

WHY YOU NEED MULTI-VECTOR PROTECTION

Modern cyber threats attack businesses and individuals indiscriminately and use multiple methods and threat “vectors” to succeed. By combining a range of threat technologies, deployed over numerous stages, cybercriminals maximize the likelihood of infection success. Even so-called “next-generation” endpoint security tends to focus on stopping an infection only after it has reached the endpoint, not preventing it from reaching endpoints in the first place. This creates security blind spots and limits their effectiveness to stopping attacks at a single stage.

Only multi-vector endpoint security will keep your business and clients infection-free through various stages and across multiple points of entry.

Single-vector protection can only stop threats at one stage of an attack, and won’t keep you or your clients safe. You need multi-vector protection that prevents infections and protects devices and users across all the stages of an attack.



MULTI-VECTOR PROTECTION

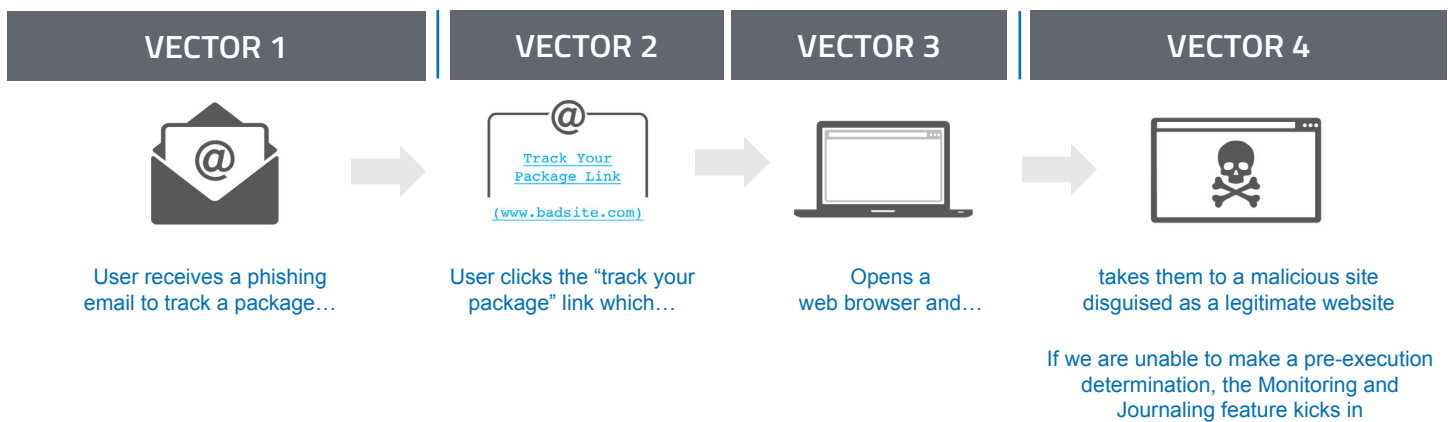
- 1 Stops malware before it downloads and executes
- 2 Provides multiple defense layers to keep phishing, credential theft, browser hijacking, keyloggers, and more from compromising end users and their devices
- 3 Allows business and MSP administrators to control the applications running on devices
- 4 Leverages real-time behavioral monitoring, threat intelligence, machine learning, and AI to rapidly identify and stop threats like Trojans, worms, and ransomware
- 5 Is fully automated to stay ahead of today’s attacks while minimizing IT overheads
- 6 Includes remediation features to roll endpoints back to their pre-infection state, without needing a full reimage

MULTI-VECTOR, MULTI-STAGE APPROACH

WEBROOT®
Smarter Cybersecurity™

With multi-vector protection, you have multiple chances at multiple attack stages to block or stop a threat before it reaches users or devices.

Real World Scenario – Phishing Attack



Webroot SecureAnywhere® Business Endpoint Protection protects you at every stage.

Attack Stage	Payload Delivery Stage	Infection Stage
<p>Email, web browsers, display ads, hyperlinks, files, social media apps, external devices like DVD or USB drives.</p> <p>Endpoints are protected with:</p> <ul style="list-style-type: none"> » Web Threat Shield » Identity Shield » USB Shield » Infrared Shield » Smart Firewall 	<p>Adware, spyware, ransomware, phishing attacks, keyloggers, viruses, and rootkits.</p> <p>Endpoints are protected with:</p> <ul style="list-style-type: none"> » Self-Protection Shield » Real-Time Anti-Phishing » Real-Time System Shield » Offline Shield » Rootkit Shield 	<p>Malicious website</p> <p>Endpoints are protected with:</p> <ul style="list-style-type: none"> » Zero-Day Shield » Behavior Shield » Core System Shield » Monitoring & Journaling » Quarantine » Rollback & Auto-Remediation

Webroot multi-vector protection prevents malware and exploits from executing, detects malicious activity post-execution, and remediates and contains malicious activity and potential vulnerabilities.