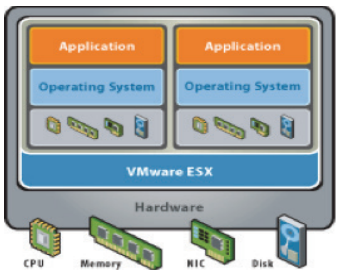
Virtualization and Security Overview

Virtual Overview

Until recently, hardware systems were designed to run one operating system, and normally only one application per server. This approach left many hardware resources (CPU, RAM, storage, network interface) vastly underutilized. With the introduction of x86 virtualization technology in the late '90s, IT administrators started to eliminate the "one server, one application" model by creating many virtual machines (VMs) residing on a physical server (hardware host).



This new approach provided the ability for a single physical server to handle several different application workloads while ensuring optimal performance and efficiency of existing resources. Since then, a majority of IT organizations have deployed virtualization and have realized 50-70% cost savings on their overall IT costs (source: VMware).

VMware customers report dramatic results when they adopt virtual infrastructure solutions, including:

- Efficiency: 60–80% utilization rates for x86 servers (up from 5-15% in non-virtualized systems)
- Cost savings: More than $3,000 annually for every workload virtualized
- Performance: Ability to provision new applications and systems in minutes instead of days or weeks
- Reliability: 85% improvement in recovery time from unplanned downtime

SMB Virtual Trends

- Server-virtual-cloud is analogous; SMBs interchanging form factor across workloads
- 50+ seats, nearly all SMBs have a server
- Over 60% of SMBs are adopting virtualization for servers and desktops
- SMBs that deploy a server for the first time are more likely to deploy a virtual, cloud-based server
- 43% of mid-sized businesses are eliminating local, on-premise servers and moving to hosted, cloud-based virtual infrastructures
- Hosted infrastructure is the largest and one of the fastest growing cloud services

Virtualization and Security

Aside from form factor, virtual systems are not very different from physical systems. They use the same operating systems and applications and provide users computing resources such as RAM and hard drives. Consequently, the ability to exploit vulnerabilities in a physical environment presents a significant threat to virtualized environments as well. In addition, virtual environments are also targets for unique threats.

Specific threats targeting virtual environments:

- Communication blind spots – Network security appliances cannot monitor communication between VMs on the same host. Some admins work around this by re-routing all communication through the appliance, but this introduces time lag.
- Inter-VM attacks – Once one virtual machine (VM) is compromised, the rest of the VMs become vulnerable.
- Hypervisor Compromises – Through less secure API, or by hyperjacking, a VM can be used to attack the hypervisor.
- Mixed trust Level VMs – VMs mixed with mission critical and non-mission critical data, results in mixed trust levels.
- Instant On Gaps – This occurs when admins rapidly deploy, clone, provision and decommission VMs (e.g., test environments). Deploying and maintaining endpoint security in this scenario can be challenging.
- Dormant VMs – Security definitions can become outdated. Reactivating these VMs can present a threat to the rest of the VMs on the host.

Deploying virtual systems to achieve significant efficiency, performance and cost savings is a step most IT administrators have taken or are considering in the future. With over 60% of small to midsized businesses (1-1,000 employees) and even more enterprises adopting virtualization, admins need to consider how best to utilize both physical and virtual systems, without adding complexity or negating the benefits offered by virtualization.

Virtual Protection Requirements

- Protection that won't impact performance or efficiency
- Lightweight client for minimal impact to CPU and storage
- Endpoint solution must sit on each virtual machine and detect threats that do not exist as files, e.g., malware in memory
- Easy to manage
  - No dedicated infrastructure
  - Same solution across all endpoints, including physical, virtual and even mobile
  - No constant, network-intensive signature updates

Competing Solutions

Agentless Approach

Most of the major competitors have server- and virtual-specific products. For virtual environments, the top security vendors recommend deploying an agentless solution. This solution sits on top of the hypervisor and depends on file system and network information passed on by the virtual infrastructure. No agent is deployed on the individual virtual machines. This approach exposes systems to sophisticated threats because agentless methods do not account for threats in memory or that don't exist as files on disk. Other negative consequences of agentless virtual protection:

- Workaround for overbearing signature-based protection solutions
- Higher costs
- Separate security application for admins to manage
- Each VM depends on outside communication to remain secure
- Not ideal for cloud-based servers since IT does not have access to the virtualization infrastructure

Signature Approach

Customers also use signature-based security for their virtual environments. The challenges experienced with signature-based security on a single system include high CPU usage, storage space consumption, long scan times, etc. Randomization or grouping scans and updates can help reduce the resource intensiveness, but still requires significant downtime for a full scan cycle.

Sacrificing performance with traditional, signature-based endpoint security or exposing virtual environments to vulnerabilities through an agentless approach are not ideal solutions.

Summary

1. SMBs are moving towards virtual, cloud-based servers and desktops
2. Revenue growth areas exist in Virtualization, SaaS and Server Security products
3. Virtual environments require protection that doesn't impact performance or efficiency
4. Competitive approaches, i.e., agentless or signature-based solutions, are not ideal for maximum protection in these environments

Webroot SecureAnywhere® Business Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection provides virtualized environments uncompromising security and maximum performance using an innovative cloud-based design and resource aware client technology. Webroot brings together innovative file pattern and predictive behavior recognition technology, with the almost limitless power of cloud computing, to stop known threats and prevent unknown zero-day attacks more effectively than anything else.

Using the world's lightest and fastest endpoint security agent, scans occur in minutes and never slow users down. In addition, because detection is in real time, it is always up to date, and provides protection against the latest threats and attacks without the hassle of daily signature and definition updates.

Webroot SecureAnywhere Business Endpoint Protection has an extremely small footprint on virtual machines, so it can be deployed to hundreds of VMs without impacting performance or storage. Additionally, once installed on individual virtual machines, Webroot SecureAnywhere Business Endpoint protection sits deeper on the Operating System, to enable maximum protection. Further, this superior protection secures physical and virtual servers and desktops, so admins only have to manage one solution.

KEY BENEFITS

Revolutionary Security

Webroot cloud security intelligence virtually removes the window of vulnerability that exists with other, signature-based endpoint security solutions, and delivers real-time protection against all types of online threats.

- Virtually eliminates the vulnerability exposure time between when an exploit is released and the time when it's detected and can be removed
- Unique file pattern and behavior recognition technology determines if endpoint activity is benign or malicious
- Instantly checks changed and new files and processes against our cloud malware intelligence database, the Webroot® Intelligence Network (WIN), to determine file and execution behaviors and track and understand their intent
- Advanced threat intelligence detects known threats and those that

FAST FACTS

Best unknown malware prevention

» Revolutionary file pattern and behavior recognition technology
» Predictive intelligence accurately detects if any file activity is benign, or malicious
» Virtually eliminates the window of vulnerability from emerging threats

Extremely fast and easy to deploy[1]

» World's smallest endpoint security client/agent (<750KB)
» Takes under 16 seconds to install
» Works alongside other security and software applications

Doesn't slow down systems or hinder user productivity[1]

» Initial system scan takes typically <2 minutes, subsequent scheduled scans <30 seconds
» Minimal CPU usage during scans
» Automatic remediation drastically reduces the need to reimage systems
» Always up to date and protected
» No definition file updates to consume network bandwidth
» Off-network users remain protected and never need any protection updates
» All users instantly protected against any new threats

Easy to manage

» Centralized Web-based management of all endpoints
» Highly automated management and reporting
» No on-premise management server hardware or software
» Full remote policy and endpoint management

Online and offline protection

» Separate policy controls for offline endpoint user management
» Ability to manage ports and devices such as USB, CD and DVD drives

have never been seen before, protecting against all known and zero-day threats
» Offline protection secures endpoints that are not connected to the Internet and offers powerful heuristics and the ability to manage ports and devices such as USB, CD and DVD drives
» WIN constantly collects information on new and potentially malicious files from across the globe, sharing it instantly to ensure up-to-the-minute protection
» No signature or definition file updates required

Ultimate Performance[1]

Webroot SecureAnywhere Business – Endpoint Protection sets new standards in deployment time, scan speeds, system resources usage, and overall endpoint footprint size, to ultimately save you time and money.

» The world's smallest client at less than 750KB
» Downloads, deploys, and installs in under 16 seconds
» Minimal CPU usage to improve user productivity
» Minimal disk space required
» Lightning fast take minutes, not hours
» Improved PC performance, even those with extremely limited system resources
» Coexists with other security products, eliminating the need to uninstall existing solutions prior to migration.
» Maximizes security and never slows you down

Minimal Management

An intuitive Web-based management console lets you easily manage endpoints and policies, view detailed service reports and logs, and manage whitelists, blacklists, and file overrides. Other management advantages include:

» No management server hardware or software to purchase, install, or maintain
» Pre-configured and default policy templates
» Easily configurable administrator alerts and notifications
» Online, ad-hoc, and scheduled real-time reporting
» Automatic threat and software updates delivered quickly and without bandwidth or performance impacts
» PCs, laptops, servers, and mobile devices can all be managed from the same console
» View users by current Active Directory, IP Range or user Workgroups

Mobilizing the Workforce

Users have become more reliant upon mobile devices to access personal and business data. Mobile devices have become attractive targets to digital attacks. Small size and portability make them highly vulnerable to theft

1 PassMark Software, "Webroot SecureAnywhere vs. Traditional Anti-virus, January 2013"

or loss. With the optional Webroot SecureAnywhere® Business Mobile Protection from the same management console you can:

» Securely lock the SIM card and enforce passwords and access timeouts
» Wipe sensitive corporate data
» Keep users safe from phishing attacks and malicious URLs with the Secure Web Browser
» KEY FEATURES

Powerful Malware Detection
Provides the most advanced real-time endpoint protection against both known and unknown malware to virtually eliminate the vulnerability window between when threats emerge and when they're detected.

Offline Protection
Stops attacks when an endpoint is offline with separate file execution policies applicable to local disk, USB, CD, and DVD drives. Also includes ability to lock down devices and ports.

Powerful Heuristics
Heuristic settings can be adjusted through 5 different levels based on risk tolerance for file execution. Heuristic settings cover:

» Advanced Analyzes new programs for suspicious actions that are typical of malware
» Age Analyzes new programs based on the time a similar file has existed within the Webroot community
» Popularity Analyzes new programs based on how often file is used or changed within the Webroot community

Rollback Remediation
A fail-safe rollback feature provides the ability to restore programs, as well as roll back cleanup processes to a previous state.

Webroot Intelligence Network
Real-time threat detection and analysis via the world's most powerful threat intelligence network, which includes over 250 million unique extractable objects with associated file behavioral characteristics.

Instant Deployment
Deploys via a packaged MSI installation file, custom deployment tool, or link to download the executable.

Software Compatibility
Compatible with all other software applications, making deployment alongside existing software very easy.

Intelligent Firewall
A sophisticated cloud-driven firewall protects users inside or outside the corporate network by augmenting the Microsoft® Windows® firewall. It monitors all outbound connections without draining endpoint resources unnecessarily. By managing and monitoring all outbound traffic, the firewall protects against malicious data exfiltration attacks and ensures that only policy-approved applications communicate outside the network. It also automatically recognizes known good and bad programs, so users aren't pestered with pop-ups or forced to make uninformed judgments.

SafeStart Sandbox
Designate unknown files to only open in a protected sandbox environment for behavioral evaluation. This helps to ensure that unwanted applications do not infect users' systems.

Server and Virtual Server Support
In addition to supporting physical Windows PC environments, Webroot SecureAnywhere can also support Windows server and virtual server environments.

Mobile Smartphone and Tablet Support
Webroot SecureAnywhere Business – Mobile Protection is available for Android™ and iOS® smartphones and tablets.

Mac® Support
Basic Mac support including remote deployment and monitoring is now available.

Resilient Distributed Cloud Architecture
Consists of multiple global datacenters to support local offices and roaming users through their nearest datacenter and provide excellent resilience and redundancy.

About Webroot
Webroot is bringing the power of cloud-based software-as-a-service (SaaS) to Internet security with its suite of Webroot SecureAnywhere® solutions for consumers and businesses. Founded in 1997 and headquartered in Colorado, Webroot is the largest privately held Internet security organization based in the United States – operating globally across North America, Europe and the Asia Pacific region.
For more information about the Webroot SecureAnywhere Business portfolio, www.webroot.com, the **Webroot Threat Blog:** http://blog.webroot.com or **Webroot on Twitter:** http://twitter.com/webroot

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 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