MSP GUIDE: WHY YOU NEED A LAYERED CYBERSECURITY STRATEGY
An organization’s total cost for a data breach in 2017 is $7.35 MILLION

Cyberattacks have impacted leading retailers, financial institutions, healthcare providers, and even elections. While awareness of cyber threats may be at an all-time high, cyberattacks are still happening, and they’re extremely expensive, both in terms of money and a company’s reputation.

In light of headline-grabbing attacks, global enterprises and emerging companies alike are looking to engage with trusted advisors who can help them identify the best cybersecurity solutions to protect their critical assets without skyrocketing their costs.

This gives managed service providers (MSPs) an excellent opportunity to build their cybersecurity practice by implementing a layered, or “multi-vector,” security strategy.
Cybercriminals are more organized, well-funded, and better educated than ever before. They are increasingly savvy in implementing multi-vector attacks, which combine a range of threat technologies, deployed in numerous stages, across multiple points of entry to infect computers and networks.

Multi-vector protection ensures that your clients’ endpoint security covers threats that attack across emails, web browsers, files, URLs, display ads, social media apps, and more—through multiple attack stages—reducing the opportunity for cybercriminals to successfully breach your clients’ network.

**SOME KEY BENEFITS OF MULTI-VECTOR PROTECTION ARE:**

1. Multiple defense layers that stop phishing, credential theft, and keyloggers
2. Detecting malware before it has a chance to download and execute
3. Heuristics and machine learning rapidly identify Trojans, worms, ransomware, and others
4. Rollback remediation returns infected endpoints to their uninfected state, without reimaging

*If we are unable to make a pre-execution determination, the Monitoring and Journaling feature kicks in.*
HOW SINGLE-VECTOR PROTECTION FAILS

The next diagram illustrates how single vector protection, such as traditional antivirus, would fail to stop an attack. If a customer clicks on a suspicious email link, they can be taken to a phishing site that drops a malicious payload onto their device. Single-vector protection has only one chance to block the threat—at the active infection stage—or it will miss the threat entirely.

THE WEBROOT DIFFERENCE

Webroot solutions deliver advanced business endpoint, mobile, and DNS protection and threat intelligence via the cloud that can help organizations swiftly identify and respond to threats. We have the experience and expertise to help you stand apart from the competition. With multi-vector protection from Webroot, you can:

WITH MULTI-VECTOR PROTECTION FROM WEBROOT, YOU CAN:

1. Protect clients’ networks and endpoints from threats that span PCs, laptops, smartphones, and even flash drives
2. Enforce security policies for any remote or on-site devices connecting to the network
3. Stop zero-day malware attacks
4. Set policies, view activity, create and run reports, and enforce security policies in one straightforward, centralized console
5. Alert IT, managers, and employees about the latest security threats and trends
According to a 2016 MSPmentor 501 survey, **Webroot owns a 36% market share** with the world’s top MSPs. The next closest antivirus player within the MSP market has only a 15% share of the market.
BECOME AN MSP PARTNER

To learn more about how multi-vector protection from Webroot can help you keep clients safe and become more profitable, visit www.webroot.com/MSPpartners

ABOUT WEBROOT

Webroot delivers network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions and BrightCloud® Threat Intelligence Services protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, Citrix, F5 Networks, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at webroot.com.