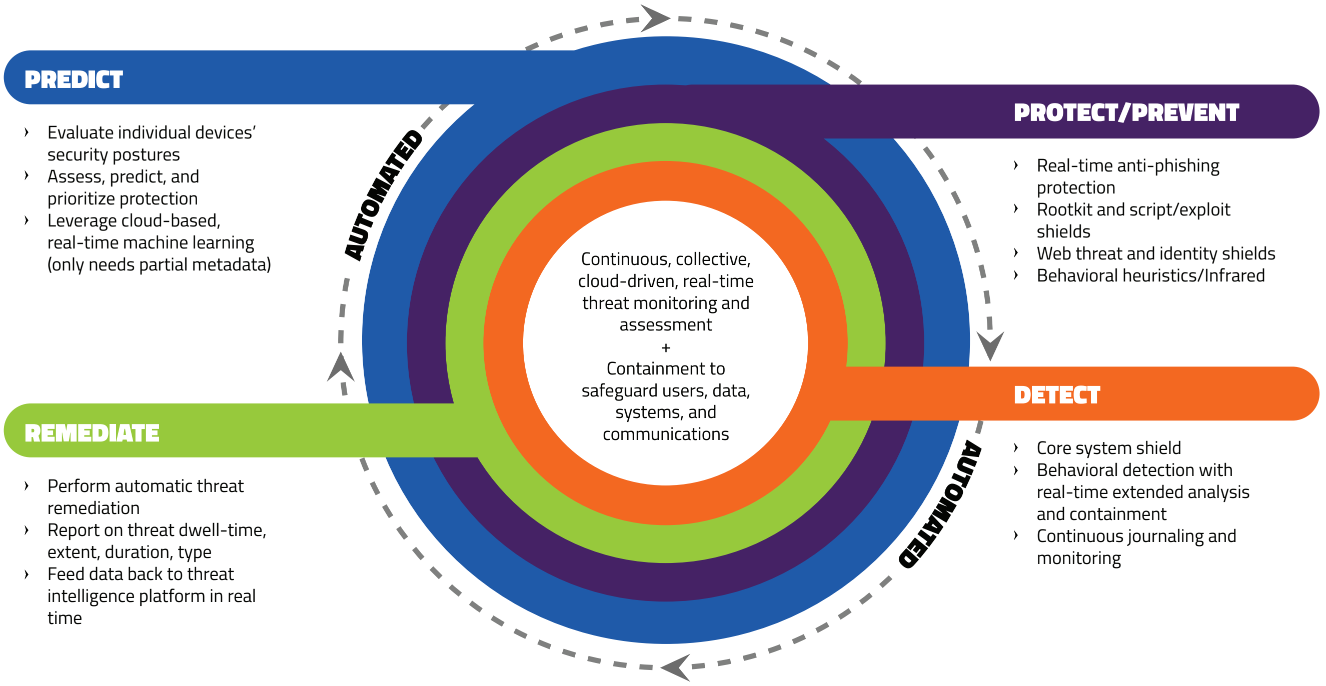
A Next-Gen Endpoint Security Solution for MSPs

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



PREDICT

- Evaluate individual devices' security postures
- Assess, predict, and prioritize protection
- Leverage cloud-based, real-time machine learning (only needs partial metadata)

PROTECT/PREVENT

- Real-time anti-phishing protection
- Rootkit and script/exploit shields
- Web threat and identity shields
- Behavioral heuristics/Infrared

DETECT

- Core system shield
- Behavioral detection with real-time extended analysis and containment
- Continuous journaling and monitoring

REMEDIATE

- Perform automatic threat remediation
- Report on threat dwell-time, extent, duration, type
- Feed data back to threat intelligence platform in real time

Continuous, collective, cloud-driven, real-time threat monitoring and assessment
+
Containment to safeguard users, data, systems, and communications

Next-Gen Endpoint Security

Defining "Next-Gen"

Although security analysts and solution vendors use a variety of terms and jargon to describe the markers of next-generation endpoint security, there isn't a set definition. Originally, the term was coined to differentiate innovators in the endpoint protection market who no longer relied upon traditional antivirus methods for detecting threats. These vendors had re-architected their detection and protection algorithms, moving away from the signature-based approaches that had been used so widely up to that point. The term "next-gen" also referred to vendor solutions that had begun using real-time methods, the cloud, machine learning (ML), artificial intelligence (AI), and/or behavioral analysis to increase efficacy and speed, and to automate threat detection and response.

As even the traditional antivirus companies who were slower to adopt "next-gen" methods began catching up—adding next-generation components to their existing architectures, etc.—the lines began to blur. At this stage in the game, a next-gen endpoint security solution really means one that is effective against the high velocity and volume of sophisticated, evolving, multi-stage attacks that are currently being launched to compromise endpoint devices and data today. To accomplish that task, a solution needs to examine every process on every endpoint to detect all types of attack vector, and block the malicious tools, tactics, and procedures attackers deploy.

Key Next-Gen Threat Detection Techniques

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

» Automated detection and response (ADR) – stops threats and remediates systems automatically

» Behavioral analysis – identifies malicious files based on behavioral deviations or anomalies

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

» Ransomware protection – records file and system changes to restore systems to their pre-infected in the event of a ransomware infection Forensics – replays attacks to help security teams better mitigate future breaches

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

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

In addition ADR, behavioral protection, and machine learning, features like customization, low system resource usage, and ease of management have also become major differentiators.

The First Next-Gen Endpoint Protection

In 2011, Webroot launched a completely new endpoint security solution to its consumer base. Until that moment, Webroot had been a traditional, signature-based antivirus vendor. With the 2011 launch, Webroot became the first cloud-based cybersecurity vendor on the market, using an advanced machine learning-based threat intelligence platform to power real-time behavioral analysis and automated threat detection. A year later, we launched Webroot® Business Endpoint Protection for small- and medium-sized businesses (SMBs). Since then, we have continually evolved and enhanced our prevention and protection to increase efficacy, efficiency, and ease of use.

Next-Gen Endpoint Security Features	Does Webroot offer these features?
Threat Prevention (pre-execution)	
Application/file blacklisting	Yes
Application whitelisting	Yes
Application/file reputation analysis	Yes
Application privilege management	No
Application/file execution isolation	No
On-host machine learning (for pre-execution file scanning)	Yes
Host intrusion prevention system	Yes
Host vulnerability scanning (e.g., reporting on unpatched CVEs)	No
Threat Detection (Post-Execution)	
Endpoint behavioral analysis with prioritized alerts	Yes
On-host machine learning (for malicious behavior detection)	Yes
User behavior analysis (used for external threat validation/risk assessment)	Yes
Additional Threat Protection and Prevention	
Continuous endpoint security monitoring	Yes
Collective real-time threat protection	Yes
Real-time anti-phishing	Yes
Web browser security	Yes
Identity and privacy protection	Yes
Remediation and Control	
Endpoint behavioral analysis with automatic containment options	Yes
Automatic, policy-based file quarantine	Yes
Automatic, policy-based endpoint rollback remediation	Yes
Automatic, policy-based network isolation	No
Device/media control (USB, shared drives, bus control, etc.)	No
Malicious in-memory activity containment	No
CVE-based virtual patching or patch deployment for third party apps	No
Endpoint full disk encryption	No
MSP-Ready Features	
Fully remote deployment and management via agent commands	Yes
Automated threat detection and response	Yes
No-conflict deployment	Yes
Small endpoint agent and device footprint	Yes
Low system resource usage during scanning	Yes
Low system resource usage during general operation	Yes
No definition update management	Yes
API for integrations	Yes
MSP ecosystem with RMM, PSA, MDR and BI integrations	Yes
Integrated trouble ticketing and 24x7 incident support	Yes
Negligible false positives/negatives	Yes

About Webroot

Webroot, a Carbonite company, harnesses the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide endpoint protection, network protection, and security awareness training solutions purpose built for managed service providers and small businesses. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Webroot operates globally across North America, Europe, Australia and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.

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