BUYERS' GUIDE

A Buyers' Guide to SecOps

An Osterman Research Buyers' Guide
Published July 2018

Carbon Black.

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond • Washington • 98010-1058 • USA
+1 206 683 5683 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

Introduction

Endpoints are the face of IT for the users in organizations, and the place of their greatest productivity when everything is working right. It's where employees work from and through, both in the office and while on the road. It's where server processes run to deliver capabilities from those on-premise environments that we haven't yet—or won't ever—shift to cloud services. Endpoints have powerful capabilities to enable and facilitate productive work and are frequently—if not continuously—used by the majority of employees to fulfill their job.

Endpoints are also one of the greatest threat vectors facing organizations today. Traditional malware threats continue unabated, but have been joined by advanced and emerging threats that cover their tracks, hide in plain sight until triggered, or try to slip in undetected through social engineering tricks or rogue/vulnerable applications. Keeping endpoints safe, secure, and sound is a job of that crosses the disciplines of IT security and IT operations.

Organizations of all sizes require the ability to keep endpoints secure and performant. Organizations at the larger end of the scale tend to have dedicated Security Operations Centers (SOCs), staffed by highly trained security personnel, and making use of specialized security tools. Organizations in the mid-market and smaller, however, usually don't have the same resources available for security, and must therefore be extremely clever in the security tools they deploy to mitigate the risks and challenges experienced daily. Mid-market and small organizations have a great need for new security and operations tools to address gaps in talent.

While the size of organizations differs, the nature of the challenge remains the same—maintain, assure and enhance endpoint performance while protecting against security threats, data breaches, ransomware, credential theft, and compliance violations. In recent years, security vendors have released new tools to help organizations in the fight against security threats and operational drift, with capabilities for constant monitoring and awareness of endpoint status.

These Endpoint detection and response (EDR) tools capture current data in real-time. This historical, activity-based data can be used for analysis to detect emerging security threats that go far beyond the capabilities of security tools that work by blocking known malware through signature files. While this offers a tremendous step up in protection, there is another complementary set of capabilities that EDR tools cannot supply—the ability to ask specific questions of your endpoints in real-time for precise data on the status or health of those endpoints, as well as the ability to act based on query results. This complementary need has led to the emergence of a new class of security and operations tools that put proactive IT hygiene, security and operational capabilities in the hands of security and operations staff members.

This new class of tools enables the following types of tasks for security and operations:

- **Which endpoints do or do not have a specific software application installed?**
  Answers are helpful for licensing management, but also awareness of outstanding patching requirements and the use of shadow IT applications that may introduce security vulnerabilities.

- **Which endpoints have a particular version of a specific software application installed?**
  The answer helps with quickly identifying vulnerable applications on endpoints and is the first step for remediating any out-of-spec endpoints—especially when new zero-day vulnerabilities are discovered.

- **Do any of our endpoints have particular registry values set?**
  The answer can pinpoint endpoints with outstanding security vulnerabilities, and again, enable precise action to rectify.

- **How many systems are using unauthorized removable devices or operating without disk encryption?**
  The answers show where remedial action is required to bring endpoints into alignment with corporate standards and compliance requirements.

SecOps Tools

The emergence of these real-time, or on-demand, SecOps tools comes on the heels of the DevOps revolution and the move beyond the waterfall model of software development. Bringing software development together with IT operations meant the ability to deliver code faster, with scripted consistency through automation, continuous monitoring to detect divergence and drift from a baseline standard, and the ability to act to address current challenges. DevOps has delivered significant benefits to organizations embracing the new model and new culture, including faster speed to market with new capabilities, responsiveness to changing market dynamics and customer requirements, and fewer deployment errors or human oversight with automation.

The underlying philosophy and tooling of SecOps embraces these same principles: faster analysis and delivery, automation for consistency of response, continuous monitoring, and the ability to act quickly. For example:

- Systematic insight into current state to enable systematic remediation.
- Continuous monitoring to detect configuration drift, security vulnerabilities, and compliance issues.
- The ability to act on endpoints without physically visiting them, for corrective and restorative action.
- Real-time insight into endpoint status and health.

SecOps tools deliver a range of benefits to organizations, specifically:

- Reduced IT complexity due to eliminating the need for multiple, disparate, overlapping, and siloed tools for use by security and operations staff.
- Reduced risk of cybersecurity threats, due to being able to proactively identify and remediate issues in real-time.
- Increased ability to leverage current IT talent for security and operations tasks, pushing back on the global shortage of cybersecurity talent.
- Bridging the culture between security and operations, by offering common tools that enable use cases across both specializations, enabling security and operations to work collaboratively on keeping endpoints safe, secure and sound. Common tools, common data, common abilities and common areas of focus creates shared culture and, as a result, faster investigations and resolutions.

Evaluating SecOps Tools

Evaluating new tools—of many kinds—is a process that covers three evaluation streams: what the product actually does, how it will work within your organizational environment, and wider issues around the vendor and its plans going forward. That is:

- **Product Capabilities**
  What does the product actually do? What are the features and capabilities on offer, and how do these align with or enable the requirements the organization has from a product of this type?

- **Product Fit and Alignment**
  How does the product under evaluation fit and align with the other current products and capabilities in your organization? For products with similar capabilities, are there integration points that can be leveraged? For products that bring unique capabilities, will they interoperate with what you already have, or will they have to be run in isolation?

- **Vendor and Product Analysis**
  Does the vendor have what it takes to support your organization over the lifetime of your need? This includes evaluation areas such as experience with similar organizations, the vendor's financial stability, support and service offerings, engagement with the user community, and their intended product roadmap and cadence of historical deliveries. The cost profile of the product for your organization also comes into the mix.

When designing your evaluation process, consider the following planning issues:

- **Stakeholders:** Who should be involved in the evaluation process, and what groups do these individuals represent? It is strongly recommended to include two or more people in the evaluation process, to reduce bias and take advantage of multiple perspectives.

- **Technical Requirements:** What product capabilities are required by your security and operations people?

- **Test Environment:** Where will the evaluation be undertaken? Will you use a subset of your production environment, a current test lab, or a specially crafted evaluation environment?

- **Deadline:** When does a decision need to be made, and why does this timeframe exist? Understanding the timing and rationale of the decision timeframe enables appropriate planning.

- **Budget:** How much budget can be spent on undertaking an evaluation, and where is this budget coming from? If multiple groups are sharing the cost of the evaluation, you will need to coordinate more intensively around resource usage and expectations.

The scope of your budget and the timeframe available for your evaluation will dictate how you actually go about running the evaluation process. Choose one or more suggested approaches from the following list:

- Review the literature and product guides made available by the different vendors. This approach is commonly called a Document Review or Desk Review. It will generate some insights, but the quality of the documentation will be a determining factor in its efficacy.

- Read what other people say about the product - such as administrators from other organizations, ideas in the vendor's product community forum, and reports from third-parties such as analyst firms.

- Attend conferences where the vendor is presenting, or where customers are presenting on their journey with the vendor's products. While a vendor is unlikely to invite a dissatisfied customer, hearing the reality of the product can provide good insights.

- Arrange a demonstration by someone who has mastered the capabilities of the product and can show off its capabilities. This could be one of the vendor's sales people, an independent consultant, or an internal employee who has been charged specifically with getting ready to demo the offering.

- Look for test results from a third-party testing service, or commission such a service to prepare an analysis for your organization. Such results should compare and contrast multiple offerings, enabling you to check comparative effectiveness.

- Build your own lab and test the capabilities directly. While this is also known as being "thrown in the deep end," it provides some of the best insights into the product capabilities on offer.

Evaluation Guide

The capabilities for SecOps tools for real-time query and response are explored in the following three tables.

1. **Product Capabilities**
   Understanding what the product actually does is essential in an evaluation. Use the following checklist to assess what is and isn't offered.

Functionality	Short Title	Feature	Evaluation / Criteria
Endpoint Interrogation	On-Demand Queries	Run an on-demand or real-time query against all endpoints to determine current, up-to-the-second status.	Verify that a query can be created and run on-demand in real-time against endpoints. A user should be able to form a query as required and instantiate its operation within minutes.
	Query Expressions	Develop a specific query expression in order to interrogate endpoints for precise data.	Verify the ability for a user to develop a specific query expression, with precise targeting capabilities for looking at pre-determined areas on the endpoint.
	Query Automation (Scheduling)	Select and schedule a query to run at a pre-determined time in the future.	Verify the ability to specify a time in the future for a query to run once. Verify the ability to specify a recurrence pattern for the query.
	Interrogation Policies	Limit the ability of specific users to interrogate specific endpoints.	Validate the ability to create scoped groups of endpoints and set access rights for interrogating these.
Endpoint Coverage	Percentage Coverage	The percentage of endpoints that are responsive to a particular query, e.g., the percentage of sensors on endpoints that have responded to a particular query.	Endpoints may be unreachable for many reasons, not the least of which is when an endpoint is in offline mode while an employee is traveling. Verify that query results provide a summary of responsiveness from the normal set of sensors that would be expected to respond. This could be based on an asset register of active sensors, or a running count of which sensors / endpoints are generally responsive.
	No Sensor Left Behind	Queries that complete on less than 100% of endpoints continue to seek results from non-responsive sensors until acceptable coverage is gained.	Determine over what timeframe a query will continue seeking results from sensors, and what triggers the query to stop.

Functionality	Short Title	Feature	Evaluation / Criteria
Query Development	Natural Language Query Builder	Popular or commonly used queries can be selected using natural language (or "plain English") expressions, rather than having to know a query language.	For users who do not know how to use a query language, verify the ability to find the right query to run using natural language search. The specific internals of the query should be hidden from view, unless the user elects to read the query string.
	Advanced Query Builder	A much broader range of precise queries can be created using query language predicates and conditions.	For users who prefer to form their own queries using a query language, verify the ability to write a specific query.
	Saving Queries for Individual Use	Save a list of frequently used, favorite, or preferred queries for a given individual user.	Verify that an individual user can save the queries they have created for later re-use. Users should be able to give each saved queries a human-friendly name and describe what it is intended to do.
	Saving Queries for Shared Use	Save a list of frequently used, favorite, or preferred queries for use by multiple users. This enables best practice to be spread across team members.	Verify than an individual user can save the queries they have created for later re-use by everyone with access to the tool. Queries should have human-readable names and a description.
	Groupings for Saved Queries	Group saved queries into a higher-level unit that makes sense based on something of commonality, such as intent, cadence pattern, or category.	Validate that saved queries can be assigned to a higher-level grouping. This feature will be of more relevance to SecOps teams who save a large number of queries.
	Query Policies	Limit the ability of specific users to create new queries.	Verify that queries can have different access rights, such as the ability to only run a pre-created query, view the results for queries, create new queries, and edit existing queries.
Result Set	Result Set Filtering and Drill Down	The result set for a query is presented along with automatically determined facets or filtering choices for further pinpointing specific information in the result set.	Verify that the query result set is presented with summary data from across the result set, allowing the user to click on specific summary data facets to further shrink the result set. Examples could include specific version numbers for software applications, installation date, and description, among others. These facets should be automatically presented based on common data fields returned by the query and displayed in the result set.

Functionality	Short Title	Feature	Evaluation / Criteria
	Result Set Column Sorting and Ordering	Columns in the result set can be sorted and ordered in different ways, to enable the user to pinpoint specific information in the result set.	Verify that the user can change the initial sorting and ordering of columns in the result set.
	Result Set Visualization	Raw data in the result set can be viewed in visual ways to provide graphical insight into current status and highlight critical issues.	Verify the ability to view the raw data in the result set using common graph and chart formats.
	Result Set Trend Analysis	Query results for the same query are saved for trend analysis.	Ensure that result sets persist beyond the time they are gathered, to enable trend analysis.
Endpoint Remediation	Single Endpoint Action	Perform action on a single endpoint.	Verify the ability for a user to connect to a specific endpoint and perform corrective or restorative action.
	Multiple Endpoint Action	Perform the same actions on multiple endpoints.	Verify the ability for a user to take corrective or restorative action against a set of endpoints simultaneously either in a console or programmatically through an API.
	Link to Taking Action	The ability to initiate immediate action on a specific endpoint from a query response.	Validate that an administrator can initiate action against a specific endpoint directly from a query response, without having to re-identify the endpoint in a separate taking action interface.
	Taking Action Policies	The ability to limit the users who are allowed to take remote action from within the console.	Validate the ability to create scoped groups of endpoints and set access rights for acting on these. An advanced ability is to route action requests for approval.
Cloud-Based Services	Cloud-based Console	Efficient access to query, analysis and remediation tools using a cloud-based console.	Ensure the availability of a cloud-based interface for running all security and operations tasks.
	Cloud Data Collection	Data can be collected from endpoints from wherever they are connected. Endpoints do not have to be on the corporate network.	Validate that endpoints can be contacted when they are connected from beyond the corporate network.
	Cloud Data Storage	Result set data is stored in the cloud, enabling common and consistent access to data for all users, and centralized investigation from one place.	Verify result set data is stored securely in the cloud.

2. Product Fit and Alignment

Exploring how the product fits with your current IT strategy and organizational governance approaches is a second strand of an evaluation. Use the following checklist to assess what is and isn't offered.

Functionality	Short Title	Feature	Evaluation / Criteria
Support for Endpoints	Operating System Support	Support for the types of endpoints being used within your organization.	Verify that the tool supports the range of endpoints you are using within your organization, including any version dependencies for operating systems. Verify support for physical and virtual endpoints.
	Image Support	Support for the corporate images you are using within your organization.	Validate that the sensor can be installed as part of your corporate image or images, and that there are no conflicts.
Sensor Behavior and Performance	Sensor Impact	The sensor operates on the endpoint without compromising its performance.	Percentage impact of the sensor on the endpoint, for memory, CPU and other system resources.
	Sensor Deployment	Deploy the sensor to endpoints in the environment.	Determine how the sensor is deployed to each endpoint, and whether the end user is able to block its installation.
Integration with Related Products	Endpoint Security	Integrate with complementary endpoint security tools that offer capabilities such as anti-malware, next-generation anti-virus, and endpoint detection and response.	Evaluate the integration options with complementary products offered by the same vendor, as well as the availability of standard interfaces for integrating with endpoint security tools from other vendors.
	Custom Integrations	APIs and other standardized methods for integrating with other products in your environment, such as a SIEM for automating and orchestrating remediation activities.	Evaluate the availability of options for integrating with the other products in your environment. Verify if these are available out-of-the-box, or if professional services are required.
Audit Logging	User Activity	Capture and record user activity to provide evidence of who did what when for security analysis and compliance purposes.	Verify how user logs are created and stored securely.

3. Vendor and Product Analysis

The final strand of an evaluation is focused on the vendor and product history and roadmap. The following table looks the features and criteria to investigate.

Functionality	Short Title	Feature	Evaluation / Criteria
Security and Compliance Accreditations	Security and Compliance	Accreditations on the tool and service that address security levels, data protection compliance requirements, monitoring for data breaches, and incident response pathways.	Request the evidence for the security and compliance accreditations held by your vendor. Look at the frequency with which these accreditations are confirmed or attested by appropriate third-parties.
Pricing	Pricing Options	Options for licensing the tools, including discounts available for having multiple products from the same vendor, and any additional maintenance and support costs.	Evaluate the overall pricing structure for your organization, based on how the pricing levels work. Determine the net benefit to your organization.
Support	Product Training	Training resources available to support new users get started, and advanced users push the boundaries.	Verify the ability of product guides, training webinars, classroom options, and advanced coaching.
	Professional Services	Availability of professional services to offer expert assistance with the product and its usage, and the options for how this is delivered.	Verify that the vendor offers professional services support to its customers. Verify if the vendor has a business partner program, and the availability in key markets for your organization of partners able to provide assistance.
	Service Level Agreements (SLAs)	Guarantees from the vendor for service uptime, and whether this is backed by financial penalties for out-of-SLA performance.	Check the SLA for the service and learn how and by whom availability for the SLA is measured. Verify the availability of any third-party audits of availability.
	User Community Engagement	Engagement with the user community.	Check which methods the vendor uses for engaging with their user community, such as online webinars, a dedicated online discussion forum, user group meetings, and conferences. Verify that the vendor encourages sharing of ideas, pre-built and tested queries, and feedback about the product with other users and the vendor.

Functionality	Short Title	Feature	Evaluation / Criteria
Training and User Materials	Product Documentation	Availability of up-to-date documentation on the product.	Verify the availability of product documentation from the vendor, how current this documentation is, and how frequently it is updated. Verify how customers access current documentation, and the change processes in place for removing outdated documentation.
Vendor Stability	History	Past performance by the vendor, and time in market.	Discover how long the vendor has been in the market for, and how they have performed financially and on any stock markets (if applicable).
	Future Outlook	Expected future for the vendor.	What plans does the vendor have going forward, and if applicable, how have these been evaluated by independent third-parties (such as industry and financial analysts).
Product Roadmap	Historical Cadence	Past performance in delivering updates to the product.	Review the historical cadence and frequency of product updates from the vendor. Evaluate the reliability of the vendor in delivering a steady stream of updates over time.
	Future Intent	Disclosed roadmap for the product, including feature updates and additions.	Review the available information on the product roadmap. Evaluate the fit and applicability of these future deliverables for your organization.

Comparing Products

Working through the above tables should give you a short-list of possible products to consider. It is important to proceed with the evaluation as fairly as possible to reduce bias and get the best outcome for your organization. This is one of the reasons for including multiple people in the evaluation. Note that any one product is unlikely to have all of the above capabilities; it's a nascent market, and development is happening at cloud speed. Nevertheless, it is good to get a sense of what's available now and what's on the roadmap.

If you need to pick between two or three products and vendors, do the following:

- Decide on the importance of each of the functionality areas to your organization in the three tables above. Some will be critical for your organization, while others will be less important. Separating the criteria into these different groups provides a way of sifting through relative strengths and weaknesses.

- Use a points system to judge the efficacy of each vendor and product against each of the functionality areas. For example, if your total points allocation is 100, and you have 10 critical areas and 20 less critical areas, divide the 100 points across both columns, giving more weight to the critical areas. For example, each critical area could be worth six points (total of 60 points), and each less critical area only two points (total of 40 points).

- Assign points to each of the functionality areas. If you have multiple evaluators involved, get each evaluator to do this by themselves first before comparing and contrasting results.

- If you have a clear winner based on the points system, enter into contract negotiations and get going as soon as possible.

Conclusion

Endpoints are critical to the performance of organizations and are one of the key vectors for security threats to undermine that performance. New SecOps tools that provide the ability to gain up-to-the-second insight on endpoint status and provide capabilities to act to remediate and rectify any problems are emerging to enable organizations to stay on the right line of performance. This evaluators' guide should help all organizations to determine the opportunity and evaluate the options.

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security. Carbon Black serves more than 4,000 customers globally, including 33 of the Fortune 100. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV). Leveraging its big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus.
Carbon Black and Predictive Security Cloud are registered trademarks or trademarks of Carbon Black, Inc. in the United States and other jurisdictions.