Closing the Circle

How to get manageable endpoint, mobile device and web security together

Contents

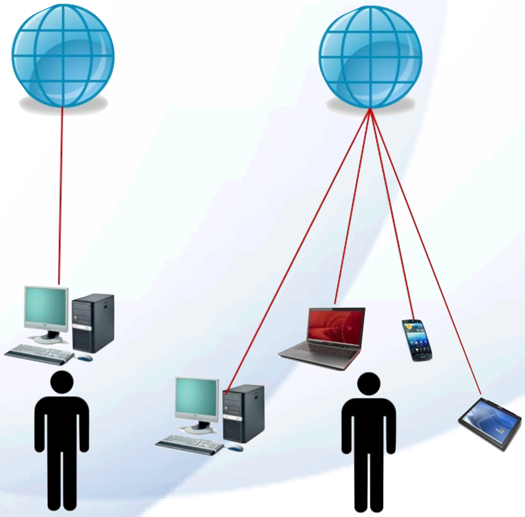
Brought to you compliments of WEBROOT

1 Closing the circle: Why you need to protect endpoints and mobile devices together

Endpoint protection has gotten more complicated

Endpoint protection has never been easy, but it once was at least straightforward. Workers had one computer, used the corporate email system and visited only a few websites while at work.

Today, endpoint protection is far more difficult. Many employees:



- Have two, three or four Internet-connected devices containing sensitive company information.
- Use several corporate and non-corporate email and collaboration programs.
- Spend hours every week on social media, entertainment, shopping and other non-business websites, many of which may be infected with malware.[1]

[1] In a recent Salary.com survey, 11% of employees reported spending more than five hours per week on non-work-related websites during work hours, and another 21% spent two to five hours: http://www.salary.com/wasting-time-at-work-2012/.

Now IT departments are faced with the challenge of protecting a wide range of devices, including desktop computers, laptops, tablets and smartphones, many of which operate outside of the company firewall.

In addition, IT groups must assume that employees are being exposed to malware and threats through many avenues, including non-corporate email and collaboration systems, social media websites and even legitimate websites that have been infected with malware.[2]

Further, many of today's most dangerous threats, such as advanced persistent threats, don't rely on a single method of attack — say, sending malware files as email attachments. Instead, they combine several. A cybercriminal might send a phishing email that lures an employee to a website, that employs a "drive-by download" to infect the employee's PC with a piece of malware, that sends user IDs and passwords out to a server controlled by the cybercriminal. Relying on endpoint protection alone may not be enough to stop these complex threats.

In this white paper we will discuss:

- Why traditional endpoints and mobile devices require overlapping (but not identical) security solutions.
- How to enhance the protection of all endpoints by adding web security.
- Why today's threats require that endpoint protection and mobile device protection activities be moved to the cloud.
- How Webroot makes it easy to "close the circle" by managing endpoint protection, mobile device protection and web security through one infrastructure.

2 Endpoints and Devices: Security Is Overlapping but Not Identical

Differences between laptop and mobile device security

The security requirements of desktop PCs and laptops overlap with those of smartphones and tablets, but they are not identical. That's why different endpoint protection products are needed, and why managing both sets of requirements through the same infrastructure provides major benefits.

PCs and laptops are subject to millions of malware variants, including viruses, worms, Trojans, rootkits, keyloggers, spyware and adware.

Signatures are available for most of these. However, every day another 130,000 malicious programs are being added to that count, often taking the form of zero-day attacks that spread before signatures can be developed and distributed.[3]

[2] One security lab reported finding 30,000 new infected webpages every day, more than 80% of which were on "innocent" web servers that had been hacked: http://www.sophos.com/en-us/press-office/press-releases/2012/01/security-threat-report-2012.aspx.

[3] The AV-TEST Institute registers 130,000 new malicious programs every day and estimates that almost 110 million variants exist: www.av-test.org/en/statistics/malware.

Return to top

For these reasons, endpoint protection solutions for PCs and laptops should include:

- The ability to quickly compare suspect files with millions of signatures.
- Heuristics and behavioral analysis to identify zero-day attacks and unknown malware variants.
- Mechanisms to block keyloggers, screen scrapers, browser hijacks and other methods of stealing employee passwords and account information.
- An application firewall to prevent questionable outbound traffic from malware to servers controlled by cybercriminals.
- Tools to prevent malware-infected files from being loaded from USB drives, CD/DVD drives and other local storage devices.

Mobile devices such as smartphones and tablets are not subject to as many threats as PCs and laptops (at least today), but worms, Trojans and spyware are beginning to appear.[4]

In addition, mobile devices have their own vulnerabilities, including “apps” that contain malware (often disguised as games or utilities), exposure to eavesdropping on communications, man-in-the-middle attacks and a high propensity for being lost or stolen.

For these reasons, mobile protection solutions need features like:

- The ability to detect and block malware specific to mobile devices.
- The ability to scan apps and their permissions.
- Alerts to notify administrators if users have disabled settings needed for good security.
- The ability to lock and wipe devices if they are lost or stolen.

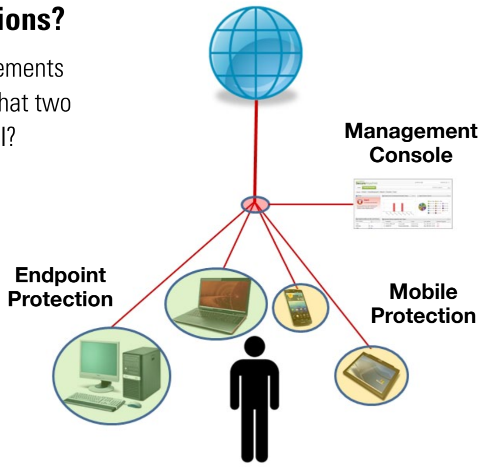
And these features need to work effectively with far fewer memory and processor resources than would be available on a PC or laptop.

Separate endpoint and mobile solutions?

If PCs and laptops have different security requirements than smartphones and tablets, does that mean that two separate products are needed to protect them all?

No. The *features* that protect the devices need to be different, but the *management tools* can be the same.

The table overleaf shows the advantages of having a single management platform for PCs, laptops and mobile devices.



[4] The U.S. Government Accountability Office estimated that the number of malware variants aimed at mobile devices grew by 185% between mid-2011 and mid-2012, to over 40,000. The agency also noted one botnet reportedly capable of infecting 10,000 to 30,000 mobile devices per day. See http://www.gao.gov/products/GAO-12-757.

	Separate Solutions	Single management platform
Learning curve	Administrators need to learn two management tools	Administrators need to learn only one management tool
Deployment	Two deployment processes	One deployment process
Management and reporting	Separate management and reporting consoles	"Single pane of glass" for management and reporting
View of employees	Divided view of the devices of individual employees	Visibility into all devices of each employee

3 Endpoint Protection and Web Security: The Value of Layers

Because many of today's most dangerous threats blend several methods of attack, endpoint protection and mobile device protection need to be supplemented by a second layer of security: web security.

Functions of a secure web gateway

Web security is provided by a secure web gateway product or service. A secure web gateway inspects web traffic at the gateway between the Internet and a company's network, or in the case of laptops and mobile devices, between the Internet and the devices.

Secure web gateways help companies protect themselves from web-based malware, enforce Internet acceptable-use policies and manage web usage.

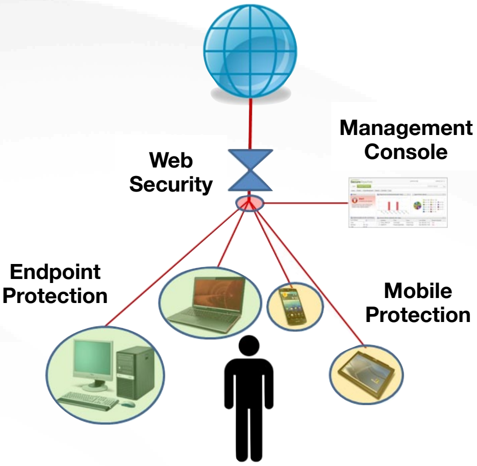
Key security and management capabilities include:

- Scanning HTTP traffic and blocking malware and spyware before they reach the company network and endpoints.
- Detecting and blocking phishing attacks.
- Monitoring webpage requests and preventing users from reaching websites likely to contain malware (URL and content filtering).
- Enforcing company policies by limiting access to social media sites, gambling and pornography sites, shopping and job search sites, online games and other non-work-related websites.
- Enforcing activity quotas that limit the amount of time individuals can spend online or the number of megabytes they can download in a day.
- Reporting web usage, so managers can look at overall web usage and patterns of visits to dangerous or time-wasting websites.

Return to top

Security implications

The ability of secure web gateways to control and monitor web usage has very important security implications, because:



- Gambling and pornography sites are notorious for being infected by malware and spyware, and even social networking sites are often compromised.[5]
- Cybercriminals are increasingly using social media websites to gather information that can be used for spear-phishing and social engineering attacks.
- Blended attacks and advanced persistent threats that count on luring employees to websites controlled by attackers can often be foiled by controls over web visits.
- Managers can use reporting to identify users who engage in risky or inappropriate behaviors on the Internet.

Beyond security, secure web gateways also help companies improve productivity, control bandwidth usage and demonstrate compliance with government regulations.

4 The Crucial Innovation: Move Intensive Processing to the Cloud

Why traditional antivirus is failing

We have explained why protecting endpoints today requires complementary endpoint protection and mobile device protection solutions, together with an additional layer of web security.

However, some readers may question this approach when many experts are debating whether traditional antivirus products have failed.[6]

Indeed, many antivirus and endpoint protection products do have serious shortcomings. Most notably, they are dependent on downloading large files of threat signatures and on performing extremely resource-intensive scans to compare files with millions of signatures. This means:

- They require software modules on the endpoint systems that are large and difficult to install.
- Scans are slow and interfere with employees' work.
- It is almost impossible to update endpoints fast enough to protect against zero-day threats.

[5] By one estimate, 40% of social network users have been attacked by malware: http://techland.time.com/2011/03/23/40-of-social-network-users-attacked-by-malware/.

[6] For example, see: "Is Antivirus Becoming Obsolete?" Ken Presti, CRN, Oct. 12, 2012: http://www.crn.com/news/security/240008434/is-antivirus-becoming-obsolete.htm.

Mobile devices suffer from different issues, most notably a lack of memory and processor resources to perform signature matching and other security activities on the devices.

But the traditional approach to endpoint protection is not the only solution available.

Innovation: Pattern matching and analysis in the cloud

The solution to the shortcomings of traditional antivirus and endpoint protection products is to move the heavy lifting of signature matching and behavior analysis into the cloud.

Moving resource-intense activities to large servers in the cloud means that:

- Only a small and easily installed client module is needed on the endpoints.
- Large threat signature files don't need to be distributed to every endpoint every day.
- Resource-intensive signature matching and pattern analysis processes can be handled very quickly by large servers in the cloud, without slowing the endpoints or interfering with employees' work.
- Advanced technologies can be used to protect mobile devices that offer very few free resources themselves.
- Information about zero-day attacks can be utilized immediately, without having to be sent to endpoints.
- A consistent set of security processes can be implemented for PC and laptop endpoint protection, mobile device protection and web protection.

Of course, it's not easy to shrink client modules and move processing to the cloud. In fact, so far, only one technology company has done it successfully for an enterprise-quality set of endpoint protection solutions: Webroot.

5 Closing the circle: How Webroot makes it easy to combine endpoint protection, mobile device protection and web security

Webroot is the first technology company to offer the combination of:

- Endpoint protection and mobile device protection managed from one console.
- Industry-leading web security services from the same vendor.
- A client-cloud architecture that simplifies deployment and management, and delivers superior malware protection.

Endpoint protection — ultimate performance with minimal management

Webroot SecureAnywhere™ Business – Endpoint Protection is an extremely sophisticated but easy-to-manage endpoint protection solution for Windows PCs and laptops. It features:

- The world's smallest endpoint security client module (less than 750 KB), which is extremely easy to deploy and initially scans PCs and laptops in six seconds or less.
- The lowest memory usage and the fastest installation time, boot time and scheduled scan time of any of the most popular endpoint protection products.[7]
- Extremely effective detection of known and unknown malware, through pattern matching, advanced heuristics and behavior recognition technology, predictive intelligence and over 100 TB of malware data.
- Security "shields" that block keyloggers, screen scrapers, browser hijacks and other methods of stealing employee data.
- An application firewall to prevent outbound traffic to servers controlled by cybercriminals.
- Tools to prevent malware-infected files from being loaded from USB drives, CD/DVD drives and other local storage devices.
- Remediation and rollback capabilities to remove threats and return endpoints to previous safe states.

Mobile protection — security and management of mobile devices

Webroot SecureAnywhere™ Business – Mobile Protection helps companies protect and manage iPhones®, iPads® and Android™ devices. Key features include:

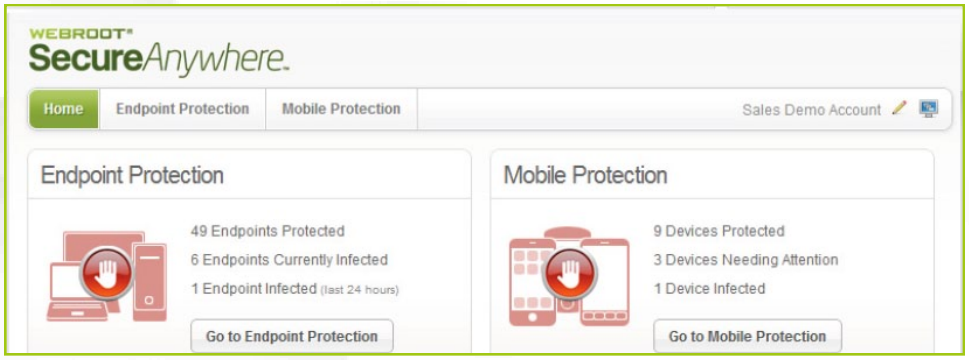
- Simple over-the-air deployment from a central web-based console.
- Detection of viruses, Trojans and spyware on mobile devices.
- Security shields that prevent malware from being installed.
- Alerts to notify administrators if users have disabled settings needed for good security.
- Remote locking and wiping of devices if they are lost or stolen or if a device's SIM card is removed.
- A small client module that runs unobtrusively and uses minimal memory and battery resources.

One management console for endpoint protection and mobile protection

Webroot SecureAnywhere™ Business – Endpoint Protection and Webroot SecureAnywhere™ Business – Mobile Protection are both managed from the same web-based console.

That means administrators need to learn only one management tool, and can take advantage of a "single pane of glass" for deploying and managing endpoint and mobile device protection.

[7] "Webroot SecureAnywhere Business Endpoint Protection vs. Seven Competitors," PassMark Software, January 2013: http://www.webroot.com/shared/pdf/Passmark_Endpoint_2013.pdf.



Endpoint Protection

49 Endpoints Protected
6 Endpoints Currently Infected
1 Endpoint Infected (last 24 hours)

Mobile Protection

9 Devices Protected
3 Devices Needing Attention
1 Device Infected

Web security — the layer in front

Webroot Web Security Service provides the additional layer of security to block malware before it reaches the company network, and to control employee access to non-business websites. Its capabilities include:

- Multiple heuristic filters to detect zero-day attacks and malware from websites and web-based email systems.
- Industry-leading real-time antiphishing technology that identifies new phishing sites hours or days ahead of other antiphishing products.
- URL and web content filtering based on over 310 million web domains divided into more than 83 categories.
- Internet access controls that allow administrators to create custom access policies for departments, groups and even individuals, and to demonstrate compliance with acceptable-use policies.
- Quota policy support that allows administrators to place limits on bandwidth consumption, time spent online and number of sites accessed.
- Logging and reporting that provides information on topics such as web traffic trends, top blocked URLs, blocked malware and individuals visiting suspicious websites.

Unique client-cloud architecture

Webroot is the first company to provide endpoint protection, mobile device protection and web security all designed with a client-cloud architecture.

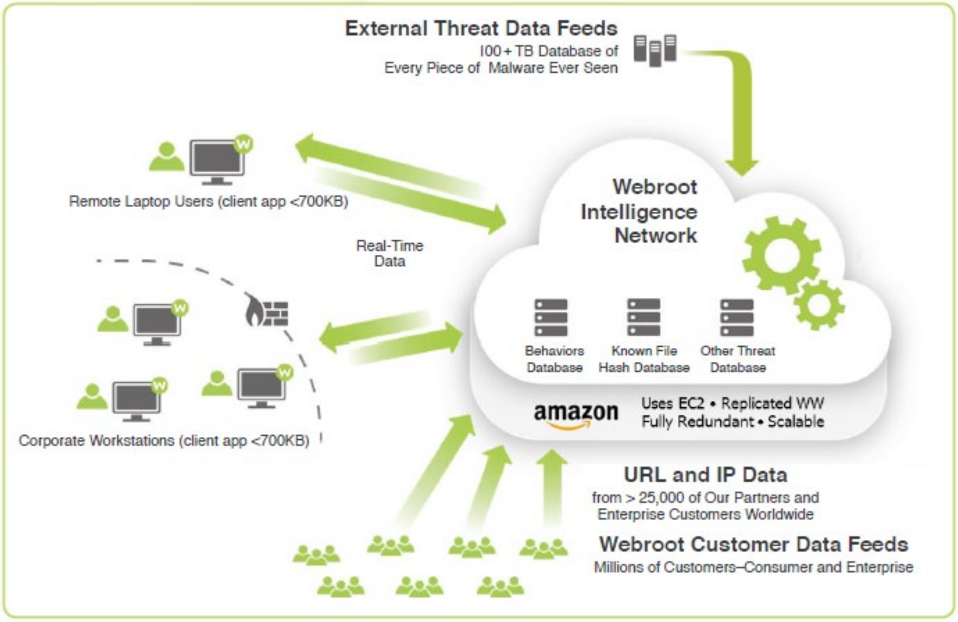
This architecture allows for extremely small client modules that can be deployed quickly and easily, and that have minimal impact on the performance of the endpoint and mobile devices.

When a new file is downloaded or installed on a PC, laptop or mobile device, the client module does not try to perform signature matching and behavior analysis on the endpoint system. Instead, it simply creates a hash of suspicious files, or a summary description of behaviors like file opens and reads and registry changes, and sends this data in real time to the Webroot Intelligence Network in the cloud.

The Webroot Intelligence Network performs the heavy lifting of intensive signature matching and behavior analysis using a database with more than 100 TB of threat data, which is constantly updated with information from over 25,000 of Webroot's partners and enterprise customers and millions of consumer customers.

The Webroot Intelligence Network then sends a response to the endpoint client classifying the file as "good," "bad" or "unknown."

The endpoint client is then able to take appropriate action, allowing the file to execute, blocking and removing it, or continuing to monitor its behavior.


External Threat Data Feeds
100+TB Database of
Every Piece of Malware Ever Seen
Remote Laptop Users (client app <700KB)
Real-Time
Data
Webroot
Intelligence
Network
Behaviors
Database
Known File
Hash Database
Other Threat
Database
amazon
Uses EC2 • Replicated WW
Fully Redundant • Scalable
Corporate Workstations (client app <700KB)
URL and IP Data
from > 25,000 of Our Partners and
Enterprise Customers Worldwide
Webroot Customer Data Feeds
Millions of Customers–Consumer and Enterprise

Summary

In today's world of employees spending hours online every day with multiple devices, Webroot offers a unique portfolio of solutions for protecting endpoints.

This consists of three offerings that can be deployed independently or in any combination: Webroot SecureAnywhere™ Business – Endpoint Protection, Webroot SecureAnywhere™ Business – Mobile Protection, and Webroot SecureAnywhere Web Security Service.

When implemented together, they provide far-reaching benefits:

- Endpoint protection for a wide range of devices: desktop PCs, laptops, tablets and smartphones.
- A single management console for endpoint protection and mobile device protection, to provide simplicity and economies of scale deploying and managing all types of protection.

Return to top

- Layered security that inspects and controls web traffic to all devices, and then protects each individual device.
- A “single pane of glass” to collect and correlate data from all types of endpoints.
- Simple licensing options that make it easy and economical to protect employees, no matter how many Internet-connected devices they have.

Appendix: Information Resources

Webroot SecureAnywhere™ Business – Endpoint Protection

Overview: http://www.webroot.com/En_US/business/secureanywhere-endpoint/

Information resources: http://www.webroot.com/En_US/business/resources/

Trial: http://www.webroot.com/customerSupport/trialRegistration.php

Webroot SecureAnywhere™ Business – Mobile Protection

Overview: http://www.webroot.com/En_US/business/mobile-protection/

Information resources: http://www.webroot.com/En_US/business/resources/#mobile-protection

Webroot SecureAnywhere Web Security Service

Overview: http://www.webroot.com/En_US/business/web-security/

Information resources: http://www.webroot.com/En_US/business/resources/