REPORT REPRINT

Cynet aims to consolidate breach-protection efforts in a single platform

APRIL 15 2019

By Fernando Montenegro

In most organizations, security teams handle many issues, including dealing with staff shortages and touching multiple tools. Cynet offers an integrated approach to these issues, bringing together features from areas such as EDR, deception, user behavior analytics, and more.

451 Research®

Summary

By now, it is a truism that 'cybersecurity is important' and that security teams are asked to do significantly more work with limited resources. The dynamics of how this problem has been addressed so far usually results in organizations deploying point solutions that may not only leave gaps but also require significant manual operations work. Cynet is looking to tackle these issues with a different approach: it offers an integrated security suite that it claims can address different aspects of breach protection in a more holistic manner, covering user, file, host and network elements.

451 TAKE

As we look at user sentiments such as that captured in our Voice of the Enterprise program, it has become common for organizations to report significant levels of workload for their security teams, along with difficulties in hiring and retaining professionals. Vendors have responded with increasing levels of support for automation and integration. Cynet is one of these vendors, offering an approach to handle breach protection by combining insights from endpoint, user behavior, network analysis and IT hygiene in an effort to provide a 'the whole is greater than the sum of its parts' theme for resource-strapped organizations. This approach has merits as it may optimize security operations. The challenge for the company will be to deliver the required level of security effectiveness across a broad range of technologies and use cases. If Cynet can do that consistently, its integrated approach will likely find receptive prospects.

Context

Cynet is based in New York City, but hails from and maintains a strong presence in Israel, where it was founded in 2015 by Eyal Gruner, Boaz Zilber, Idan Amir and Netaneal Amar. The company has about 90 employees. Cynet originated within BugSec, an Israel-based specialty security consulting firm that has been active since 2005.

The company is currently led by co-CEOs Uzi Krieger and Eyal Gruner. Gruner was cofounder and CEO of Versafe, which was acquired by F5 Networks in 2013. He's also on the board of BugSec. Krieger was brought in as co-CEO in early 2018, coming from his previous role as VP of marketing at Stratoscale.

Cynet has raised a total of $20m across two funding rounds. The latest tranche – a $13m series B round in June 2018 – was led by Norwest Venture Partners and included Ibex Ventures and Shlomo Kramer. The company puts its current revenue at $10m-20m.

Strategy

Cynet's main thesis is that organizations are looking to optimize how they do breach detection overall, and that an automated, integrated offering can be appealing if it can break known silos in security. The integration the company proposes is based on having a model that looks at the security aspects of host, network, file and user elements to track process execution, user activity and network traffic. The company reports that it has hundreds of customers with an aggregate pool of about one million endpoints. Clients range from SMBs to midmarket firms to enterprises, with no specific vertical standing out. Cynet claims that some of its larger customers have upwards of 100,000 endpoints.

The company's go-to-market strategy is twofold. For European customers, it has been building direct field sales capabilities and it targets larger organizations. Fulfillment is done via the channel. It also uses a similar model for strategic customers in Asia. In North America, the company is initially targeting smaller-sized clients – SMB and midsized – that it reaches through its internal sales capabilities. Interestingly, Cynet indicates that it has no public strategic alliances. Other than the use of external threat feeds to support its detection efforts, the company claims to have developed all of its modules and technology.

Cynet is looking to expand its North American presence and is currently in the process of forging channel relationships. It is also working with its strategic customers to expand deployments, aiming to capitalize on broader adoption of integrated security approaches.

Products

The vendor's approach is centered on offering broad environment visibility covering what it considers four key vectors of concern: user activity, file execution, network traffic and host processes behavior. Cynet aggregates security signals from these areas into a holistic view from which it can provide threat discovery and mitigation. The offering also includes elements of IT hygiene such as vulnerability assessment, asset management, and others. The key objective is to help customers reduce the burden of responding to security threats, which translates into a variety of use cases. There are elements of plain IT hygiene via identification of vulnerable systems and managing those vulnerabilities.

To tackle threat prevention and detection, Cynet's agent monitors files at pre-execution and runtime, as well as user behavior and network analytics. It also employs an additional deception layer of decoy data files, passwords and network connections. Detections are developed with signatures built into the platform or written with the support of the company's managed service offering. Lastly, the embedded analytic capabilities are designed to disseminate threat information to the rest of the organization and potentially other Cynet customers.

The company offers architecture options that support on-premises, SaaS, private cloud and hybrid deployments and has indicated that ease of use is a key component of its vision. The client is deployed to Windows, Mac or Linux endpoints, and connects either to a server within the organization or directly to Cynet's SaaS presence. Organizations choosing to deploy a server within their environments can also send network telemetry and system logs for enrichment.

The agent is offered in both persistent and dissolvable form factors and interacts with system events via both user-mode and kernel-level components. The agent can coexist with other endpoint security agents on a target endpoint. As 'security signal' data is collected by the endpoints, it is sent to a correlation engine that processes inputs against signatures and rules that can fire automated or manual remediation actions.

Cynet implements functionality from distinct areas. Endpoint-protection features include malware protection via machine learning static analysis, threat intelligence and signatures, as well as behavior-based protection against exploits and other types of malware or abuse. Endpoint-detection and response features support process behavior analysis and investigations. The offering includes capabilities for user behavior analysis and network analytics. This latter set aims to tackle use cases such as detecting credential theft, lateral movement, reconnaissance and data exfiltration.

The company also implements deception capabilities – setting up lures to trick attackers into revealing additional information – and vulnerability management, as it can report on out-of-date components that may increase an organization's vulnerable attack surface. Once incidents are detected, the offering is architected to distribute relevant threat information to other nodes in its environment. Cynet then offers a broad set of remediation options, ranging from disabling access for specific users to deleting or quarantining files or various options around host isolation and configuration. These options can be executed directly or scripted and integrated with the rest of a customer's environment.

Cynet indicates that its 24/7 security operations center (SOC) is a key component of its offering. Dubbed CyOps, the team is responsible for investigating malicious activity and creating new detection signatures for them. It is also aimed at assisting customers with proactive threat hunting, remediations and escalations. Additionally, CyOps is responsible for distributing findings to the rest of Cynet's installed base.

Competition

By choosing to integrate multiple functions, Cynet is betting that the whole is greater than the sum of its parts. Still, this choice puts it in competition across several fronts. The vendor's agent footprint offers functionality that overlaps with traditional endpoint security products. As such, the competition is fierce. Alternative offerings come from Crowdstrike, Carbon Black, Symantec, McAfee, Trend Micro, and many more. In the midmarket, contenders include Bitdefender, Malwarebytes, ESET, F-Secure, Panda Security, Webroot, and more.

Cynet's features in other areas such as network, deception and user analytics bring in many other rivals. Darktrace, ExtraHop, Securonix, Vectra Networks, Palo Alto Networks and Microsoft, among others, offer capabilities in network and user analytics. Deception specialists include Attivo Networks, Illusive, TrapX, and others.

The ability to offer support via a SOC is becoming a common feature across the industry, and Cynet is looking to differentiate by including this feature in its offering. Still, it should encounter managed security service providers such as Secureworks, Red Canary, eSentire, and others. Against such broad competition, Cynet anticipates that it will be able to differentiate by highlighting the synergy between the various components of its offering and the benefits it can bring, including automation and risk reduction.

SWOT Analysis

STRENGTHS

Cynet's approach of offering a single interface for many aspects of breach protection and IT hygiene offers the potential to simplify security operations.

WEAKNESSES

The company's 'broad versus deep' approach means it may not be able to address the needs of organizations with more sophisticated actors in their threat models.

OPPORTUNITIES

As organizations struggle to keep up with security demands, many are seeking opportunities to streamline the delivery of security functionality. Cynet's approach may fit well in this dynamic.

THREATS

Many security vendors with deeper functionality in their specific areas have spent significant effort adapting their offerings to support resource-constrained customers and may deliver similar benefits through orchestration and managed services.