WHITE PAPER

WEBROOT
Smarter Cybersecurity™

Why You Need Web and Endpoint Security to Protect Your Organization

by George Anderson, Product Marketing Director, Webroot

CONTENTS

Introduction 3

Preventing Infections and Breaches 4

- Proven Virus and Spyware Prevention .....
- BrightCloud® Threat Intelligence Stops Unknown Threats .....
- World's Largest and Most Accurate URL Categorization Database .....
- Unique – Real-Time Anti-Phishing Protection .....
- Tamperproof Agent .....

Minimized Management Complexity 6

- Streamlined Web Management .....
- Granular Control .....
- Guaranteed Service With World Class Support .....
- Tamperproof Logging and Scheduled Management Reporting .....

Reduced Operational Risk 7

- Desktop Web Proxy – DWP .....
- Global Secure Datacenter Network .....
- Customizable Web Security Dashboard .....

How Cloud-Based Web Security Compliments Your Endpoint Security 8

- Web Threats .....
- Some Statistics From Our 2015 Threat Brief .....

Conclusion 9

INTRODUCTION

Using the Internet today is the single greatest risk factor to your employees' devices becoming infected and your network being breached. It's become especially risky for any organization with a highly mobile workforce, which these days is most of us. Recent research by Forrester[1] showed 60% of employees working from home a few times per month and 38% at least one day or more by week in organizations with over 1,000 employees. The risks from web usage are so high that security and risk professionals deem it critical that a secure web gateway should be an essential first line of defense.

For many years web security has been little more than URL filtering (controlling what web sites users could access) and maybe routing web traffic through a separate network perimeter antivirus. However, as the web became more dangerous, more complete "secure web gateway" solutions emerged offering combined web security features that included – URL filtering, file-type filtering, application filtering, and additional web malware protection.

Some of the most recent web security development is around "cloud-based" web security services. These work by moving web security onto the Internet layer and by stopping web threats before they reach the traditional DMZ network perimeter layer. They allow organizations to still comply with HR, Legal, duty of care and regulatory compliance requirements, and critically they also enforce consistent web policies and usage, regardless of physical location.

The Webroot SecureAnywhere® Web Security Service was one of earliest, purely cloud-based secure web gateway solutions (launched in 2007). Today's service is completely different from then, but it still provides a cost-effective alternative to conventional, on-premise secure web gateway solutions. With a centralized, easy to use, and intuitive web-based management console, the Web Security Service removes the need for any on-premise IT infrastructure. And, in combination with its tamperproof, lightweight endpoint agent, it's easy to deploy anywhere.

Next-generation secure web gateway security doesn't only prevent infections and breaches and minimize web security management complexities, it also significantly reduces the operational costs and risks of protecting users against advanced malware threats, spear phishing, and other sophisticated attacks by intercepting and tackling them before they infect the user and your network.

The bottom line is that Internet web security and web usage need to be addressed separately from your endpoint protection, because it's unrealistic to expect your last line of defense, your endpoint security, to be 100% effective against all types of web threat.

PREVENTING INFECTIONS AND BREACHES

The web is the number one infection and breach vector into organizations. So, being able to effectively stop web threats is paramount. The Webroot SecureAnywhere® Web Security Service guarantees the protection of users against known viruses and spyware. Through its pro-active security layers and use of Webroot BrightCloud® Threat Intelligence Platform, the Web Security Service predicts and protects against unknown and advanced web attacks.

The cloud architecture allows users to be directly authenticated to the service for seamless enforcement and protection, regardless of their physical location. The device agent ensures users cannot bypass web usage policies and thereby helps to increase productivity and facilitate the consistent enforcement of essential HR, legal, compliance, and "duty of care" obligations. Highly accurate and effective, BrightCloud Threat Intelligence combined with our predictive web malware infection prevention is how Webroot is able to stop web threats and turn the Internet into a safe place to do business.

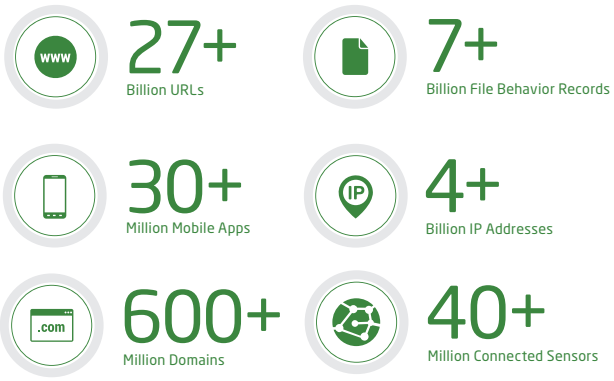
Proven Virus and Spyware Prevention

The Webroot SecureAnywhere Web Security Service offers advanced prevention against web malware and spyware. The next-generation endpoint protection, including antivirus, host intrusion prevention (HIPS), and malicious traffic detection operates at one layer to prevent infections, detect compromises, and stop web threats with real-time threat intelligence. On another layer, non-signature-based advanced exploit and heuristic protection – plus propriety defenses against JavaScript, Shellcode, and cross-site scripting – are used to handle web exploits and stop threats many other solutions miss.

BrightCloud® Threat Intelligence Stops Unkown Threats

The Webroot SecureAnywhere® Web Security Service provides additional Internet protection layers by fully leveraging the global BrightCloud® Threat Intelligence Platform - it encounters tens of millions of instances of malware and potentially unwanted applications and monitors billions of IP addresses and URLs every day. It produces real-time, contextual, and

[1] Forrester's Global Business Technographics® Telecommunications and Mobility Workforce Survey, 2015



predictive threat intelligence that spans the widest spectrum of attack vectors and allows Webroot to implement an instant defense-in-depth strategy against malicious web traffic to and from the cloud.

Contextual threat intelligence is the only way to fight back against today's cybercriminals and give organizations back a security edge. It's what makes our threat intelligence not simply a cloud-based data repository of security data but one of the most powerful real-time threat platforms of its kind.

The figures are staggering. The BrightCloud Threat Intelligence Platform scans the entire IPv4 address ranges over three times per day to continuously score and accurately classify unsurpassed numbers of URL's, IP addresses, and domains. It analyzes millions of new and updated files and apps for malicious behavior and studies major malware trends based on data from millions of endpoints and network/security devices. All of this, and more, is then used to continuously enrich the BrightCloud Threat Intelligence Platform and allows us with absolute accuracy to protect organizations preventatively from sophisticated web attacks. The Platform is literally a real-time sandbox of the entire Internet turned into applied threat intelligence.

World's Largest and Most Accurate URL Categorization Database

The Webroot Web Security Service uses our BrightCloud® Web Classification Service to keep track of hundreds of millions of websites to protect users from being exposed to spyware, drive-by malware, and the many other types of malicious code encountered during normal Internet usage. Unfortunately, even legitimate sites are compromised regularly these days and often shift rapidly between malicious and benign to avoid detection.

The Webroot BrightCloud® Web Classification Service has over 600 million domains scored and classified and described under 83+ categories. It deals with websites in over 45 languages and analyzes over 740 million IP addresses, uncovering over 85,000 net new malicious IPs per day.

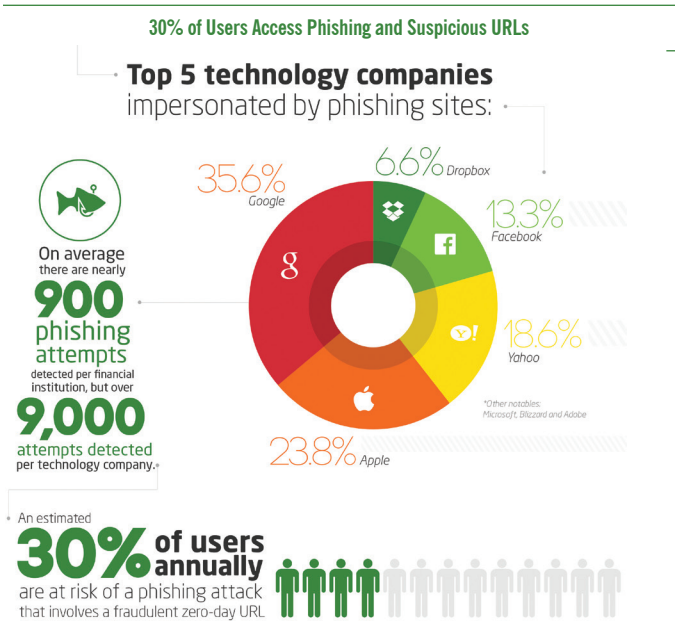
This super accurate content classification provides administrators with granular control over users' website access, enables flexible policy enforcement and offers precise Internet usage management reporting. With the world's most comprehensive and accurate coverage of the web it's easy for an administrator to create web access policies that are specifically tailored to match the compliance, HR, and legal requirements they need to enforce. Accurate classification also results in little re-classification being needed and reduced support calls from staff.

Unique, Real-Time Anti-Phishing Protection

Phishing and spear phishing attacks that hide web URLs and try to get users to provide sensitive information are the single most successful tactic in helping cybercriminals hack into organizations' networks. Webroot research has shown that during 2014, 30%[2] of our web users were at risk from a phishing or spear phishing attack.

The Webroot SecureAnywhere Web Security Service uses a unique and propriety real-time assessment to ensure users are always connected to genuine sites and not interacting with a phishing site..

Additionally, to mitigate data losses and protect users from inappropriate content, filters can be activated based on web application, file type, file size, and more.



Tamperproof Agent

Clever and resourceful users often try getting around being monitored by using proxies. Like other web security threats, these proxy sites are blocked by the URL filtering policy, but they appear so quickly that users may still circumvent monitoring.

Propriety technology in our Web Security Service is purpose-designed to defeat any user attempts to bypass policy controls by identifying even brand new web proxies.

[2] Webroot 2015 Threat Brief

MINIMIZED MANAGEMENT COMPLEXITY

A key design aim of the Webroot Web Security Service is to minimize the management complexity associated with web security management (particularly for organizations with multiple locations and/or a highly mobile workforce) while improving security, increasing user visibility, enforcing flexible policy controls, and reducing overall operational costs.

The Webroot Web Security Service offers a secure, centralized, cloud-based management console that is available from anywhere via a web browser. It's designed to be both intuitive and simple to use while making management and enforcement of granular policies straightforward. It offers anytime, anyplace access to the console for configuration, user deployment, web policy management and reporting – coupled with full roles-based access permissions.

Streamlined Web Managment

Our cloud-based approach to web security provides global user visibility, regardless of location, and an ease of management not normally found in on-premise solutions. Unlike the on-premise approach we don't kill remote users' web performance by forcing them to "backhaul" through a VPN to access the web via the network. Instead we seamlessly authenticate users from anywhere and by doing so eliminate the excessive costs of having to deploy web security at multiple office locations.

Without cloud-based web security, the constantly increasing use of the web to access business related applications, the dramatic growth in remote access, remote work, and use of multiple types of mobile devices to access the web all cause headaches for IT security administrators.

Along with the hugely increased risk of infections, the issue we face today is figuring out how to protect users and enforce web usage policies while reaping all of the productivity benefits the web brings.

Granular Control

Malware protection is a given, but web security management also means being able to filter the file contents entering and leaving your organization. It also means being able to control (right down to the individual user level if needed) through URL filtering what categories of website a user may or may not go to.

However, real granularity also means being able to extend policies to also limit how much time per day – and when – a user is allowed to visit certain categories of website. For added flexibility, an administrator may also want to restrict certain web sites but allow their users to override that decision. When it comes to social media the ability to define which applications within a site are allowed to be used, and when, is important to assure appropriate usage and maintain productivity.

Guaranteed Service With World Class Support

A major difference when buying cloud-based web security is that there is no on-premise hardware or software involved. The normal operational maintenance of security updates, patching, and having hardware support are also obsolete. There is also no need to budget for high-availability or disaster recovery as they come built-in as standard within Webroot cloud security solutions.

Webroot also offers a comprehensive Service Level Agreement (SLA) that covers service uptime, known virus and spyware detection, response times in the case of any service failures, time to get a policy enforced, and the other safeguards needed when the IT infrastructure is managed by a 3rd party, rather than by an organization.

Webroot Web Security Service also offers some of the best standard SLAs and support response times in the security industry.

Tamperproof Logging and Scheduled Management Reporting

As web usage may involve HR, legal, compliance, and user disciplinary actions, it is critical that full logs are kept of user web traffic and also audit logs for administrators' when using the web console.

The Webroot SecureAnywhere Web Security Service does both, and unlike many other secure web gateways, these logs are instantly available for the past twelve months, meaning there are no delays to your reporting or investigations. The service also offers log reporting and export to SIM/SIEMS.

Because of the visibility the Webroot SecureAnywhere Web Security Service provides, individual managers, IT, and other departments can see and understand their users' web behavior through the reporting provided in the management console. To save time and effort the reports created may be saved and re-run on a regular schedule without having to re-create them every time. They can also be assigned and collated together and sent to a pre-determined circulation list at fixed time periods. All of this automation of reporting means that administrative time is minimized and timely management reporting comes as standard.

REDUCED OPERATIONAL RISK

There are some considerable operational risks with delivering web security. Some users resent being monitored, as it stops them from behaving inappropriately or wasting time at work. For these reasons, they will look for ways to circumvent the controls in place, which presents both high security and compliance risks. The Webroot SecureAnywhere Web Security Service was designed specifically to stop the circumvention and ensure that all users' web traffic is directed, monitored, and reported through the Web Security Service.

This is also important to reduce the operational risks with remote users to ensure compliance.

Desktop Web Proxy

One of the key ways in which Webroot reduces operational risks and stops users from circumventing the web filter is through the deployment of the Desktop Web Proxy (DWP) agent. This easily-deployed, tamperproof client ensures all users are directed through the Web Security Service. It also transparently authenticates users on the service, helps them to intelligently negotiate hotel hot spots and other complex login situations, and prevents remote users from tampering with their browser settings.

Global Secure Datacenter Network

Another way in which Webroot reduces operational risks for our customers is by operating within a highly scalable, resilient, and meshed architecture of interconnected global datacenters (primarily Amazon Web Services) through which we operate the Webroot SecureAnywhere Web Security Service. These datacenters operate on a fully redundant basis, so even in the eventuality of a total datacenter failure, the Webroot Web Security Service will continue to operate through all of our secondary datacenters. This level of redundant and scalable IT infrastructure architecture allows us to provide carrier level uptime.

In addition to operating from within highly secure datacenters, Webroot operates strict access controls, regularly conducts penetration testing, and has accredited and audited the web security service to the SAS70 Type II.

Customizable Web Security Dashboard

Being able instantly to see what is happening with web usage is a highly practical way of reducing the operational risks of web security. The Webroot SecureAnywhere Web Security Service offers administrators a customizable dashboard that gives them an "at a glance" status of web usage within their organization and the impact web browsing is having on their bandwidth usage and other key metrics.

HOW CLOUD-BASED WEB SECURITY COMPLIMENTS YOUR ENDPOINT SECURITY

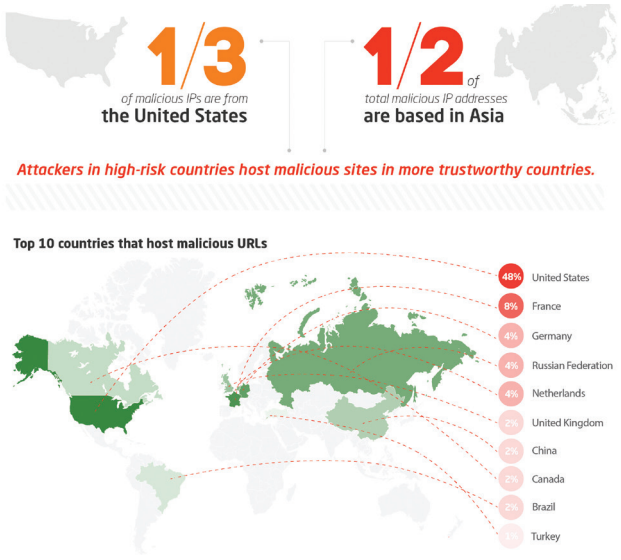
A question often posed is, "If I already have endpoint security, why do I need web gateway security?"

That is an understandable question and position. However, it does assume that endpoint security should be the first and the last line of defense. While endpoint security will provide varying degrees of protection from web threats, and offer in some cases a few web access controls, the defenses are basic and were never meant to offer the depth or levels of protection found in a dedicated secure web gateway.

In fact, relying on endpoint security is turning the security posture problem on its head. It's accepting that you should let malware inside your network before dealing with it!

Web Threats

In 2015 Webroot published its first Threat Brief – Insights from Collective Threat Intelligence. It reported that Webroot has seen a continued rise in the number of malicious URLs, IP addresses, malware, and mobile applications used to enable cybercriminals to steal data, disrupt services, or cause other harm. With more breaches at major retailers, financial institutions and technology companies in the headlines and scores of other, smaller breaches in 2014, the trend in 2015 shows no signs of slowing down. Here are some Infographics of the findings:



High-risk Countries Host Malicious Sites in Trustworthy Countries

Safe Categories Contain Highest Risk URLs

1	Spam URLs	30.9%
2	Malware Sites	13.7%
3	Business and Economy	7.8%
4	Proxy Avoidance and Anonymizers	6.7%
5	Phishing and Other Frauds	6.4%
6	Society	5.1%
7	Shopping	5.1%
8	Travel	2.7%
9	Health and Medicine	1.8%
10	Entertainment and Arts	1.8%

Top 10 Categories Suspicious to High Risk URLs – Safe sites are risky too.

When it comes to web malware, most of the statistics and data are generated by security vendors as part of regular generic security updates and specific research related to them offering secure web gateway technology.

What is undeniable from all the research others and Webroot have conducted is that day to day Internet usage is highly risky.

Some Statistics From Our 2015 Threat Brief

- 85,000 net new malicious IP addresses were launched every day, or over 31 million throughout 2014
- Less than 55% of all URLs are trustworthy
- Out of the top 10 site categories visited by Webroot customers (business & economy, society, travel, Shopping, etc.) six of those categories also appeared in our Top 10 Categories of Suspicious to High Risk URLs
- 30% of Internet users access phishing sites
- 15% of new files are malicious executables

CONCLUSION

There are still many organizations without a secure web gateway relying on their endpoint security to stop web malware or using older, on-premise solutions that only partly answer today's mobile web usage and security management needs.

Given that the average business confronts about 5,000 malware threats every single month and that many of the threats lie outside the detection realms of conventional endpoint antivirus, it's clear why the web is the number one security risk and how the Webroot SecureAnywhere Web Security Service offers a very relevant web security prevention and protection service to all sizes and types of enterprises.

Web gateway security offers different checks, controls, and balances, and by offering an additional and complimentary layer of security should be an essential part of your security posture.

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