WEBROOT
Smarter Cybersecurity™

Multi-Vector Protection

Securing users and devices across all stages of a malware attack

Introduction

Educating users is an undeniably effective way to protect them from phishing, ransomware, and other malware, but it takes much more than that to stop attacks. There are many risks to networks that user education can't reduce—from malicious sites mistakenly categorized as benign to watering-hole attacks that infect trusted sites. To combat these challenges, businesses need well-designed antimalware that protects across a variety of attack vectors and infection stages. That's where multi-vector protection comes in.

According to analysts, effective multi-vector protection must be able to predict, prevent, detect, contain, *and* remediate cyberattacks.[1] In other words, they recommend security across numerous attack stages to prevent ransomware and other malware from loading or executing in the first place.[2] This kind of multi- vector defense is crucial for an effective, layered cybersecurity strategy.

This paper focuses on multi-vector protection as it relates to business endpoints and their cyber defense layers.

Attack Vectors

An attack vector is any method cybercriminals may use to compromise internet users or devices. According to Tech Target:

"An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element. Attack vectors include viruses, e-mail attachments, web pages, pop-up windows, instant messages, chat rooms, and deception.

"To some extent, firewalls and antivirus software can block attack vectors. But no protection method is totally attack-proof. A defense method that is effective today may not remain so for long, because hackers are constantly updating attack vectors, and seeking new ones, in their quest to gain unauthorized access to computers and servers."[3]

That last point is extremely important and bears emphasizing. Hackers are always refining and reinventing attack vectors. This means endpoint security vendors must constantly update their defenses to remain effective against attacks. Unfortunately, many attackers have the resources, time, and access to test their methods against endpoint defenses until they successfully break through, putting endpoint security vendors at a disadvantage.

Today's Threat Landscape

One strong example of a multi-vector attack is phishing, which was behind 93%[4] of security incidents and breaches in 2017. Two-thirds of the phishing attacks that resulted in a breach were followed by some form of malware installation.

Multi-vector attacks are designed to exploit the blind spots of conventional signature-based security, allowing threats like ransomware to infiltrate systems undetected. Unfortunately, even the more modern endpoint solutions available today still rely—at least in part—on signature-based detection models, making them vulnerable to multi-vector attacks.

According to Webroot threat research, 93% of all malware released is unique to a single endpoint. That means today's malware is almost always an unknown threat; it's always adapting and morphing into unique variants, into something that's never been seen before.

Single-vector endpoint security vendors can only protect end users once a threat is known, and only after a full malware installation attempt has been made on the endpoint. The infection itself will only be blocked if there is a local signature specific to that new threat variant. Extrapolating from the data Webroot has collected, that means there's up to a 94% chance the traditional solution won't be able to easily stop those threats.

Even newer, next-generation endpoint solutions, which are typically more effective than their traditional competitors, are ill-equipped to fight modern attacks. These solutions often only protect endpoints at the infection stage, and only across a single vector, relying heavily on models that are often not completely up to date.

A Real-World Multi-Vector Attack Scenario

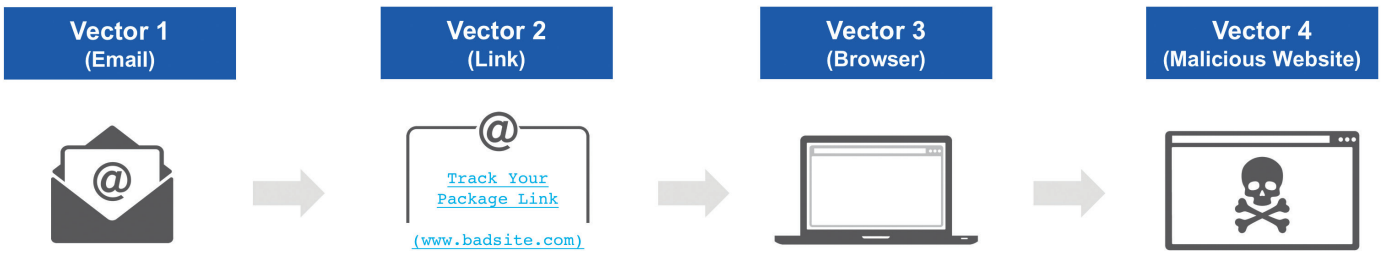
By far, the most common threats today are highly polymorphic ransomware variants that move across multiple attack vectors. Consider the following attack scenario:

Vector 1: A user receives an email for tracking a package.

Vector 2: The email contains a "track your package" link, which the user clicks.

Vector 3: The link opens the user's web browser to a fake site. The site is a polymorphic phishing site that's virtually indistinguishable from a legitimate one.

Vector 4: The site drops a malicious ransomware payload onto the user's machine.



Real-World Multi-Vector Attack Scenario

[1] Gartner, Inc. "Magic Quadrant for Endpoint Protection Platforms." January 2017.
[2] Forrester Research. "The Forrester Wave™: Endpoint Security Suites." October 2016.
[3] TechTarget.com. "What is an attack vector?" May 2012.
[4] Verizon. "2018 Data Breach Investigations Report." April 2018.

How Single-Vector Protection Fails

In the above scenario, a single-vector solution would only be able to protect the recipient of the email at the final stage of the attack, when malware is installed on the machine. At that point, the single-vector solution has only a few options for stopping the malware, either by identifying and blocking it using a signature, with a machine learning algorithm, or perhaps behavioral defenses.

If the solution misses the malware, then it has failed in its only chance to keep the machine infection-free. Recall that there's a 94% chance that a signature has not yet been created to detect and block the new threat. If the threat uses an attack type the single-vector solution has never seen before, and they're not connected to a larger, real-time threat intelligence platform, then there's a reduced chance of stopping the attack.

Multi-Stage, Multi-Vector Protection

The first stage of an attack is where your defenses should begin, where breaches should be prevented from occurring in the first place. Webroot SecureAnywhere® Business Endpoint Protection uses several shields that perform different tasks to prevent compromises throughout the different stages of an attack.

Web Threat Shield

The Webroot Web Threat Shield protects users as they browse the internet. For instance, when someone uses a search engine, the Web Threat Shield analyzes all search results and uses Webroot threat intelligence to display color-coded search annotations backed by web reputation scores in real time.

That means internet users are notified—before they click—that a site has a risky or poor reputation, even if its URL category is considered safe. If a user clicks through to a website with a poor reputation score that's currently displaying malicious behavior, they'll see a policy-managed block page.

The Web Threat Shield also adds a line of defense against phishing. Any link a user clicks from an email triggers the Webroot BrightCloud® Real-Time Anti-Phishing Service. The service performs a time-of-request scan to determine whether or not a site poses a phishing risk. Between the Web Threat Shield and the Real-Time Anti-Phishing Service, Webroot can prevents more than 99% of phishing and spear-phishing attacks.

Identity and Infrared Shields

The Identity and Infrared shields go a step further to protect users and prevent attack-stage incidents. The Identity Shield locks down the operating system and browser to neutralize phishing, DNS poisoning, keystroke logging, screen grabbing, cookie scraping, clipboard grabbing, and browser and session hijacking attempts.

The Identity Shield automatically looks for identity threats by analyzing, detecting, and blocking malicious content. It verifies each website to determine if there has been redirect, or whether the site has been blacklisted. It also stops websites from creating high-risk tracking information and blocks third-party cookie installation originating from malicious tracking websites. Additionally, the Identity Shield automatically blocks untrusted programs from accessing protected data, such as user login credentials.

Multi-Stage, Multi-Vector Protection

The Infrared Shield is another layer of defense that blocks threats early in their lifecycle. When users visit low-reputation websites, the Infrared Shield interrogates any applications that are introduced into the system. If a program was recently released, has suspicious attributes, or if there isn't enough information due to relative unpopularity, the shield blocks it before it can run.

Payload and Infection Stages

If a malicious payload does manage to make it past these shields to the infection stage, Webroot begins to operate very differently from other endpoint security solutions.

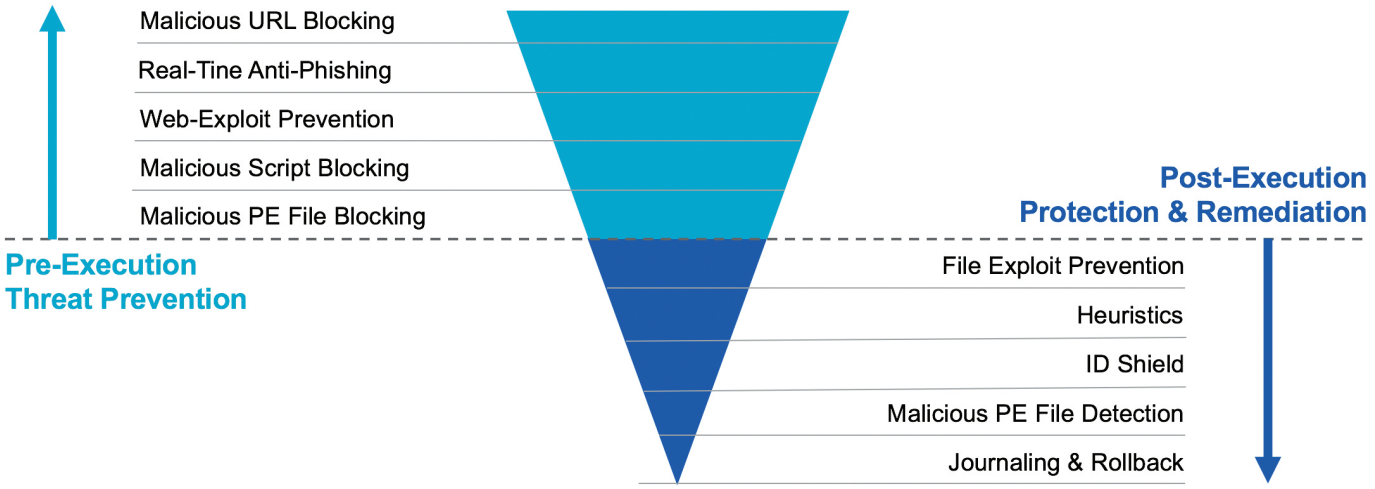
While a payload is downloading, Webroot SecureAnywhere® Business Endpoint Protection predicts whether a file or process is malicious before it ever executes. At this stage, files are immediately categorized as good, bad, or unknown, with a high level of accuracy.

The unknown categorization is the one that sets Webroot protection apart. Other solutions would need to make a good or bad determination immediately upon download, which could result equally in false positives or infections. The unknown categorization allows Webroot to monitor the file closely to make determinations based on its characteristics, behaviors, history, and relationships to other internet objects.

Payload Execution and Infection Remediation

Using self-protection shields, Webroot prevents malware from modifying our software settings and processes to guarantee it keeps operating properly even if an endpoint is under attack. The small agent footprint also combines with our cloud architecture to make it more difficult to disable Webroot protection, compared to larger-footprint, endpoint-only solutions.

Webroot solutions also leverage the Webroot® Threat Intelligence Platform to provide collective protection. When a new threat is identified and blocked for one Webroot user, all Webroot-protected endpoints around the globe are automatically protected from that threat in real time.



Multi-Vector Protection Efficacy Layers Pre- & Post-Execution

Additionally, Webroot uses its Threat Intelligence Platform to continuously analyze all applications and processes running on an endpoint, checking for suspicious behavior. If detected, it blocks any attempts to modify system settings, even if an endpoint is offline. The platform's extensive behavioral rule sets also check for unknown malware behaviors.

All of this means that Webroot protection is not forced to choose between a false positive or negative ruling because it monitors and journals all unknown and suspicious processes. In short, it misses less and detects more than many other vendors.

Finally, if a payload is later categorized as malicious, Webroot protection can automatically remediate the damage, rolling the endpoint back to its pre-infected state. All these system containment and multi-vector defenses are designed to provide better prevention and higher efficacy than conventional endpoint security solutions.

Unparalleled Efficacy

A key advantage of a multi-vector, multi-stage approach to stopping malware is knowing how long an infection is contained before being removed, i.e. its "dwell-time."

In the 2018 Webroot Threat Report, we found that 1 in 50 new executables on our users' devices were malware and overall Webroot's consistent efficacy rate through our multi-vector protection approach is 99.7% or better.

Conclusion

No endpoint security vendor can guarantee 100% protection 100% of the time. But vendors who offer a comprehensive set of layered defenses are significantly more effective at preventing attacks than those that focus solely on antimalware.

In an ideal security situation, an attack should be thwarted before an infection can become active on a user's machine. With the velocity, variety, and success rate of modern blended attacks, the only way for you to achieve this level of security is by leveraging multi-vector protection to secure users and devices through all stages of an attack.

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