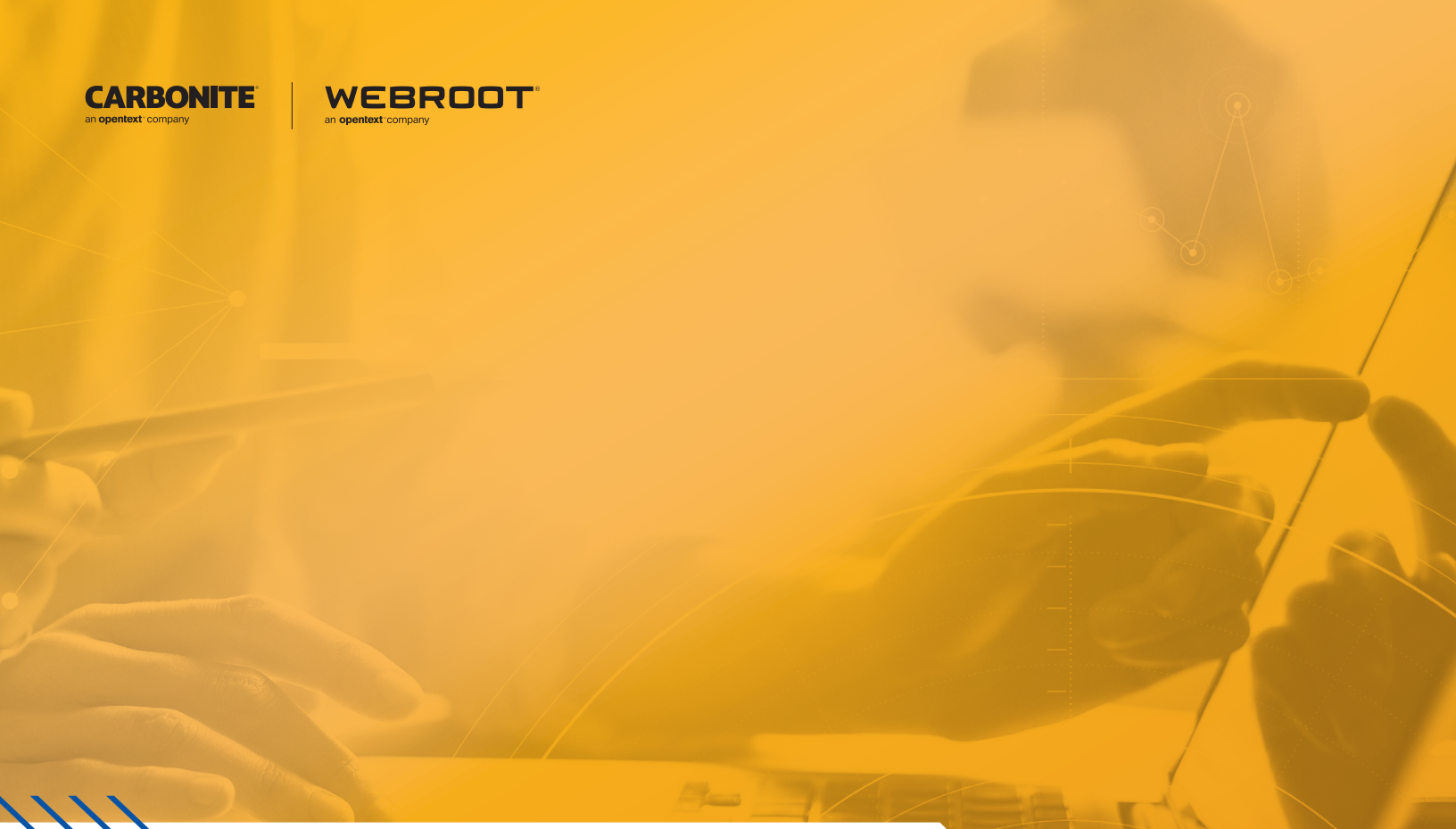
CARBONITE
an opentext company

WEBROOT
an opentext company



MSP GUIDE

Selling layered cybersecurity

In the managed services world, **relationships are key**.

Not only do your clients expect a certain level of quality in the services they receive; they also place a great deal of importance on the individual working relationship. Clients want to know they're being taken seriously as people and are being served by MSPs who understand their needs on a personal level.

By the same token, it's equally important for MSPs to align with well-known, trusted solution vendors who are committed to their partners' success. Particularly when selecting cybersecurity solutions to resell, MSPs need to carefully balance quality, ease of use and pricing. After all, today's businesses are already aware that they need cybersecurity to protect their business and customers. It's not a matter of whether they plan to invest in security at all; it's a matter of which services they'll buy with their IT budget.

Finally, MSPs have to choose a cybersecurity vendor that accounts for all the angles and multistage tactics cybercriminals use to attack. From phishing to drive-by downloads, malvertising to ransomware, social engineering to code injection, your clients' businesses are at risk every day. The cybersecurity vendor you choose needs to offer layered protection against these types of blended — or "multivector" — threats without slowing down clients' end users.

Assessing your prospects' needs

Despite the number of cyberattacks in headlines every day, and the general acceptance that using the internet poses some risk, many organizations have only a baseline understanding of their security vulnerability. The first step in selling layered cybersecurity is determining your clients' specific needs.

Questions to ask when evaluating your clients' security risk:

1. Do you think your organization could be attractive to cybercriminals? Why or why not?
2. How much do you depend on the services of partners, suppliers and other organizations?
3. How integrated are they into your IT processes?
4. Do they have the same risk threshold?
5. Which processes or systems represent your greatest assets from a cybersecurity perspective?
6. When was the last time one of your executives discussed the importance of security with your employees and stakeholders?
7. How much risk will you bear in relation to these processes?
8. What is your plan of action in the event of a security incident?

Questions to ask when evaluating your clients' financial commitment to security:

1. How much of your security budget is devoted to solving past problems?
2. How much do you spend on structural investments?
3. How much do you spend on systems and tools?

Making the case for cloud-based vs. on-premises solutions

While many companies have adopted cloud-based solutions, others have remained on the sidelines, often citing concerns about data security, IT spend and control over their critical assets. When discussing cloud-based solutions, it's important to address the pros and cons of on-premises solutions as well.

The case for cloud-based solutions

Cloud-based threat management capabilities are evolving rapidly, offering huge potential for cost benefits and operational efficiencies that on-premises solutions can't provide.

In addition to sharing the costs of infrastructure, bandwidth and expertise across clients, cloud-based solutions allow organizations to share information to correlate intelligence and block blended attacks.

Cost efficiencies

Companies can engage the resources and expertise of a cloud-based security solutions provider, paying for only what they use.

Sound investment

Investing in cloud-based solutions allows organizations to take advantage of an OPEX model to reduce capital expenses, helping them realize potential cost benefits throughout the year.

Flexible solution development

Businesses can rapidly adjust cloud computing capabilities to scale to the volume of internal and external threat information.

Data security

Cloud-based solutions can enable safer information sharing by combining analytics from multiple sources without compromising data security.

The case for on-premises solutions

Despite the clear operational efficiencies and potential cost savings that a cloud-based security solution provides, some organizations opt to deploy on-premises threat management solutions. This option does come with some advantages:

Customization

An on-premises solution provides IT teams with complete control over meeting compliance mandates. Since data and applications are stored on servers in-house, IT teams always know the location of their data and assets.

IT control

Organizations can fully customize and integrate systems to meet their specific business needs.

Unfortunately, on-premises solutions also bring a number of challenges, including:

Scarcity of cybersecurity talent
These days, cybersecurity professionals with cybersecurity expertise are in high demand.

Cost to maintain an information security team
Qualified information security professionals come with a hefty price tag (approx. $92,600, per the Bureau of Labor Statistics)

Limited capacity and scalability
Traditional on-premises systems often don't provide enough storage capacity, processing power or scalability, impeding the ability to view and analyze data across the enterprise.

Resource usage
On-premises solutions usually have a set fee, regardless of how much the organization uses.

Partner benefits with multivector protection from Webroot

Webroot's combination of advanced, cloud-based business endpoint protection and threat intelligence can help organizations identify and respond to multivector threats more quickly, maximize IT resources and reduce overall operating costs. This key differentiator brings a competitive advantage to your service offerings and enables successful value-based selling.

With Webroot, you can:

- **Protect** clients' networks and endpoints from multivector threats that span PCs, laptops, smartphones and even flash drives
- **Alert** IT, managers and employees about the latest security threats and trends
- **Launch** Security Awareness Training courses to transform end users from your weakest security link to a strong first line of defense
- **Stop** zero-day malware attacks
- **Set policies**, view activity, create and run reports and enforce security policies in one straightforward, centralized console
- **Enforce** security policies for any remote or on-site devices connecting to the network

The Webroot Partner Edge MSP program

The Webroot Partner Edge program provides the industry-specific tools, security and threat intelligence services, training, integrations, certifications and platforms you need to ensure trust and reliability with your customer base. By partnering with Webroot, MSPs get access to innovative resources that help effectively grow your MSP business, including:

- Marketing toolkit and sales resources
- Lead generation and an exclusive partner community
- Co-branded emails and content syndication
- Marketing funds and activity reimbursement

Endpoint protection

- <5 MB agent deploys in seconds
- No reimaging and no signature updates
- Simple online management and RMM/PSA integration
- Zero conflicts and zero infrastructure to maintain

DSN protection

- 100% cloud-based, no servers, hardware or software
- Stops threats at the domain level, before they hit endpoints
- Backed by Webroot BrightCloud® Web Classification
- Enforces internet usage policies seamlessly
- Adds a revenue stream and reduces costs

Security awareness training

- Engaging, interactive courses
- Proven efficacy for reducing phishing clicks
- Fully customizable phishing simulator with +200 templates
- Regulatory compliance courses included
- Microsoft® Azure AD onboarding and auto-enrollment

Flexible cloud-based management

Webroot solutions and security awareness training use cloud-based management, which requires no on-premises hardware or software. The Webroot console provides MSPs with a hierarchical view of the endpoints under their protection. It gives them global visibility over their customers, as well as the ability to drill down to group and individual user views. It also enables MSPs to see in real time how many devices each customer deploys, or whether any endpoints need attention.

Competitive comparison

Installs in an average of 3 seconds.[1]

Uses over 50x less hard disk install space than Bitdefender®[1]

Uses 25x less memory than Kaspersky® during system idle[1]

Scans 113x faster than Sophos® during scheduled scans[1]

Needs over 5x less memory during an initial scan than ESET®[1]

Become an MSP partner
To learn more about how multivector protection from Webroot can help you keep clients safe and become more profitable, visit:
www.webroot.com/MSPpartners

[1] PassMark Software. "Webroot® Business Endpoint Protection vs. Eight Competitors." (March 2019)

Contact us to learn more — Webroot US
Email: wr-enterprise@opentext.com
Phone: +1 800 772 9383

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training and data backup and disaster recovery solutions, as well as threat intelligence services used by market-leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia and Asia. Discover cyber resilience at carbonite.com and webroot.com.