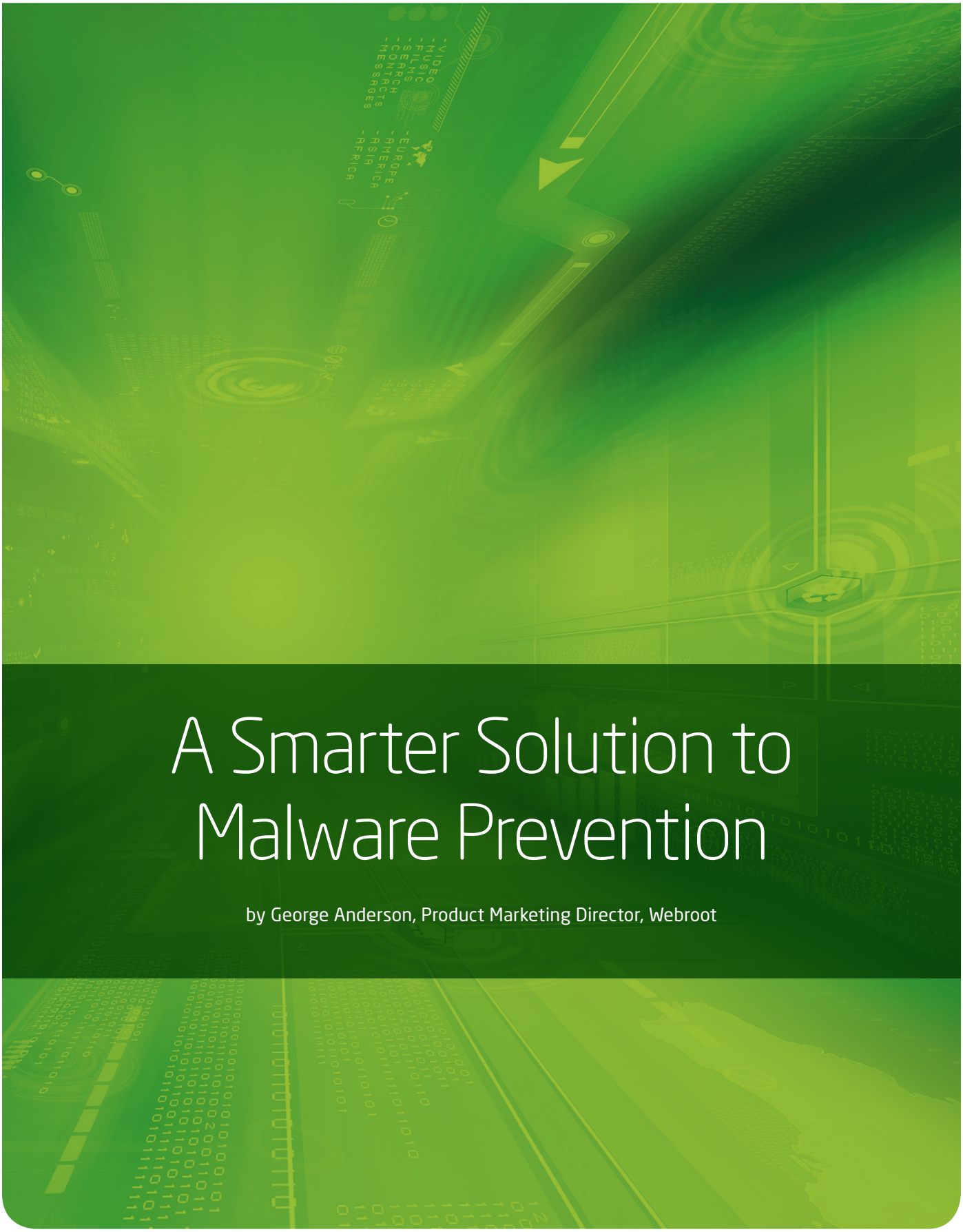
WEBROOT
Smarter Cybersecurity™



A Smarter Solution to Malware Prevention

by George Anderson, Product Marketing Director, Webroot

CONTENTS

INTRODUCTION

Traditional endpoint security has failed to keep up with today's threats and is exposing organizations to unacceptable levels of risk. It's time for smarter, next-generation malware prevention to replace traditional defenses. New approaches to malware can wrest back control and give security administrators greater visibility and control over their endpoints at a lower cost than traditional solutions.

This paper looks at the endpoint threats organizations are facing, the means to combat those threats, and why next-generation, cloud-driven protection offers the smartest way to prevent endpoint malware infections.

TODAY'S ENDPOINT THREAT LANDSCAPE

Endpoint security effectiveness began to diminish as far back as 2006, when cybercriminals began using basic malware variant automation tools. Since then, there has been huge growth in the appearance of new malware and threat variants.

To give that growth context, AV-Test.org, a well-known security testing organization, charted the rise of new malware variants every year starting in 1984. In 2005 there were under 1 million new malware variants appearing each year; in 2007 there were 6 million; in 2010 there were about 18 million; and by 2016 there are now over 140 million new malware threats per year and rising.

Fully automated exploit tools became readily available around 2010, leading to the accelerated growth seen in new malware variants over the past 5 years. By December, the count for 2015 reached over 142 million malware variants, meaning new malware hitting the internet at over 16,250 threats per hour!

Traditional antivirus uses signatures to stop malware. To build a detection signature a system must first be infected with a specific malware variant so the antivirus vendor can then research the threat and a signature. Only then can that vendor push that signature to its clients to stop the given threat and its close variants. This process is time-consuming, and creates a large window of vulnerability between when an infection compromises an endpoint and when the signature is available. The sheer volume and variety of new malware renders the signature detection approach untenable. And, considering that many new malware variants target fewer than 50 endpoints, the likelihood of an antivirus vendor having access to a sample in the first place is minuscule.

New, unknown, zero-day malware attacks present numerous challenges for conventional antivirus solutions and force their efficacy down to about 45%[2]. According to Brian Dye, Senior VP for Information Security at Symantec, "55% of cyber-attacks go undetected by commercial software. Cybercriminals now regularly leverage zero-day exploits and custom built Trojans to achieve their ends."

According to industry research published at the end of September 2014 many enterprises have little confidence in the efficacy of antivirus software alone. 62%[3] of enterprise security professionals strongly agree or agree that antivirus software is ineffective at blocking advanced malware. Part of that lack of confidence is due to the different threat vectors available for malware to infiltrate endpoints. Of particular note over the past few years has been the success of spear phishing attacks, in which an email message appears to come from a trusted source or a colleague but contains a link that, if followed, immediately infects the endpoint. For spear phishing to work, the source must appear known and trusted, with legitimate information in the email that supports its validity, and the request must also seem to have a logical basis. Unfortunately, the technique is highly effective, requiring only an average of 12 targeted emails for a greater than 95% success rate. Worse yet: an astonishing 62%[4] of breaches go unidentified for months.

Antivirus vendors have tried to deal with the pitfalls of signature detection by utilizing other detection methods like port controls, application whitelisting, and more advanced malware detection. Advanced malware detection uses different types of file and process analysis, such as emulation and sandboxing. But what antivirus vendors have really done is to use a combination of signature-based detection methods to cover known malware and exploits like viruses, worms, spyware, bots, Trojans, buffer overflows, and blended attacks, then added reputation-based detection, using emulation and code analysis coupled with behavioral runtime analysis.

There are a lot of security layers in a modern antivirus client, and through this revised approach, traditional antivirus is better able to identify malware infections. Nonetheless, even with these added defenses, the old problem remains: it takes too long to stop malware, and the resources consumed on each endpoint to identify malware negatively affects system performance dramatically.

This lack of success has seen the arrival of many new ways to counter malware from non-traditional antivirus vendors—including Webroot. Not only can some of these newer solutions replace traditional defenses, but many are also designed to enhance traditional antivirus protection. Webroot combines the new alternative strategies with a unique approach that leverages cloud-driven protection, offering a solution for all types of endpoint malware prevention.

1 AVTest.org, January 2016
2 The Wall Street Journal, May 2014
3 ESG Research: Endpoint Security Survey, September 2014
4 Verizon RISK Report 2013

THE ISSUES WITH TRADITIONAL ANTIVIRUS PROTECTION

Recent ESG research showed that 56%[3] of the companies surveyed have purchased new endpoint security technologies in addition to those used in the past. 85%[3] are planning to increase their endpoint budget somewhat or substantially, while 63%[3] see no single endpoint security vendor delivering a product suite that meets all of their organization's requirements.

Operationally, nearly 30%[3] believe endpoint security requires too many manual processes and almost 40%[3] see security staff spending too much time on high-priority endpoint security issues.

It's clear that current endpoint security from any vendor doesn't totally match market needs, so let's compare and contrast these findings with the issues Webroot customers have had in the past with endpoint security, and whether their concerns also substantiate the ESG survey findings.

Scans and Updates Interfere with User Productivity

Huge strides have been made in the past few years by conventional antivirus vendors to improve their installation, scheduled scanning times and use of local device system resources. However, as annual, independent PassMark[5] Software performance benchmark testing shows, conventional antivirus often continues to hog system resources and slow down users' systems. In the ESG survey, 48%[3] of respondents reported that their antivirus products impact overall performance of endpoint systems (e.g., slow booting, slow system when performing a scan, scans take too long, etc.).

Because of this, some users may disable their endpoint security, while some administrators will avoid running scheduled scans during the day to avoid user complaints. Such workarounds present increased risks for both users and the organizations involved. At best, users still deal with slowed system responses and lost productivity.

Protection and Out-of-date Signatures

Traditional antivirus still relies on regular signature updates. But no matter how quickly these updates are pushed out to endpoints, they are out of date by the time they're installed. Administrators trying to ensure all of their users are completely updated face a logistical nightmare, especially if compliance regulations mandate that all systems remain up-to-date at all times. Consider too the upkeep and costs associated with update servers, the massive bandwidth consumption each time an update is pushed out, and the myriad other issues and costs of ownership and operation. All of these issues are resolved by a cloud-based antivirus solution, as the updates occur over the air and in real time, ensuring users stay protected and compliant with minimal resource usage or operational costs.

High Reimaging and Productivity Loss Costs

Traditional antivirus only offers limited remediation: it can remove the malware but cannot return the system to its pre-infected state, meaning the damage done to the system often requires a total reimage. As such, even remediated infections can still be very costly, as IT personnel have to take the time to remediate or reimage systems, while the affected user's productivity is impacted.

Poor Incident Response and Support

When Webroot still offered conventional antivirus, we constantly battled poor levels of customer satisfaction. The process of gathering log files, waiting for new definition signatures, cleaning up infected machines, and the hours spent on the phone all added up to unacceptably low customer satisfaction—and that's just as true today with conventional antivirus protection. Furthermore, organizations also face high fees for provided support.

One of the best ways to avoid the need for support calls is to proactively build automatic processes and procedures into the agent. Webroot SecureAnywhere solutions integrate support into the agent and management console, making it available 24x7x365 at no additional cost. Customers can leverage the in-product help, decreasing support time and costs, which has led to our customer satisfaction rising to 95%.

Complex, Time Consuming Management

As new malware variants advance and administrators add layers of security, management complexity can become unbearable. The ESG Survey found 26%[3] of respondents stated their antivirus was too cumbersome to configure and manage to its full potential. This complexity results in greater management overhead, often without any significant reduction in infections.

Another facet of operational management is the need for different client agents for different applications. For instance, a desktop requires a different agent than a server or virtual deployment. Thankfully, these issues are also addressed by newer approaches to malware prevention.

THE ISSUES WITH NEW MALWARE PREVENTION

New approaches vary considerably in their capabilities, and Gartner is now categorizing most of them under a new Market Guide heading of Endpoint Detection and Response (EDR), or Endpoint Threat Detection and Response (ETDR).[6]

According to Gartner, this emerging market satisfies the need for continuous protection from advanced threats, as well as significantly improved security monitoring, threat detection, and incident response capabilities.

3 ESG Research: Endpoint Security Survey, September 2014
5 PassMark Software, "Webroot SecureAnywhere® Business Endpoint Protection vs. Seven Competitors", February 2014
6 Market Guide for Endpoint Detection and Response Solutions, 13 May 2014 ID:G00259856

These new approaches are typified by how they record endpoint and network events, store them in centralized databases for analysis, and develop tools to continually search the database and identify tasks that can:

» Improve security to deflect common attacks

» Identify ongoing attacks earlier (including insider threats)

» Respond rapidly to those attacks

ETDRs also help with rapid investigation into the scope of attacks and provide remediation capabilities.

The typical ETDR is primarily differentiated in five ways:

1. The quality and age of the information they collect
2. The correlation and analytics they perform against the information
3. The richness of context, threat, and vulnerability intelligence that is incorporated into the analytics
4. The actionable intelligence that is ultimately derived from the analytics
5. The ability to change the state of the endpoint, i.e., patch, isolate, or remediate

Gartner adds that ideal solutions will provide rapid time to value, with predefined analytics, combined with out-of-the-box threat and vulnerability intelligence feeds that can identify and prioritize input and outputs for indicators of compromise (IOCs) as well as maintenance suggestions to harden endpoints.

These solutions should also fit into Gartner's Adaptive Security Architecture around the four categories of prediction, prevention, detection, and response, while operating within a closed loop of continuous monitoring and analytics.

For most organizations, finding an acceptable time to value can be a concern with ETDR because of the time and resources these newer solutions require. As Gartner points out, "organizations must consider staffing needs to run these tools. They are not set-and-forget functionality and will require a trained security operations staff to get value. If increasing security staff is not an option, then consider outsourcing to emerging [managed security services providers] that specialize in EDR." But what if both of these are not an option or are unaffordable?

Another concern is that many of these solutions rely on other software or infrastructure to be of use, such as security information and event management (SIEM) systems. In addition, they are not all equal at proactive prevention and remediation. In fact, some are very reactive by nature because vendors use them to collect forensics data from infections. Further concerns are that endpoint protection platform vendors are too narrowly focused on detection, resulting in long dwell times, increased damage and delayed incident response times when breaches inevitably occur.[6]

Webroot falls into a hybrid category, operating with the characteristics of an ETDR with real-time monitoring, predicting, detecting, and preventing the impacts of attacks on individual endpoints. Unlike an ETDR, SecureAnywhere solutions offer the same proactive protection, along with a smarter, cloud-based approach that doesn't require costly and burdensome staffing and infrastructure, nor does it have an unclear time to value.

CLOUD POWER VERSUS THREAT SIGNATURES

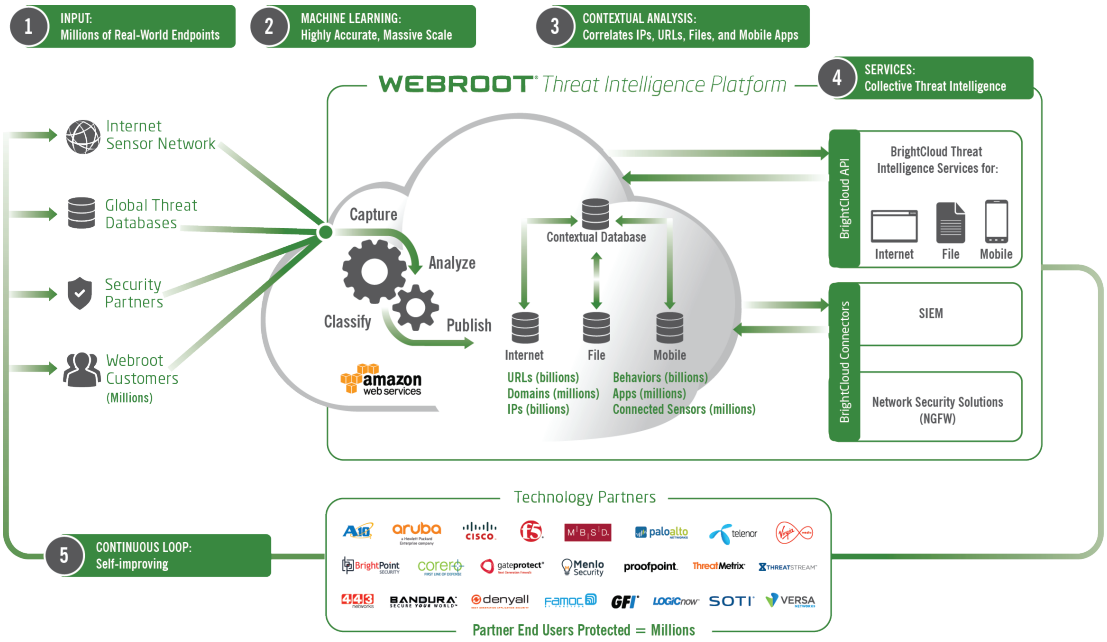
With all the hype around cloud computing and the shift by organizations of all sizes and industries toward cloud-based platforms, many antivirus vendors have jumped onto the cloud bandwagon. For most antivirus vendors, that has meant letting users manage endpoints through a cloud-based management console or moving the update server into the cloud. For the more sophisticated antivirus vendors, it has also meant adding some real-time detection when an endpoint behaves strangely or when users click on malicious URLs. But the fundamental architecture and approach to malware prevention remains the same: capture malware, create a detection signature, update the database on every user's endpoint, and stop future infection attempts by that threat.

Webroot's approach to cloud endpoint protection is completely different. Webroot uses the nearly limitless power of the cloud to leverage big data analytics and Hadoop® and Cassandra™ processing to not only stop known threats but also analyze and predict emerging threat patterns. Our proprietary infrastructure utilizes numerous resources and advanced heuristics to uncover and categorize new files and processes as they execute for the first time on endpoints.

Unlike conventional antivirus that offers generalized protection against malware, Webroot's cloud-driven prevention is automatic and customizable. The high volume and highly targeted nature of today's malware means endpoints need to be protected on an individual basis and cannot rely on a local database of outdated malware signatures. Traditional protection can't help users identify the low-impact, under-the-radar persistent attacks that are rarely recognized and never draw enough attention for detection signatures to be created.

By harnessing the processing power of the cloud, Webroot has moved the heavy lifting involved in malware identification and categorization away from the endpoint and into the Webroot® Threat Intelligence Platform. Using the vast contextual intelligence of the Webroot Threat Intelligence Platform, Webroot solutions can identify and stop malware in real time and make accurate predictions and determinations of whether or not an observed file is malware the moment it tries to execute and infect an endpoint.

6 Market Guide for Endpoint Detection and Response Solutions, 13 May 2014 ID:G00259856



Hadoop® nodes for massive transaction processing with high performance, ultra-fast response times

Cassandra™ Ring – for worldwide high availability Big Data analytics

Big Data Drives Predictive Identification of Malware by the Webroot Threat Intelligence Platform

Webroot® Threat Intelligence Platform

The Webroot Threat Intelligence Platform is continuously updated with collective threat intelligence and contextualized security information from every endpoint running Webroot software. This system allows us to protect all of our customers in real time the moment an infection is encountered on any Webroot-secured endpoint, meaning Webroot solutions become stronger each time an endpoint is added anywhere in the world.

A CLOUD-BASED ANTIMALWARE APPROACH

When you disrupt the status quo, it's only natural to look at your potential weaknesses compared to a traditional, signature-based antivirus methodology.

False Positives

One frequently heard is concern that Webroot solutions might produce false positives, in which the agent flags a harmless file as malicious. However, thanks to the combination of advanced machine learning and human threat analyst involvement, Webroot is able to provide highly accurate threat determinations. Additionally, to help avoid false positives in large or complex endpoint environments, we recommend running the initial deployment in silent audit mode. This allows the agent to categorize unusual or home-grown applications that may incorrectly be categorized as malicious because of their execution permissions. Running silent audit mode can help administrators identify any problem files or processes, legitimate or malicious, without automatically blocking them, giving the administrator the option to whitelist harmless applications that seem suspicious and tailor their Webroot protection.

Offline Protection

Another common query is whether Webroot products protect offline devices. When the agent is offline, the offline policy is enabled, restricting the applications that can run on that endpoint. For instance, a USB containing a threat that previously infected the endpoint would be immediately blocked. Even if the offline policy is not in place, the agent still actively looks for new or highly changed files and processes, which, if detected, will activate the automatic journaling feature, backing up the system in its healthy state, and restricting the activity of the malware. When that endpoint does go back online, the new or changed files are categorized, and if they are found to be non-malicious, they will be marked known good and allowed to run. Any files found to be malicious are immediately be blocked and quarantined, and the automatic rollback remediation will revert the endpoint to its last known good state.

Layered Security

According to the Wall Street Journal and Symantec, traditional antivirus clients run at only 45%[2] efficacy, meaning it's only a matter of time before users get infected. Because of this, many organizations choose to layer endpoint security. This can increase management and cost, in addition to impacting user productivity as various protection solutions compete for system resources. Because Webroot solutions don't rely on bulky signature updates and take up minimal space and resources on an endpoint, they can be run alone or layered alongside other security software without interference.

2 The Wall Street Journal, May 2014

WHY NEXT-GENERATION ENDPOINT PROTECTION IS SMARTER

As Gartner states in their Endpoint Protection Platforms Magic Quadrant 2016, "The cloud lookup results in a very small and fast EPP client. Webroot is the only vendor in this analysis that reports on malware dwell time." That means that Webroot knows when a new infection arrives on any individual endpoint because we prevent malware at the precise time of infection, not later when it's detected by a signature.

Time of detection is the only data that conventional endpoint can report, and that detection time can be seconds, minutes, days, or even months after the endpoint was infected.

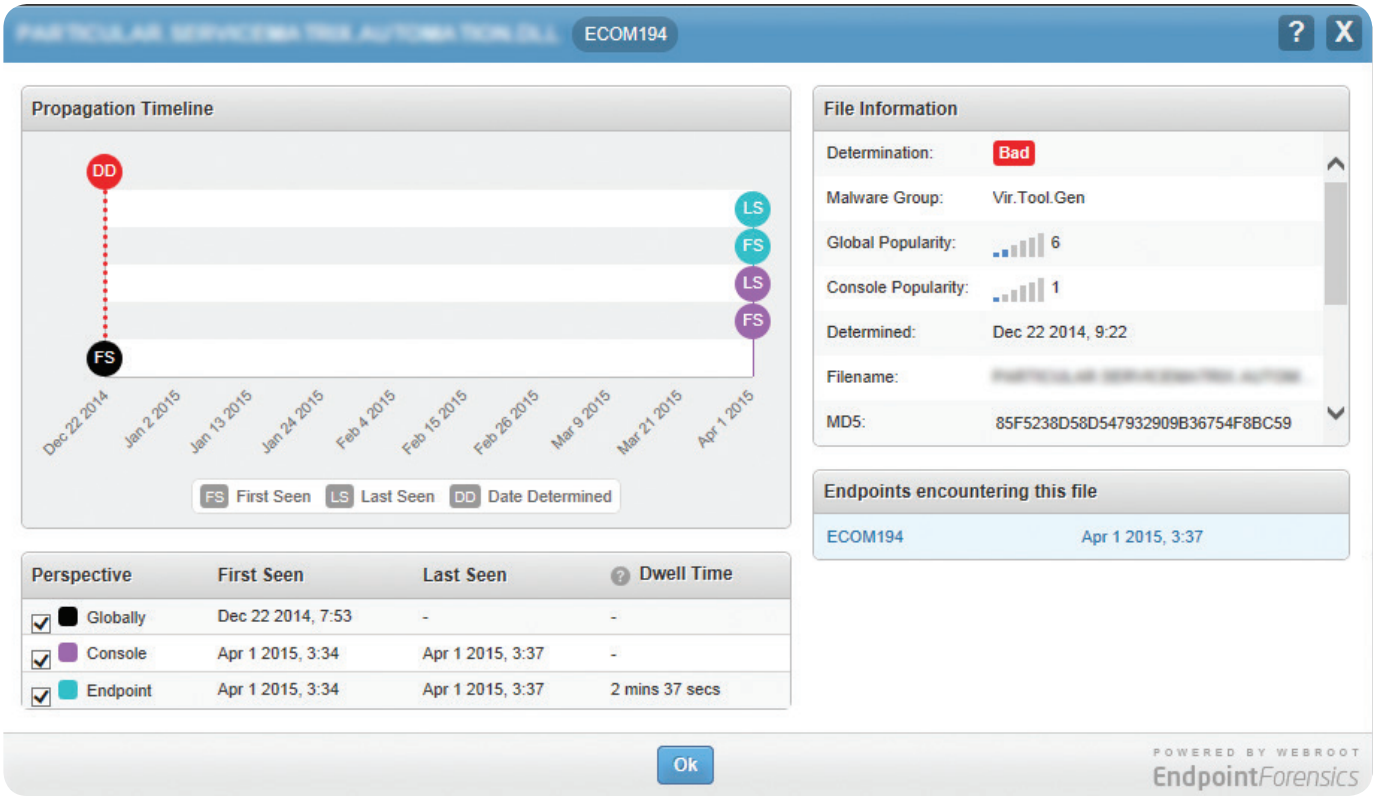
Like other antivirus and antimalware vendors, Webroot is in a constant cyber-battle with malware writers who look at ways to test and defeat our defenses. Even with all the innovation behind the Webroot approach to identifying and stopping malware, we would never be so bold as to claim 100% efficacy. However, what we can say is that our customers categorically confirm the significant reduction in infection rates when using Webroot compared to other antivirus vendors. Per Gartner, "Webroot again received the highest satisfaction scores from reference customers that were contacted for this Magic Quadrant." We deliver real-time, measurable efficacy and minimize the need to reimage users' devices, thereby reducing corresponding IT costs and productivity impact.

Dwell Time

Webroot works at the point of infection, marking the introduction of any new or changed processes, categorizing them as known good or known bad in real time, and our efficacy is currently well over 99.8%. However, the agent is not always able to categorize new unknown or changed processes right away. At that stage, the SecureAnywhere™ agent restricts what these undetermined files and processes can do and starts journaling their activities. In this way, when the agent does categorize these undetermined files and processes, it can either remove the restrictions, or automatically block, quarantine, and remediate any changes made to the system if the undetermined file is later determined to be known bad.

Utilizing the time stamp logs, Gartner mentioned in their Endpoint Protection Platform Magic Quadrant, Webroot now reports dwell time in the following manner:

Dwell time – how long an endpoint has an unknown file or process running



SUMMARY

Any time a newer, smarter solution arrives on the market, it is met with skepticism and resistance. Only through rigorous testing and tentative adoption can the market begin to understand how effective a different approach to an age old plight can be. The IT security market is also particularly conservative with unproven technology. But as malware writers continue to get smarter and more devious, malware prevention systems need to advance at the same rate.

With proactive cloud-based protection that secures in real time, today's organizations can finally begin to do more than keep pace—they can get ahead. At Webroot, we strive to continue our evolution to help consumers and businesses of all sizes do just that. Our solutions deliver highly accurate predictive threat intelligence to detect, remediate and prevent modern malware attacks, keeping users around the globe safe no matter how or where they connect.

About Webroot

Webroot delivers next-generation endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions and BrightCloud® Threat Intelligence Services protect tens of millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, F5 Networks, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
800 772 9383

Webroot EMEA
6th floor, Block A,
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0)870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900