WEBROOT®
Smarter Cybersecurity™

Partnering with Webroot

Capturing Opportunity in a World of Dynamic Security Threats

TABLE OF CONTENTS

Mobility Expands the Challenge....3
Capturing Opportunity in a World of Dynamic Security Threats 3
Building a Practice-based Services Approach 3
The Webroot Advantage 4
The Webroot® Channel Edge® Partner Program....4
Conclusion....4

Picture a fortified underground bunker with a single aboveground entrance. Install an iron reinforced door with a secure keypad. Add a heavily armed guard and you've got a good chance of fending off anyone who might try to enter unauthorized. Now imagine that the facility is above ground, with 100 doors, all with different access codes that are managed and modified by the employees who access them. Less secure, right? Now imagine 500 underground tunnels accessing that same facility, each with its own door, but the doors' locations change. Such is the challenge of securing the corporate network today.

Solution providers no longer have the luxury of dealing with one bunker (the datacenter). All doors (endpoints) are dispersed across employees who access the corporate network from the office, home, hotels and airplanes, via a variety of devices, and on open, public WiFi.

Cybersecurity is a somewhat nebulous term in the executive suite, encompassing both physical and virtual environments, and it is often difficult to ascertain acceptable risk and appropriate level of investment in the face of today's complex threat landscape. Companies invest in addressing their security vulnerabilities, but unforeseen breaches remain a consistent threat, impacting end user and IT productivity and compromising sensitive data. Another complication is that the number of endpoints a company must protect is constantly growing. Because these endpoints are often used outside of the corporate environment, they are dependent on users to secure them, making the task of protecting assets across the enterprise even more daunting. But the challenge this new paradigm presents also brings unique opportunities for both traditional resellers and managed service providers (MSPs).

To put this challenge in sharp focus, a 2014 study by the Ponemon Institute sponsored by Hewlett Packard found that the average cost of cybercrime for US-based companies climbed to $12.7 million, a 9% increase from 2013. In addition, the average time to resolve a cyber-attack jumped from 32 days to 45 days. The same study reported a 144% increase in the number of successful cyber-attacks per year over a 4-year period from 2010 to 2014, rising to a total of 122 per company.

With this type of data, its likely that the end user community will continue to increase its focus and spending to guard against an ever expanding matrix of threats that imposes greater costs in terms of lost of productivity, reputation and revenue each year.

MOBILITY EXPANDS THE CHALLENGE

Mobility has changed the game dramatically for customers contemplating corporate security. IT departments face a user base which not only demands access to resources whenever it needs them and from any device, but also requires access from devices outside the direct control of IT staff. These personal devices, part of the Bring Your Own Device (BYOD) wave of computing, are often mixed-use devices that access CRM applications prior to a morning sales call and post to a personal social media account in the evening. Each represents an endpoint with access to the corporate network with varying degrees of exposure. Even when a company can exert control over these devices by leveraging VPNs or dedicated work images, security updates and access control can be difficult. These devices are moving targets, completely changing the game for those responsible for implementing security solutions.

THREATS ARE EVER-PRESENT AND EVER-CHANGING

The threats corporations face today have evolved from prank hacking by rogue individuals for personal fame to sophisticated attacks meant to disrupt the very business of the target. In addition to the targeting of corporate information, every endpoint also becomes a target for attacks aimed at employees using corporate resources. The same phishing and malware threats that steal users' personal information on home devices are just as likely to find their way to the systems used for work. In fact, as technology evolves and work and home lives merge, it becomes even more likely that a hacker looking for bank account information or passwords to social media accounts might just as soon attack the systems used for business.

BUILDING A PRACTICE-BASED SERVICES APPROACH

The increased sophistication of threats and fluctuating definition of corporate endpoints means solution providers have the opportunity to build security practices that help businesses address these challenges. However, it's not enough to simply represent someone else's offering and expect to thrive and grow profitable revenue. Solution providers need their own differentiation and value—something they offer that no one else can.

When delivering effective cybersecurity, solution providers must focus not only on the technology to prevent breaches, detect malware and monitor companies' security status, but also their own consulting expertise to help clients do security planning and create employee awareness. Cybersecurity offerings should include services like threat vector analysis and assessments, needs/gap analysis, building security future-state roadmaps, and integration work with existing platforms, such as a customer's current RMM solution. Providers must become a trusted advisor to their clients, helping them continually assess their security status and evolve their infrastructure as new threats emerge. A cornerstone in developing this capability is making the right investments in training and certifications, and to have a team capable of this level of consulting.

But competitive services alone are not enough to capture market share. The technology partnerships that solution providers choose are also a way to differentiate from the competition.

THE WEBROOT ADVANTAGE

Whether you are a traditional solution provider looking to sell cloud-based solutions or an MSP adding cybersecurity services to your portfolio, a strong partnership is necessary for success. Solution providers should seek a partner with the right combination of technology and business practices in order to achieve competitive advantage and profitability.

Technology

Above all, technology must be easy to install and easy to maintain. All customers have horror stories of software that ends up as shelf-ware because it was too difficult to install and maintain. Cloud-based solutions that require less of an investment in dedicated infrastructure address many of those concerns, offering solution providers a selling advantage. For the customer, they provide an attractive cost of ownership profile over on-premises solutions.

Core to the Webroot advantage is its real-time, collective threat intelligent platform. Unlike signature-based antivirus or antimalware solutions installed on the endpoint, Webroot uses its cloud-based platform to constantly monitor endpoints and protect them against even unknown threats automatically. The Webroot BrightCloud Threat Intelligence Platform delivers highly accurate heuristics and behavioral analysis to help system administrators assess potential malware that is often missed by traditional endpoint solutions that rely on signatures.

Webroot uses a big data approach to security, backed by a network that gathers, processes and correlates terabytes of threat data in real-time on behalf of all of Webroot's global subscribers. For example, if one Webroot-protected endpoint discovers a new threat, the updated threat information is available to all covered devices automatically and in real time via BrightCloud Threat Intelligence. Competitive solutions might take days or weeks to provide this information. This access alone constitutes a distinct competitive advantage for the solution provider versus signature-based solutions.

Business Practices

To offer the best solutions, making the right partnerships is key. Emerging technology firms and vendors must make meaningful investments in both time and money to help channel partners grow. Solution providers should look for a security vendor that delivers a simplified blueprint for success, including buy-in from all levels of the vendor organization and synchronized efforts to onboard, enable and grow business.

Webroot provides its partners with personalized relationships in which the onboarding and enablement process is driven by interfacing with people who are aligned on partner success. Skilled subject matter resources are supported by co-marketing initiatives and sales support in addition to expert technical resources. Incentives, lead generation, enhanced margins for qualified partners and co-branded resources are part of the program that supports and rewards Webroot partners.

THE WEBROOT® CHANNEL EDGE® PARTNER PROGRAM

The anchor of the Webroot Channel Edge Partner Program is the Channel Edge Toolkit. This resource is an innovative set of sales and marketing tools to help you effectively grow your business. The Toolkit gives partners easy and convenient access to training, co-branded emails and datasheets, free product trials for clients, and more. Connecting to the Toolkit is fast and straightforward because no logins or passwords are required. A partner's entire sales team can have access to tools and sales materials directly from their desktop. In addition to traditional materials, the Channel Edge Toolkit sets itself apart by providing syndicated web content for lead generation and automated social media content which can automatically deliver thought leadership content within a partner's own Twitter feed.

CONCLUSION

The opportunities for resellers and MSPs to help customers meet the complex requirements of security have never been greater. Cloud-based Smarter Cybersecurity™ solutions from Webroot offer partners an easy way to take advantage of this variable threat landscape and provide an excellent building block to grow a full security practice. The combination of world-class technology, superior business practices and the Webroot® Channel Edge® program will translate into increased profitability and competitive advantage for partners who focus on security solutions. For more information, visit www.webroot.com/us/en/partners.

About Webroot

Webroot provides Smarter Cybersecurity™ solutions. We provide intelligent endpoint protection and threat intelligence services to secure the Internet of Everything. By leveraging our cloud-based collective threat intelligence platform, computers, tablets, smartphones, and more are protected from malware and other cyberattacks.Our award-winning SecureAnywhere™ intelligent endpoint protection and BrightCloud® threat intelligence services protect tens of millions of consumer, business, and enterprise devices. Webroot technology is trusted and integrated into market-leading companies including Cisco, F5 Networks, HP, Microsoft, Palo Alto Networks, RSA, Aruba and many more. Webroot is headquartered in Colorado and operates globally across North America, Europe, and the Asia Pacific region. Discover Smarter Cybersecurity solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
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