IDC MarketScape

IDC MarketScape: Worldwide Endpoint Specialized Threat Analysis and Protection 2017 Vendor Assessment

Robert Westervelt

THIS IDC MARKETSCAPE EXCERPT FEATURES: CARBON BLACK

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Endpoint Specialized Threat Analysis and Protection Vendor Assessment

Source: IDC, 2017
IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Endpoint Specialized Threat Analysis and Protection 2017 Vendor Assessment (Doc # US42385717). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

This IDC study represents the vendor assessment model called IDC MarketScape. This research is a quantitative and qualitative assessment of the characteristics that explain a vendor's current and future success in the marketplace. This study assesses the capability and business strategies of the market leading endpoint specialized threat analysis and protection (STAP) vendors. This evaluation is based on a comprehensive framework and set of parameters for enterprises that seek modern, signatureless endpoint threat detection, prevention, response, and remediation capabilities. A significant and unique component of this evaluation is the inclusion of the buyers' perception of both the key characteristics and the capabilities of these endpoint STAP providers. As one would expect of market leaders, overall, these firms performed very well on this assessment. Key findings include:

- Few differentiators exist among the underlying technologies used to detect and prevent known and previously unknown threats on the endpoint. To identify leading solutions, this analysis considered the functionality of the endpoint client and the level of automated remediation, response, and mitigation capabilities provided to customers. It considered each vendor's managed, professional, and threat intelligence services offered to customers. It also examined the comprehensiveness and cohesiveness of the vendor's solution set to correlate threat information from endpoint, web, messaging, and network attack vectors.

- Enterprise inquiries seeking assistance with the vendor selection process over the past year ranged from organizations seeking to bolster threat prevention at the endpoint to those that had suffered multiple ransomware infections seeking alternatives to their existing antivirus software. Organizations with heavier networking security influencers had endpoint security from Cisco, Palo Alto Networks, and Check Point on their short list. Those with dedicated incident responders or vocal endpoint administrator influencers tended to have Carbon Black, CrowdStrike, and Cylance and modern threat detection and response products from McAfee, Symantec, and Trend Micro on their short list.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

This research includes analysis of 11 modern endpoint security solutions from security vendors that were the subject of numerous enterprise inquiries over the past 12 months. This assessment evaluated existing capabilities, the endpoint client, and other characteristics of each firm. It also examined the size and/or the breadth of managed and professional security services each vendor offered to customers. It is conceivable, and in fact the case, that other security vendors compete with these 11 endpoint security vendors on an equal footing. As such, this evaluation should not be considered a "final judgment" on the firms to consider for a project. An enterprise's specific objectives...
and requirements will play a significant role in determining which firms should be considered as potential candidates for thorough evaluation and testing during the selection process. Further:

- This analysis was conducted from September to December 2016 and follow up interviews with customers and vendors took place in the first three months of 2017.
- The primary detection and/or prevention method for Endpoint STAP products must be signatureless. The solutions must provide continuous endpoint monitoring and endpoint forensics to support rapid response and remediation. Some security vendors were excluded from this analysis because IDC considered the endpoint STAP product incomplete or lacking full integration into the overall offering for signatureless defense, security incident response, and remediation tools. For example, some products lacked advanced machine learning-based threat detection at the time of this analysis.
- IDC also exclude a minority of vendors that used containerization at the endpoint and may have required specific CPU or other specific hardware requirements. Those technologies have been widely adopted for smaller, targeted deployments.
- Finally, traditional, signature-based antivirus engines and other widely used threat detection and prevention technologies often continue to play a role with modern endpoint security offerings. These long-standing technologies are still used to reduce false positives and lessen the load on analytics engines and other innovative detection and prevention components.

**ESSENTIAL BUYER GUIDANCE**

The market is flooded with endpoint security technologies, incident response tools, threat intelligence feeds, and behavioral analytics. Know what the key requirements are before shopping for modern endpoint threat detection, prevention and/or response, and remediation solutions:

- **Endpoint agent functionality**: Modern endpoint security products should provide a kernel-based or hybrid agent that detects and can be configured to block regardless of endpoint device connectivity. Evaluate the space and CPU requirements of the endpoint client. Determine which detection and prevention capabilities are enabled by default. Some prevention capabilities must be carefully tested and tuned to avoid disrupting custom applications and scripts. Gauge the existing false positive rate, and compare how the new solution impacts it. Enabling prevention often causes an increase in false positives.
- **Managed and professional services**: Adding modern endpoint security products may impact internal incident response workflow and remediation processes. Organizations of all sizes are choosing to augment IT security with managed security services. Some vendors offer their own managed services. Others refer customers to managed services provider partners. Vendors also have various levels of professional services, such as risk assessments, penetration testing, incident response training, and boots-on-the-ground breach support retainer services to consider.
- **Cloud based or on-premises**: Determine the organization's preferred deployment model for endpoint security, and examine the architecture of the vendors you are evaluating. Some security vendors provide a lightweight agent combined with cloud-based analytics and a web-based management console. Other providers require an on-premises management appliance for analytics and historical search for incident response. And other vendors provide a hybrid approach with cloud-based analytics, an on-premises management appliance, and an endpoint client.
● **Live response and automation**: Determine if your IT team can support solutions that provide live response and remediation tools and extensive endpoint forensics. Many security vendors sell a standalone endpoint security solution and a more extensive offering that supports active threat hunting and integrated live response and remediation tools. It may be more prudent to adopt the lightweight, standalone solution to meet immediate requirements and then add more extensive components when they are needed.

**Before Evaluating Endpoint Security Products**

A few basic steps can make the difference between adopting a tool that isn’t the right fit and adopting one that supports existing requirements and can grow and be adapted to changes to the organization’s environment. Take the following steps before evaluating vendor products:

- Assess the organization’s existing endpoint security solutions and whether they are properly configured and maintained. Carefully evaluate the investments already made throughout the organization's IT security architecture. Identify ways to bridge siloed security technologies to create a comprehensive approach for threat detection and prevention.
- Examine the existing security program to determine whether the security posture can be improved by fine-tuning common security best practices. Many data breaches stem from failing to patch highly used productivity software and poorly configured and managed network devices and applications. Enterprises often poorly communicate security policies or communicate them effectively but lack policy enforcement mechanisms.
- Cybercriminals target the human fallibility in all of us. A significant number of attacks are delivered through spam and phishing messages containing malicious file attachments or links to attack websites. Consider implementing a sustained security awareness training program. Evaluate the effectiveness of the enterprise’s messaging security technology.

**VENDOR SUMMARY PROFILES**

This section briefly explains IDC’s key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor’s strengths and challenges.

**Carbon Black**

Waltham, Massachusetts-based Carbon Black (formerly Bit9) is a Leader in this IDC MarketScape for endpoint STAP for its feature-rich response and threat-hunting offering, Carbon Black Response. The company was renamed from Bit9 following its acquisition of Carbon Black in 2014. That acquisition added incident response, threat hunting, and remediation capabilities that incident responders continually praise.

In addition, Carbon Black sells an application control product that is used by many of its customers as an effective approach to blocking advanced threats, and in July 2016, it acquired Confer, a security start-up that is positioned as a modern, cloud-delivered antivirus alternative with converged EDR.

Carbon Black sells three products: Cb Defense (formerly the Confer offering), which is an antivirus alternative that provides signatureless prevention and detection aimed mainly at security administrators looking to secure end-user systems; Cb Response for incident response and threat hunting targeted at security operations centers (SOC) and incident responders; and Cb Protection...
(formerly the Bit9 platform) for application control that would appeal to IT operations teams looking to secure servers, critical systems, and targeted whitelisting application control deployments.

Customers interviewed by IDC highly praised Cb Response, choosing it over competitive solutions to improve their triage, threat hunting, incident response, and remediation processes. Carbon Black has a strategic plan to fully integrate Confer and leverage its cloud-based architecture to create a unified platform with a single agent and integrated back-end infrastructure. Carbon Black plans to continue to offer the products separately for customers that require on-premise security products.

The security vendor also views its threat intelligence cloud as a unique differentiator against competitive offerings; it feeds advanced threat intelligence to all three endpoint products. The information combines multiple antivirus engines, threat intelligence feeds, and indicators of compromise as well as proprietary and customer-created patterns of attack as part of its analytics engine. The alerts are coupled with the deep contextual information needed to investigate and rapidly block and respond to new threats.

Cb Response, the incident response and active hunting solution, is recommended for larger organizations. It gathers continuous behavioral and contextual data on millions of endpoints to investigate and rapidly respond to new threats. In January 2017, the company addressed the scalability of Cb Response to support up to 150,000 endpoints per server cluster. Previously, it had been limited to about 40,000 seats.

Cb Defense combines prevention, detection, and response into a single offering, giving security teams complete visibility over their enterprises. Cb Defense provides strong behavioral prevention capabilities and can be set to block file system activity, network communication such as a malware callback to a command and control infrastructure, or automatically kill malicious processes associated with memory-based attacks. Cb Defense is a certified antivirus offering by Coalfire, and it is also a HIPAA- and PCI-compliant AV offering. A recent update enhances Cb Defense with critical Cb Response features including enhanced in-memory visibility, binary detonation of malware, and an improved user interface. The update also includes the "live response" feature, which allows for complete remote remediation through a secure shell into an infected machine, automated remediation, and open API's for integration with third-party products.

Cb Protection provides application control for servers and critical systems. Organizations can establish automated software controls and protection policies that completely lockdown corporate assets, intellectual property, and regulated data. The solution also integrates file/system integrity monitoring, device control, memory protection, and hardening to ensure that malware and non-malware attacks are not allowed to execute.

**Strengths**

- The Carbon Black Response platform is heralded by a wide variety of incident responders and security operations center personnel for the rich contextual information it uses to support alerts. Organizations can set up custom rules to isolate hosts, block custom malware, or automatically trigger an action in third-party products such as a policy enforcement change in an application whitelisting solution or a rule supporting an intrusion prevention system.
- Carbon Black Live Response is a differentiator against competitor products and provides responders the ability to conduct remote remediation. Responders use the tool to set up a secure tunnel into an affected system. Customers praise the Cb Response for its extensive
default functionality. Responders can run remediation scripts, collect memory and process information, and issue system-level calls.

- Enterprises that lack IT security resources or those seeking an alternative to traditional antivirus should take note of Carbon Black's $100 million acquisition of Confer and its subsequent integration into the company's portfolio as Carbon Black Defense. This makes Carbon Black a solid cloud-delivered antivirus alternative.

**Challenges**

- Carbon Black Response is viewed as an endpoint forensics or an active threat hunting tool for incident responders. The solution supports prevention, but at the time this document was written, blocking capabilities are available via the Microsoft EMET integration, and custom policy creation is required to prevent file-less attacks.
- Automated response, a feature increasingly requested by enterprises with limited IT resources, is not yet a core component of Carbon Black's offering. The company generally refers those seeking automation to its third-party APIs and integration with security information event management systems.
- Carbon Black partners for managed services and doesn't offer professional services. It recently added a crowdsourced cloud and threat research offering.

**APPENDIX**

**Reading an IDC MarketScape Graph**

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

**IDC MarketScape Methodology**

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.
Market Definition

The specialized threat analysis and protection market overlaps the endpoint, messaging, network, security and vulnerability management, and web functional markets. The products help protect enterprises from modern malware and attack techniques that are typically not detected by traditional signature-based technologies. STAP products use a variety of non-signature-based protection methods including, but not limited to, sandboxing, behavioral analysis, file integrity monitoring, telemetric heuristics, containerization, netflow analysis, and threat intelligence. These solutions are typically tied to on-premise or SaaS-based analytics to provide alerts and context for incident responders. Some products only detect and alert, while others have automated remediation components. Although some features within STAP may appear in other products, this competitive market consists of dedicated STAP solutions.

LEARN MORE

Related Research


Synopsis

This IDC study uses the IDC MarketScape model to provide an assessment of a number of providers participating in the endpoint specialized threat analysis and protection market. This IDC MarketScape is an evaluation based on a comprehensive framework and a set of parameters that assesses providers relative to one another and to those factors expected to be most conducive to success in a given market during both the short term and the long term.

"Endpoint security vendors have created innovative solutions that support detection and prevention of known threats and zero-day threats, and many of them incorporate robust platforms that support active threat hunting, response, and remediation capabilities. The vendors in this evaluation have captured a significant amount of the market with innovative and sometimes bold approaches to providing endpoint threat protection." – Robert Westervelt, research manager and lead of IDC’s Data Security practice


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.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights. IDC and IDC MarketScape are trademarks of International Data Group, Inc.

Copyright 2017 IDC. Reproduction is forbidden unless authorized. All rights reserved.