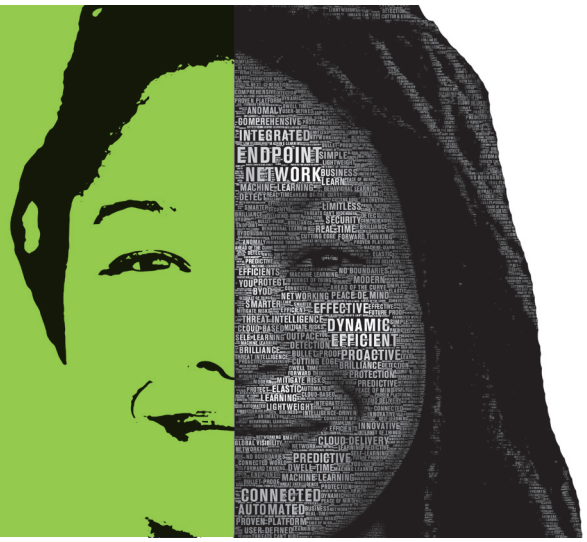
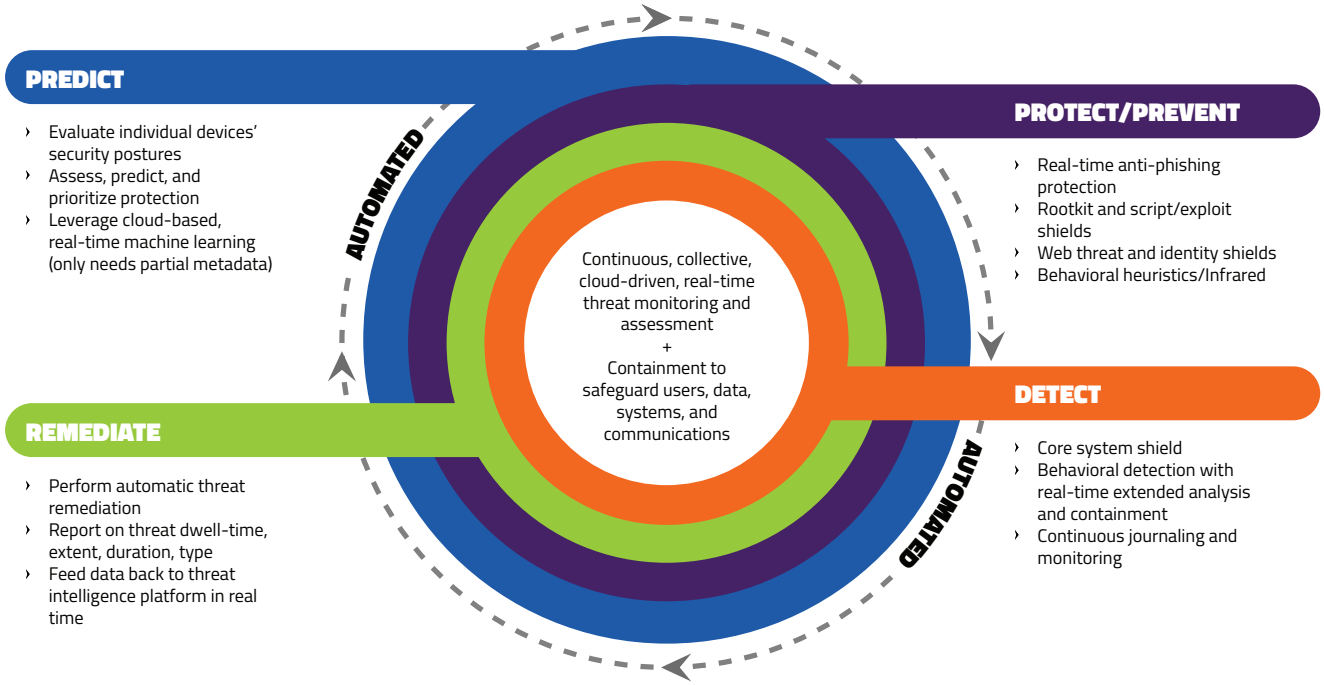
WEBROOT
Smarter Cybersecurity™

Webroot Business Endpoint Protection
A 'Next Gen' Endpoint Security Solution



Cutting Through the Hype to Discover Real Next-Gen Threat Detection and Response



Next-Gen Endpoint Security

Defining "Next-Gen"

Security experts, analysts, and vendors use a variety of terms and jargon to describe the makeup of their next-generation endpoint security, with none agreeing on a set definition. Originally, the term was coined to differentiate innovators in endpoint security, meaning those who no longer relied upon traditional file scanning methods to detect threats.

Modern malware solutions have re-architected their detection and protection approaches to use more advanced prevention, detection, and prevention methods that don't rely on the slower, signature-based defenses that were then widely used.

The term next-gen also refers to solutions that use real-time predictive methods like machine learning (ML), artificial intelligence (AI), and behavioral analysis to increase prevention efficacy and speed. In some cases, the term extends to automated threat detection and response capabilities. Today many "traditional" antivirus companies have added next-gen features to their existing architectures and lines between the two have begun to blur.

Today, a next-gen endpoint security solution does have some differences (many of them involve better system performance and multi-vector defense layers). But the real question is: "Is my endpoint protection highly effective at protecting me and my system from the sophisticated, multi-level attacks being used to infect devices today?" To accomplish that, you need endpoint protection that examines every process on every device and counters all attack vectors to stop the malicious tactics now in use every day.

Key Next-Gen Threat Detection Techniques

Typically, a next-gen endpoint security solution should employ:

» Automated detection and response (ADR) to stop threats and remediate systems automatically

» Behavioral analysis to identify malicious files based on behavioral deviations or anomalies

» Threat intelligence that processes data through ML and AI algorithms to determine whether a file or process is malicious

» Ransomware protection to record file and system changes so systems can be restored to their pre-infected state in the event of a ransomware infection

» Forensics capable of replaying attacks to help security teams better mitigate future breaches

» Endpoint detection and response to continuously monitor systems and networks to mitigate advanced threats

» Anti-script/anti-exploit protection that prevents application exploits from launching

In addition, features like granular policy customization, low system resource usage, and ease of operation are also major differentiators.

Webroot® Business Endpoint Protection – The 1st Next-Gen Endpoint Protection

In 2011, Webroot launched a completely re-architected and unique endpoint security solution to replace our traditional, signature-based antivirus products. In doing so, Webroot became the first cloud-based cybersecurity vendor using an advanced machine learning-based threat intelligence platform to power real-time predictive and behavioral analysis to deliver highly automated threat prevention and protection.

Since then we have continually evolved and enhanced our prevention and protection capabilities to increase efficacy, efficiency, and ease of use. This approach is highly attractive for small to medium-sized businesses and managed service providers because it arms them with an endpoint security solution that just works, and is highly effective at stopping attacks designed to compromise both users and their devices.

The following are some of the key ways in which Webroot® Business Endpoint Protection uses next-gen and other advanced endpoint protection capabilities to protect devices and users from being compromised and infected.

Webroot – Advanced Endpoint Protection	
Threat Prevention (pre-execution)	
Application/file blacklisting	✓
Application whitelisting	✓
Application/file execution isolation	✓
Application/file reputation analysis	✓
On-host machine learning (for pre-execution file scanning)	✓
Host Intrusion Prevention System	✓
Threat Detection (Post-Execution)	
Endpoint behavioral analysis with prioritized alerts	✓
On-host machine learning (for malicious behavior detection)	✓
User behavior analysis (used for external threat validation/risk adjustment)	✓
Dwell-time network and device infection reporting	✓
Remediation/Control	
Endpoint behavioral analysis with automatic containment options	✓
Automatic, policy-based endpoint configuration roll-back	✓
Automatic, policy-based file quarantine	✓
Malicious in-memory activity containment	✓
Additional Threat Protection/Prevention	
Continuous endpoint security monitoring	✓
Collective real-time threat protection	✓
Real-Time Anti-Phishing	✓
Web browser and safe search security	✓
Privacy and identity credential protection	✓
Next Gen Performance Features	
Automated system malware protection and containment	✓
Highly effective predictive pre-execution protection	✓
Auto-quarantine and system remediation	✓
Low system resources usage - RAM; CPU and Disk - in use and at idle	✓
Low system resource usage - general operation	✓
Negligible false positives/negatives	✓

Summary

Webroot® Business Endpoint Protection offers the advanced prediction, detection, prevention, and protection today's organizations need. And, with its cloud-based architecture and advanced multi-vector approach to stopping user and device attacks, a highly effective and efficient endpoint security solution that simply works when it comes to stopping infections and compromises.

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