WEBROOT
Smarter Cybersecurity™

3 TIPS TO HELP MSPS MAKE MONEY WITH DNS PROTECTION

DNS filtering can reduce the number of malware infections and security breaches by up to 88%. Imagine the cost savings for you and your clients.

Uncontrolled internet access is a big risk for your clients. But proxy solutions are expensive to maintain and manage, and cost-effective alternatives are few and far between. That means your clients may rely on endpoint security alone to protect their businesses from web threats, but as an MSP, you know that's not enough.

With a DNS-layer security solution, you can protect your clients from up to 88% of web-borne malware before it even hits their endpoints or networks. Read our checklist for 3 simple tips to help MSPs like you sell the value of DNS protection to your clients.

Underscore the importance of shared responsibility.

DNS protection is an additional layer of security that will reduce the number of security incidents your clients face. In turn, this reduces costs associated with infections spreading through open ports, as well as user productivity loss and overall business downtime.

Remind clients that the average cost per security incident is approximately $80,000,[1] while the cost of adding DNS protection is around $1.50 per user per month, or $20 per user per year. That means that, for a minimal investment in high-quality, low-cost DNS protection, the gains are considerable.

Pro tip from our MSP partners: *You can offer DNS protection as part of a premium security package, for an additional cost, or you can include it as a standard component of your bundled security offerings alongside endpoint security and patching services. With either pricing model, MSPs and businesses alike benefit from savings due to fewer incidents and service calls.*

[1] BBB.org "Cyber Security." (May 2018)

Remind clients of regulatory compliance requirements.

The different industries in which your clients operate may have compliance requirements. Additionally, human resources departments may have requirements of their own. With a DNS protection solution, you can restrict internet use across a network, by group, or even at the device level.

You may be surprised just how many of your clients require this kind of flexibility. For example, any business offering healthcare services is subject to HIPAA. Organizations conducting business in Europe are subject to GDPR. In the U.S., HR teams often have acceptable use policies to ensure Title VII and safe workplace protections are in place. These are just a few of the numerous examples of workplace compliance concerns modern businesses face.

Did you know: *Businesses that operate internationally may be subject to international data protection laws. Even if your clients are U.S.-based, if they conduct business with anyone outside of the U.S., they need to be aware of and comply with that country's specific regulations.*

Show, don't tell.

Network-level threats represent a real danger for MSPs and their clients. DNS calls can be used to steal credentials, launch fileless attacks, compromise data, and much more, while remaining relatively well-disguised in ordinary network traffic. Additionally, activities like streaming media and torrenting can present both cybersecurity and major compliance risks, not to mention the effects they can have on corporate bandwidth.

If your clients aren't sold on the importance of DNS protection, offer them a free trial and share reports on sites visited, DNS requests blocked, etc. The results of the trial will likely provide the evidence you need to convince the skeptics.

Note: *Torrent sites continue to be major sources of malware,[2] not to mention being bandwidth hogs and productivity sinks. Your clients might be surprised to learn what kinds of risks their end users—employees and guests, alike—are unwittingly taking.*

[2] www.bleepingcomputer.com/news/security/fake-movie-file-infects-pc-to-steal-cryptocurrency-poison-google-results