WEBROOT®

Reinventing Antivirus

How cloud architecture and behavior recognition are changing the security game and making traditional antivirus obsolete

Contents

Brought to you compliments of
WEBROOT®

Introduction: Traditional Antivirus is Becoming Obsolete

Have you seen a lot of articles and blog posts with titles like "Is Antivirus Dead?" If so, there is a good reason: Traditional signature-based antivirus technology is rapidly heading toward obsolescence.

But there are new approaches that can make antivirus effective and practical again. Here we will look at three of them:

- Client/cloud architecture
- Behavior recognition
- Journaling and rollback

Together, these three approaches represent a major rethinking of antivirus technology, a major shift in antivirus that creates a new type of technology that is able to detect and counter today's malware.

What's Wrong with Traditional Antivirus?

Traditional antivirus products are based on signature recognition performed on endpoints. That is a failing strategy because:

- The number of recognized threats has grown so huge that it is impractical to keep endpoint systems updated with signatures, and it's impossible for endpoints to compare files against all known signatures.[1]
- Hackers and cybercriminals are using botnets and other techniques to propagate zero-day threats before signatures can be distributed to endpoints.
- Often no signatures at all exist for targeted threats aimed at single individuals or organizations.
- Hackers are using techniques like malware crypters, server-side polymorphism and QA testing (yes, lab testing (to better disguise malware from antivirus packages so they cannot be recognized by signatures.[2]

For these reasons, it is no wonder most information security experts question the ability of signature-based antivirus products to block the newest and most dangerous forms of malware.[3]

Client/Cloud Architecture

The "fat client" architecture of traditional antivirus products relies on heavyweight modules on endpoint systems to compare suspicious files with threat signatures. This configuration has major drawbacks:

- Malware scanning and signature comparisons slow down processing on the endpoint, which reduces productivity, frustrates users and, in some cases, causes users to turn off the antivirus software.
- Thousands of new signatures need to be sent to endpoints, often 5MB per endpoint each day, which eats up bandwidth and requires monitoring by systems administrators.
- In many cases, roaming and remote users are vulnerable to zero-day attacks because they don't get recent signature updates until they connect to the corporate network over a VPN.

A client/cloud architecture fundamentally changes this dynamic. Only a very small client is needed on the endpoint. This client finds new files and creates hashes (signatures) of those files. The hashes are sent to a cloud-based server and compared with a large signature database. Responses are sent back to the endpoint system (see Figure 1 on the following page).

[1] The AV-TEST Institute registers over 75,000 new malicious programs every day and estimates that over 90 million variants exist: http://www.av-test.org/en/statistics/malware/.

[2] *Why relying on antivirus signatures is simply not enough anymore*, Dancho Danchev, Webroot, February 23, 2012: http://blog.webroot.com/2012/02/23/why-relying-on-antivirus-signatures-is-simply-not-enough-anymore/.

[3] See, for example, *Antivirus: Dead, Dying, or Here to Stay?* Dave Shackleford, IANS Research, January 6, 2012: http://www.iansresearch.com/blogs/ians-perspective/antivirus-dead-dying-or-here-stay; and *Is Antivirus Becoming Obsolete?* Ken Presti, CRN Magazine, October 3, 2012: http://www.crn.com/news/security/240008434/is-antivirus-becoming-obsolete.htm.

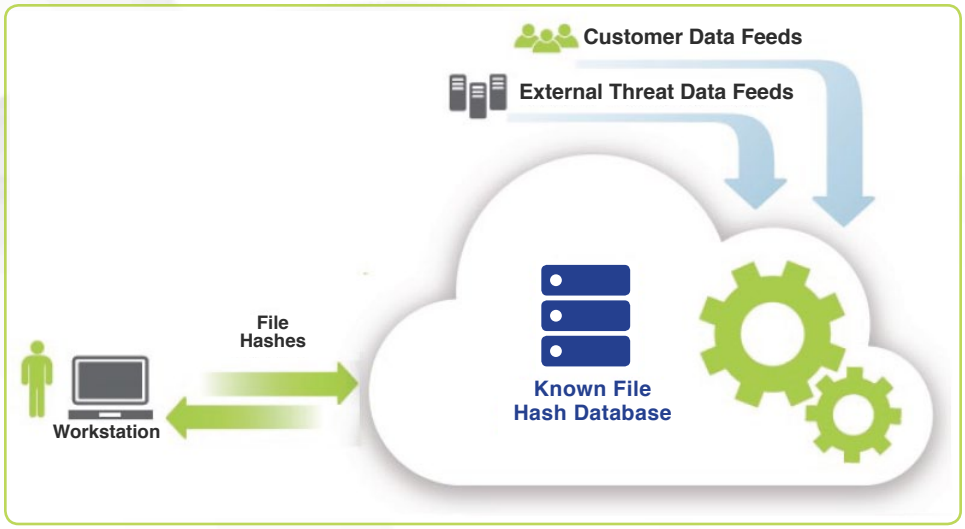

Figure 1: A client/cloud architecture can off-load signature-matching to the cloud, eliminate large signature file downloads and better protect remote users.

The client/cloud architecture has tremendous benefits over traditional antivirus products:

- Very little processing takes place on the endpoint, so there is no impact on end-user productivity.
- There is no appreciable impact on bandwidth usage or network performance, since only a few dozen hashes per system are exchanged over the network (typically about 120KB per day) instead of thousands of new threat signatures.
- The cloud-based system can host huge signature databases and use massive servers to perform pattern matching, so signature comparisons are more complete and faster.
- The cloud-based system gets real-time threat data feeds from test laboratories, antivirus clearinghouses, security vendors, thousands of enterprises and millions of users, so zero-day threats can be blocked as soon as they are identified.
- Roaming and remote users can be protected from zero-day attacks as soon as they connect to the Internet.
- Systems administrators don't need to spend time installing fat clients or distributing signature updates to every endpoint system.

Fat-client antivirus products are effectively obsolete. A client/cloud architecture is the *only* way to make real-time signature-matching practical and effective.

Behavior Recognition

But even the fastest and most comprehensive signature matching will not catch zero-day and targeted attacks for which no signatures exist.

The key innovation to address these threats is behavior recognition — coupled with a client/cloud architecture.

Behavior recognition technologies allow programs to execute in a safe "sandbox" and watch for behaviors that are typical of malware — for example, editing registry keys, accessing email distribution lists or trying to disable anti-malware packages.

But this process is not as simple as it first sounds. The patterns of behavior that separate malicious from benign can be complex. Those patterns need to be captured and compared against a large database of threat behaviors. And to be effective, the behaviors database needs to be updated continuously.

Figure 2 shows how behavior recognition can be implemented with a client/cloud architecture. In this process:

1. Unknown applications and executable files are executed in a sandbox on the endpoint system.
2. File opens, reads and writes, registry key changes and other activities are recorded, and behavior data (the list of activities) is sent to the cloud-based server.
3. The behavior data is compared with a large database of malware behavior patterns and analyzed by a set of rules (heuristics) that help determine whether the behaviors are benign or malicious.
4. Responses are sent back to the endpoint system, indicating which programs should be quarantined and which should be allowed to execute.

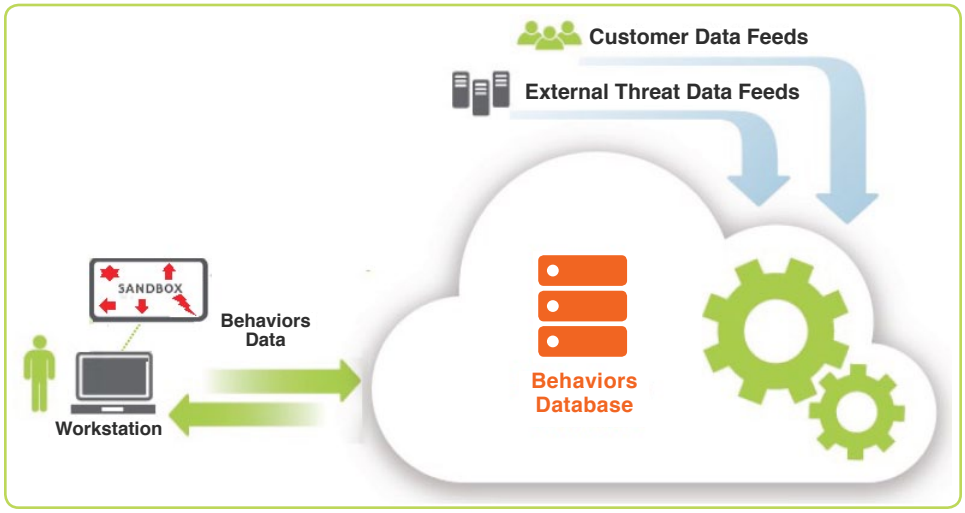

Figure 2: Behaviors are captured in a safe sandbox and compared against malware behavior patterns and rules.

This approach identifies malicious programs by their actions, even when no signatures exist.

And because the pattern and rule analysis is done on the cloud system, there is no impact on endpoint performance and checking can be done against an extremely large behaviors database. Further, data from new threats is available immediately from external sources, and newly discovered behavior patterns can be used right away to protect everyone else.

Journaling and Rollback

But even behavior recognition is not enough if it is only *short-term* behavior recognition. Some malware writers are clever enough to delay the onset of malicious behavior so it doesn't appear in the sandbox right away.

So the third element of reinvented antivirus is long-term behavior analysis combined with journaling and rollback.

With this approach, programs are allowed to execute, but modifications to files, registry keys, memory locations and other entities are journaled. This allows the software to create a "before" and "after" picture of each change.

If behavior analysis identifies the program as malicious, the program can be deleted and all of the changes it made can be rolled back, returning the endpoint to a known good state.

This approach:

- Mitigates the effect of malware that cannot be detected by signature-matching or short-term behavior recognition.
- Eliminates huge amounts of work cleaning up and re-imaging infected systems — which surveys show can consume as much as one-third of the support staff's time.
- Makes it possible to recognize the same threat on other systems, and at other enterprises.

How Webroot Puts the Pieces Together

Has anyone implemented these concepts, and do they perform as advertised in practice?

Yes. All three approaches are used in Webroot® SecureAnywhere™ Business - Endpoint Protection. Here we discuss how it works (shown in Figure 3 on the following page) and the results.

Webroot SecureAnywhere Business - Endpoint Protection uses an agent of less than 700KB on endpoint systems, which can be installed in under six seconds (as measured by independent test lab PassMark Software). This contrasts with fat clients of hundreds of megabytes used by traditional antivirus products, which typically take three minutes or longer to install.[4]

Test results show that the client/cloud architecture can dramatically change the impact of antivirus software on endpoint system performance.

[4] The performance figures in this section are from PassMark Software, Webroot SecureAnywhere Endpoint Protection Cloud vs. Seven Traditional Endpoint Security Products, updated February 2012: http://www.webroot.com/En_US/sites/land-business-migration/. See also PassMark Software, 2012 Consumer Security Products Performance Benchmarks, Edition 4, updated April 12, 2012: http://www.passmark.com/ftp/totalprotectionsuites-apr2012.pdf.

When PassMark Software tested eight popular antivirus products for scanning times, Webroot, with its client/cloud architecture, was by far the fastest. A complete initial system scan took only 50 seconds, which was less than half the time it took the second-best product and only 40% of the average time (two minutes and four seconds). Memory usage during the initial scan was 12MB, which was only 21% of the second-best product's usage and barely 10% of the average (120MB). Memory usage during system idle was 4MB, which was only 6% of the average.

The cloud component of SecureAnywhere Business - Endpoint Protection is the Webroot Intelligence Network. This provides over 75 terabytes of signature, behavioral, "bad URL" and other threat data. That is orders of magnitude more than can be managed by fat-client products on endpoint systems. This means that Webroot can detect far more malware variants and can effectively utilize behavior recognition.

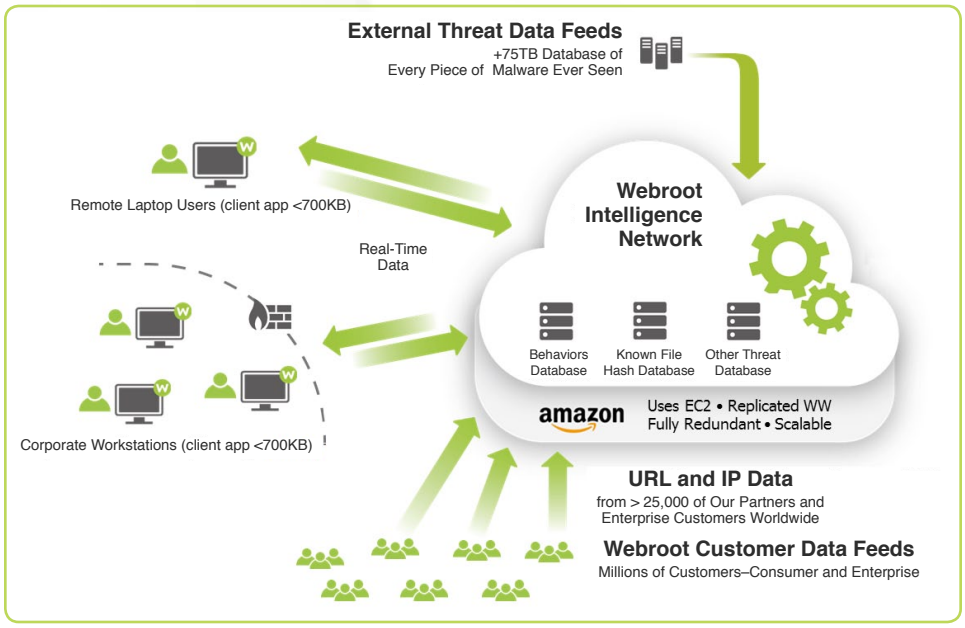

Figure 3: Webroot's client/cloud architecture and the Webroot Intelligence Network

The Webroot Intelligence Network is updated constantly with input from over 25,000 partners and enterprise customers, and millions of consumer customers, so both remote and headquarters users have immediate access to threat data as soon as it is available.

Finally, the Webroot Intelligence Network infrastructure uses fully redundant cloud resources located around the globe to provide the highest levels of reliability and the lowest latency.

Conclusion: See it Yourself

Traditional signature-based antivirus is obsolete. But there are fresh new concepts that can make anti-malware effective again. This paper discussed three of them:

- Client/cloud architecture
- Behavior recognition
- Journaling and rollback

Together, these approaches can improve performance, detect a far wider range of malware and dramatically reduce the time systems administrators and support staff spend distributing signature updates and cleaning infecting systems.

But this is not an academic discussion. You can see these concepts working in your own environment.

For more information,
please visit http://www.webroot.com/En_US/business/secureanywhere-endpoint/.

For a free trial of SecureAnywhere Business - Endpoint Protection,
go to http://www.webroot.com/En_US/business-trial.html.