remediation options, with both manual and automated remediation options available. The system also provides file analyses, sandbox sample analyses, and more, all managed through its single user interface. This provides the customer organization with insights and context around malicious activity affecting its systems and networks, enabling it to respond to current threats more effectively and be more prepared for whatever may come next.

### SWAT Support

Cynet reinforces its 360 platform with a 24 x 7 Cyber SWAT team, called CyOps, as an integrated part of its offering (not a paid add-on). The team provides threat hunting across customer environments, incident response assistance, file analysis, and other incident investigation services. The front line comprises a team of 10-15 analysts on shifts, backed up by a team of top security researchers and multiple threat feeds. All these elements combine into a real-time value product and a real-time threat landscape feed.

### Open for Integration

Although Cynet has designed and built its platform as a comprehensive threat prevention solution, the vendor recognizes opportunities in mature organizations that have developed security infrastructure. In these cases, Cynet can be deployed as an EPP and EDR solution and integrated with the existing security stack, sending alerts to the client's SIEM or log analysis tool, which will continue to serve as the main organizational security backbone. Even in its standard deployment model (i.e., when the Cynet platform is the main backbone and the client utilizes all its prevention and detection functionalities), Cynet still ingests data feeds from firewalls, proxies, Active Directory, and more.

### Doubling Up — With Deception

Although deception as a military technique has existed since Sun Tzu, in the field of cybersecurity, it is still only gradually gaining traction on the market. This is due, in part, to the demanding nature of running and updating deception solutions, which must be regularly rejuvenated to keep them fresh. To date, Cynet has provided deception capabilities using decoy files and folders placed within the network to attract attackers. Once an attacker accesses one of these files or folders, it sets off alerts and triggers tracking mechanisms that enable the client to track the attacker's activity. As a further step in its development, Cynet is now adding decoy nodes and servers to its deception capabilities to enhance the deception and increase the likelihood of attracting and detecting hackers within the network.

## *Business Strategy*

Cynet highlights two customer groups that are particularly responsive to its value proposition:

- Large Organizations: Despite their size, some large organizations may not sustain a large enough security team. Cynet enables these organizations to gain protection from both standard and advanced threats within their existing resources.
- Medium-Sized Organizations: With basic security in place, these organizations are looking for protection from advanced threats that traditional antivirus and firewall cannot confront. Cynet's solution can either be used to augment the existing antivirus or replace it altogether.

Cynet has three distinct go-to-market approaches. In Europe, the company maintains a large field sales team that works with channel partners and primarily targets the enterprise space. The focus in the U.S. is on the midmarket, which is targeted mostly by the vendor's inside sales team. The third approach is established partnerships with leading managed security service providers (MSSPs).

## FUTURE OUTLOOK

The proliferation of security toolsets and integrated stacks to provide advanced threat protection, in response to the operational needs of end-user organizations, is driving a tendency toward market consolidation. End-user companies and institutions need to defend themselves against both commodity threats and advanced threats. Large, established security vendors are reacting to the need for unified, integrated security infrastructure in two ways: first, with strong mergers and acquisitions activity to integrate acquired technologies into their offerings; second, through the creation of partner communities from which third-party solutions can be integrated. The emergence of Cynet as a natively consolidated platform provides the vendor with compelling positioning compared with that of acquisition-based platforms.

The dynamic threat landscape — in particular, the commoditization of advanced hacking tools that make formerly sophisticated attacks accessible to "common" cybercriminals — will drive the expansion of the advanced threat protection market. Protection against advanced threats is increasingly an actual and tangible concern for all organizations, regardless of vertical market or organization size. At the same time, organizations still need to protect themselves against large volumes of "standard" threats. The role of easy-to-deploy, consolidated, and automated breach protection should expand, in line with the twofold challenge that organizations now face.

To address this future demand, Cynet plans to heavily invest in marketing and sales to maximize its engagement with potential prospects that could deploy the Cynet 360 platform either as a part of, or as a replacement for, their current security stacks.

## ESSENTIAL GUIDANCE

### Advice for Cynet

Three significant forces are driving the market for advanced integrated security platforms: the dynamic threat landscape and proliferation of advanced threats; the emergence and evolution of a growing number of innovative security solutions that address specific needs; and the challenge for organizations to manage and maintain that solution stack with the skills and resources of their existing security programs. Cynet brings a compelling proposition to the market, but it is not the only player operating in this space.

IDC recommends that Cynet focuses on the following:

- European Expansion: Cynet's enterprise clients in Europe constitute a significant portfolio of references. The vendor should seek to build on this with a drive into the European midmarket, supported by inside sales, with vertical-specific experience highlighted in the pre-sales phase. As the company builds its installed base and reputation in Europe, this can then be used to support expansion in the lucrative U.S. market — intensifying the inside sales program and developing partnerships to start pushing up from the midmarket into the enterprise space.
- Partnerships: Although Cynet is keen to promote its natively built solution and unified interface, it would also make sense to expand its reach by enlisting allies. On one hand, this could mean using technology vendor partnership initiatives to fit in with broader product environments. On the other, systems integrators and MSSPs promise expanded customer access as a part of broader deployments, managed services, and so forth.
- Adoption Paths: Cynet is seeking to blaze a trail in the automated detection and remediation space but is aware of the caution with which many organizations view automated remediation. The possibility for granular adoption of automation makes this more palatable to clients. However, the vendor could go a step further in terms of managing and enabling this process with pre-configured templates or adoption paths. These could be further customized for specific verticals, geographies, and/or architectures.

- Mobility Protection: IDC research has found that DX is a business priority for 89% of organizations, with mobile devices and remote workers pillars of digital business. Although mobile devices are not yet a leading entry point for security breaches, they are increasingly targeted as part of the attack surface. Cynet needs to work to introduce mobility protection capabilities to reassure its customers and prospects that it is protecting as much of their infrastructures as possible, as well as to remain in line with its own comprehensive "360 degree" protection message.

## LEARN MORE

### Related Research

- *Worldwide IT Security Products Forecast, 2018-2022: Do You Make Friends or Acquire Technology to Round Out a Portfolio?* (IDC #US44182918, August 2018)
- *Survey Results: More Security Spending Does Not Lead to Fewer Incidents* (IDC #US44520918, December 2018)
- *IDC Market Glance: Cybersecurity AIRO, 1Q19* (IDC #US44774419, February 2019)

## 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 CEMA

Male namesti 13
110 00 Prague 1, Czech Republic
+420 2 2142 3140
Twitter: @IDC
idc-community.com
www.idc.com