Carbon Black.

Critical Requirements for an Endpoint Security Solution

Deciding on an endpoint security solution can be a difficult task. Many organizations know their current security has gaps, but don't know where to begin in the search for something new. To help with this, SANS has created a guide to evaluating these solutions. The guide outlines the necessary requirements you should look for, as well as how to prepare to run a test.

At Carbon Black, we have seen over and over again that businesses are looking for three things:

Superior Protection | **Actionable Visibility** | **Simplified Operations**

Based on these requirements, we have created a checklist of the features from the guide that we believe are the most critical to your evaluation.

Protection & Detection

CRITICAL

- **Prevention architecture operates on attackers' tools, tactics, techniques and procedures, not just on malware. Recognize and kill patterns that are malicious***
- **Access to multiple forms of prevention, including ability to select and customize based on the specific endpoint***
- **Provide ability to create, test, and quickly deploy policies to improve prevention and reduce false positives***

- Identify and quarantine known and unknown malware
- Protect against fileless attacks such as Flash exploits, browser vulnerabilities exploits, and other techniques that attackers use
- Ensure that NGES software cannot be disabled or altered by an unauthorized user

Cloud-Based Intelligence & Big-Data Analytics

CRITICAL

- **Capture unfiltered endpoint activity data and efficiently send it to the cloud for analysis***
- **Incorporate new and evolving technologies into the product offering through the cloud to aggressively identify and block attacks***

- Gather threat intelligence from multiple sources for integration into NGES, using a cloud-based intelligence and analytics engine and use this intelligence to identify malicious behavior and increase endpoint protection over time
- Participation of the vendor in the threat intelligence community

Carbon Black.

Critical Requirements for an Endpoint Security Solution

Visibility & Context

CRITICAL

- **Build and customize queries and reports related to endpoint state and activity across the entire organization***
- **Reveal the full chain of processes affected by the malware/malicious behavior***

- Log all results/resulting actions from detection of/response to malware/malicious behavior. Present all logged information in human-readable format, independent of the administrative interface
- Provide visualization tools, using both graphical and plain language presentations for real-time visibility and retrospective analysis of events
- Provide interface capability (e.g., API) for integration with other tools, such as a SIEM system, for broader detection and response supports

Performance

CRITICAL

- **Minimize false-positive events, which happen when the product blocks access to a legitimate program***

- Provide protection, including identification of new, potentially malicious, behavior, with minimal impact on the endpoint user experience
- Have lightweight impact on endpoint system resources

Operational Requirements

CRITICAL

- **Standard and custom integrations with third party products***
- **Consolidated cloud based management console for all modules***
- **Collaborative defense. Supports workflows for various security related roles and groups***

- Simple deployment. Supports both manual and automated methods of endpoint deployment
- Multiple endpoint platforms supported: Windows, Mac, & Linux
- Lightweight communication. Support bidirectional communication of threat information between endpoints and the cloud for holistic and robust monitoring

SANS

If you'd like to read the full SANS guide, go to:
carbonblack.com/sans-evaluation-guide