ESG Brief

Webroot's Intelligent Approach to Endpoint Security

Date: September 2015 **Author:** Doug Cahill, Senior Analyst; and Jon Oltsik, Senior Principal Analyst

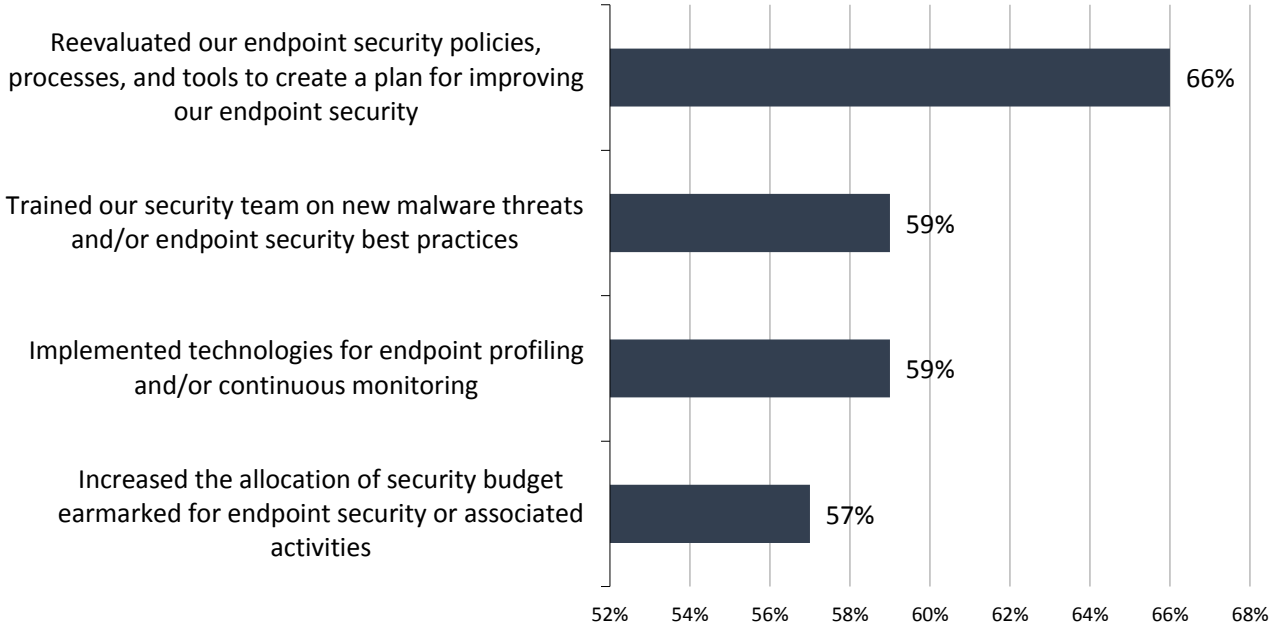
Abstract: *The endpoint often plays a central role in the cyber kill chain, serving as the entry point and staging ground for a broader attack, a dynamic that has raised the stakes in protecting the endpoint attack surface area. Today's endpoint security market is in transition, with customers seeking solutions that protect against zero day malware and exploits while evaluating whether "next-generation" solutions augment or replace traditional antivirus. Webroot SecureAnywhere Business Endpoint Protection strives to bridge the gap with a smart approach to detect, prevent, and remediate malware on endpoints.*

Reevaluating Endpoint Security

Because traditional antivirus (AV) can be ineffective against advanced threats, which are dynamic in nature and thus evade static, signature-based binary matching, many organizations have begun to deploy additional endpoint security controls for continuous monitoring, dynamic analysis, threat intelligence, and more. While this approach has improved detection efficacy, it has done so with an incremental operational cost, especially at scale. Research conducted by ESG highlights actions customers have taken to improve their endpoint security posture (see Figure 1).

Figure 1. Actions Organizations Have Taken with Regard to Endpoint Security

With regard to endpoint security, which of the following actions – if any – has your organization taken over the past two years? (Percent of respondents, N=340, multiple responses accepted)



Source: Enterprise Strategy Group, 2015.

After decades of antivirus as the sole line of defense to protect corporate endpoints, two-thirds of the respondents indicated they have reevaluated their endpoint policies, processes, and tools. To support these initiatives, well over half

of the participants surveyed cited an increase in their security budget earmarked for endpoint security with almost the same percentage of respondents stating that have purchased new products in the last year.[1]

Advanced Endpoint Threat Protection Must-haves

The bar for a truly advanced endpoint security product is high given the need to provide both breadth in device coverage and depth of functionality at a reasonable cost of ownership.

Early stage, emerging, and established vendors alike are all working to meet a rich set of requirements, which includes the following:

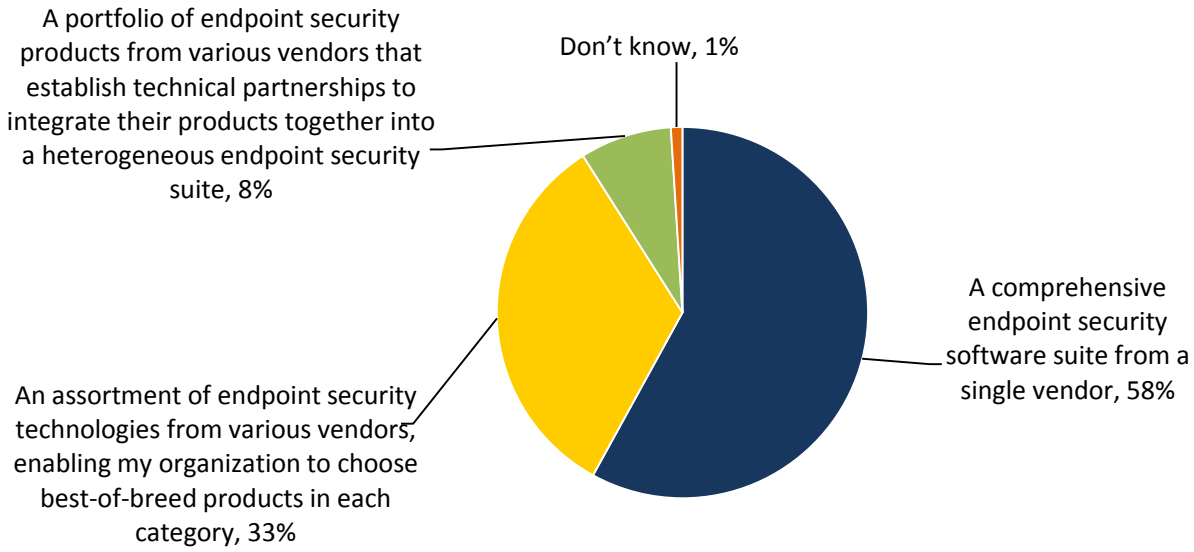
- **Detection of Known and Unknown:** In addition to stopping "known bads," advanced solutions will also detect previously unknown threats with methods such as reputation ratings, behavior-based heuristics, static/dynamic file analysis, and more.
- **Wide-ranging Threat Lifecycle Prevention and Detection:** Contemporary endpoint security solutions must prevent and detect malware and exploits and allow for automated response capabilities including quarantining, remediation, and forensics.
- **Broad Platform Support:** The multi-device end-user and the increasing relevance of Mac OS X in business means support for Windows, Mac, iOS, and Android are needed to eliminate the need for multiple solutions. If an organization's definition of endpoint includes servers, then support for Linux is also important.
- **Coordinated Depth in Defense via Integrations:** To expedite detection and response from endpoint to network and vice-versa, advanced solutions will integrate with network sensors and controls, SIEMs, and analytic platforms, as well as threat intelligence sources via standards such as STIX/TAXII, OpenIOC, and CEF.
- **Operationally Efficient:** In addition to an easy-to-install, lightweight agent, customers should have the option of deploying an on-premises management server or subscribing to a cloud service to alleviate management tasks associated with scaling the management server and setting it up in a high-availability configuration.

Furthermore, 58% of the respondents in the aforementioned ESG research stated a desire to procure a comprehensive endpoint security suite from a single vendor (see Figure 2).[2] This data reflects the need for improved security efficacy and operational efficiency from a single endpoint security solution.

[1] Source: ESG Research Report, *The Endpoint Security Paradox*, January 2015.
[2] Source: Ibid.

Figure 2. Type of Endpoint Security Technology Approaches Most Attractive to Organizations

As new endpoint security requirements arise and your organization considers new endpoint security controls and analytics, which of the following choices do you think would be most attractive to your organization? (Percent of respondents, N=340)



Source: Enterprise Strategy Group, 2015.

Webroot Aims to Provide Efficacy Without Impact

Webroot SecureAnywhere Business Endpoint Security is a good example of what customers require in an advanced endpoint threat protection solution, employing a four step process to detect the known, vet the unknown, and remediate infected systems back to a good state. Webroot's four steps include:

1. **Detect Known Bad Files:** While CISOs are focusing their attention on advanced and targeted threats, pedestrian malware grows more voluminous and problematic every day. To address this continual annoyance, endpoint security solutions must be built on a foundation of strong antivirus protection. Webroot SecureAnywhere includes such basic antivirus capabilities with an efficient implementation. To maximize system performance and remain transparent to users, SecureAnywhere eliminates the need to perform file system scans by employing its cloud-based software reputation service, BrightCloud, to identify known good and bad software. By comparing cryptographic hashes with BrightCloud, known bad software is prevented from executing, reducing the overall attack surface.
2. **Identify Known Bad Behaviors:** The introduction of zero-day malware and exploits and targeted attacks perpetrated by spear-phishing, drive-by downloads, and other methods necessitates advanced approaches to protect endpoints from compromise. In addition to static analysis, dynamic analysis is effective to detect bad behavior. Unknown files not previously seen in Webroot's customer base, and not yet cataloged in its threat intelligence database, are analyzed dynamically by running the new executable with an eye toward detecting suspicious behaviors, which, if observed, result in that file being blocked.
3. **Detect Unknown Bad Files:** Executables that are not known to be bad and that do not initially exhibit malicious behavior could, in fact, be stealthy malware attempting to evade detection, but blocking all such files would impede

end-users' productivity. As such, advanced endpoint security solutions will allow the file to execute while it is being further analyzed, with the ability to roll back to a known good system state should the new file be determined to be malicious. SecureAnywhere allows files that are neither known nor exhibit suspicious behavior at initial runtime to execute in a protected mode during which a journal of intercepted system calls is created. This approach allows high-risk post-execution actions such as data exfiltration to be disabled until a verdict on the file has been rendered.

4. **Remediate and Close the Intelligence Loop:** Infected endpoints also present an operational tax in the form of the time it takes to reimage contaminated machines while end-users lose valuable time. Modern endpoint security solutions will remediate by returning the system to its last known-good state and share the new threat intelligence information with the community. If a file is ultimately determined to be malicious by SecureAnywhere, all system changes (i.e., registry settings, processes, file downloads, etc.) are reversed and its markers are added to Webroot's BrightCloud threat intelligence service to enable detection in step one the next time it is seen by a Webroot customer.

By meeting these requirements, Webroot employs a smarter approach to endpoint security by allowing users to continue to work uninterrupted while the trustworthiness of files are evaluated. Webroot's BrightCloud Threat Intelligence service effectively leverages the cloud to not only aggregate threat information but also make the latest such intelligence available to all subscribers, thereby increasing efficacy. This use of cloud-delivered intelligence brings into question the need for traditional, signature-based AV, although some organizations may choose to stay the course with AV for defense in depth on the endpoint. Webroot SecureAnywhere Business Endpoint Protection hits other must-haves with broad device support, a lightweight agent for high performance, and a cloud-hosted management console that should effectively lessen operational cost.

The Bigger Truth

The endpoint is often the point of infection in an organization, with adversaries exploiting multiple vulnerabilities to gain a foothold from which to move laterally and gain access to data assets. With signature-based antivirus proven as ineffective against advanced malware and exploits, today's threat landscape has necessitated the use of additional endpoint security controls to mitigate risk associated with the endpoint soft spot. What is required to address the threats of today and tomorrow are endpoint security products that meet the requirements of a truly advanced, next-generation solution. Webroot's SecureAnywhere Business Endpoint Protection covers these bases, representing a solution organizations may want to consider as part of their evaluation of the endpoint security process, policies, and products.