WEBROOT
Smarter Cybersecurity™

DNS Protection: An Overlooked Layer of Cybersecurity

How MSPs Can Protect Clients at the Network's Edge

Introduction

Uncontrolled internet access is a high-risk activity for any business, regardless of size, but it is particularly dangerous for the small to medium-sized businesses (SMB) that make up a managed service providers' client base. Unfortunately, endpoint security alone is no longer enough to keep clients safe from modern cyberattacks. And, as MSPs well know, remediating threats that have successfully infiltrated the network is challenging and extremely time-consuming. That's why today's MSPs are increasingly turning to services that can stop threats before they hit the network.

The domain name system, or DNS, is a hierarchical naming convention for services, computers, and any other resources connected to the internet or a private network. DNS servers take text-based browser inputs and translate them into the unique internet protocol (IP) addresses that direct devices and services to the desired site. By redirecting end user web traffic through a cloud-based, domain-layer security solution, MSPs can finely tune and enforce web access policies, ensure regulatory compliance, and stop nearly 90% of threats at the network's edge.

When MSPs layer DNS protection with endpoint protection, they give clients comprehensive security that can handle modern threats, without imposing huge cost or bandwidth burdens. Unlike internet proxy servers and web security appliances, which can be expensive to configure and manage, DNS protection solutions are lightweight and easy to deploy and maintain. That makes them an ideal fit for MSPs, who must not only consider the initial purchase cost, but also the time required to install, configure, and maintain a new security solution.

Of course, not all DNS protection solutions are created equal. When selecting a DNS security product, there are three key criteria MSPs should consider:

» **Efficacy:** Does the solution deliver comprehensive, effective real-time protection based on up-to-date threat intelligence?

» **Ease of use:** How quick is the deployment process? Is the solution easy to configure? Is it scalable?

» **Flexibility:** Does it include policy management to ensure HR and regulatory compliance (HIPAA, PCI, GDPR, etc.)? Will you be able to use it to enforce web access policies and improve end user productivity?

Why DNS Protection is Crucial

It's clear that organizations across the globe are facing a rapidly escalating network security problem. According to the 2018 Global Threat Landscape report from Arbor Networks, 87% of service providers[1] reported having experienced a distributed denial of service (DDoS) attack during 2017.

Similarly, a recent report from EfficientIP queried 1,000 organizations around the world and found that 76% of the respondents were subject to a DNS attack over a 12-month[2] period. Citing the need for attackers to become more creative as organizations grow more secure, the report notes, "As DNS is mission-critical, but open by design and typically not monitored, it has become the perfect target to exploit it in as many ways as possible. Despite the reality of risks, companies are not sufficiently aware of the diversity of the menace."[2]

Indeed, networks are being attacked via DNS for a broad variety of criminal purposes. DNS is a primary enabler for the following exploits:

» **Botnet command and control (C&C):** Can be used to perform DDoS attacks, steal data, send spam, and allow the attacker access to the device and its connection; once infected, bots will perform DNS queries to connect with the C&C server for further instructions and/or to pass harvested information.

» **Advanced Persistent Threat (APT) attacks:** Designed to spread, morph, and hide within IT infrastructure to execute a long-term strategic attack; many require low-level communications with a C&C server to direct actions and exfiltrate sensitive data.

» **Ransomware:** An increasingly prevalent threat, often uses DNS-reliant communications with C&C server to initiate payload download.

» **Web-based threats:** Over 85% of malicious links[3] are hosted on legitimate compromised sites.

Other DNS-based attacks include DNS amplification, DNS tunneling, cache poisoning, and name collisions; the list goes on. Unfortunately, a key issue is that many organizations simply leave ports 80 and 443 open to allow DNS traffic to find its destination, effectively leaving the network's front door wide open.

Choosing a DNS Security Solution: Efficacy

When an MSP selects a domain-layer security solution, it goes without saying that effective client protection is the number one priority. In the past, many businesses deployed web proxies to achieve the same goal, but those solutions brought numerous drawbacks:

» Inconvenient deployment, require hosting and managing

» Policy servers are complex to configure, often underutilized

» Web filtering inaccuracy, can omit newly-compromised sites

» Expensive to scale across multiple locations

» Causes slowdowns when parsing site content, enforcing layers of policy

By contrast, DNS-based solutions lack the deployment complexity and scalability issues of proxy solutions—no on-premises servers are required—and are much simpler to operate. And because they only look at top-level domains, DNS-based security solutions can make decisions and apply policies in a fraction of the time required by proxy-based solutions.

However, there are distinct differences between the various DNS-based security products available to MSPs. Many of the companies who now offer these products began as content filtering and proxy vendors, and have only recently expanded into domain protection. This may be problematic, as they may lack the security background and access to the quality and quantity of threat intelligence that more experienced security vendors gather.

Simply put, the level of protection any DNS security solution can provide is ultimately determined by the breadth, depth and update frequency of its threat intelligence. The more a DNS protection product is integrated with an established security vendor, the more likely it is to accurately identify and block malicious and unwanted websites.

Choosing a DNS Security Solution: Ease of Use

When MSPs standardize security solutions and procedures across multiple client sites, they minimize the amount of time IT staff must spend deploying and managing those products. And when they boost efficiency, MSPs also boost their profitability. As such, the ideal DNS protection product would integrate with the MSP's existing endpoint security management console to simplify deployment and administration tasks, compared to standalone DNS security solutions. This latter point is noteworthy; taking the time to master separate management consoles for various security solutions can significantly increase an MSP technician's workload.

Initial deployment should take only minutes, only requiring the MSP to direct its clients' internet traffic through the DNS protection service's domain name system security extension servers to check and control each client's web access. The ability to customize web access policies for each client using both global and site-based policies is a key feature that MSPs should demand.

Choosing a DNS Security Solution: Flexibility

While delivering maximum security is the obvious objective of a DNS protection solution, it should also give MSPs the flexibility to accommodate specific policy requirements for each of their clients. This policy management capability is particularly valuable in terms of meeting a client company's compliance needs, whether based on internal standards or industry regulations, such as HIPAA, PCI, and GDPR.

For greater convenience, a DNS security product should include an extensive range of preset policies and granular filtering options to appropriately manage users' access levels to dangerous or unwanted websites. Productivity policies can help an MSP's clients significantly boost their end user efficiency by limiting online distractions. In addition, using policies to block undesirable types of traffic, such as media streaming, can dramatically improve their network bandwidth.

Other key features MSPs should look for in a DNS security solution include:

- **Ability to use customizable block pages:** Enables MSPs to use either their own or client-specific block pages when end users try to access blocked content.
- **Whitelist/blacklist support:** Allows creation of customized overrides based on a client's specific needs.
- **Ability to assign a different policy to by IP or user:** This lets MSPs easily secure a client's guest network or apply more granular user policies to staff both outside and inside the corporate network.
- **Guest WiFi protection:** Many organizations offer guest/public WiFi networks for visitors or customers in a client's business (such as a coffee shop, retail store, gym, airport, or doctor's office). These access points are equally vulnerable to attack and demand the same level of protection as corporate networks, but pricing that reflects the number of users is often unknown. Look for a solution that can also secure your clients' guests.

The Webroot Answer to DNS-layer Security

Webroot SecureAnywhere® DNS Protection offers a simple yet effective way to prevent everyday web usage from becoming a major security risk. DNS Protection takes only minutes to deploy, requires no on-site hardware or software, and is integrated directly into the Global Site Manager console for MSPs. This is the same console MSPs use to administer all Webroot SecureAnywhere protection.

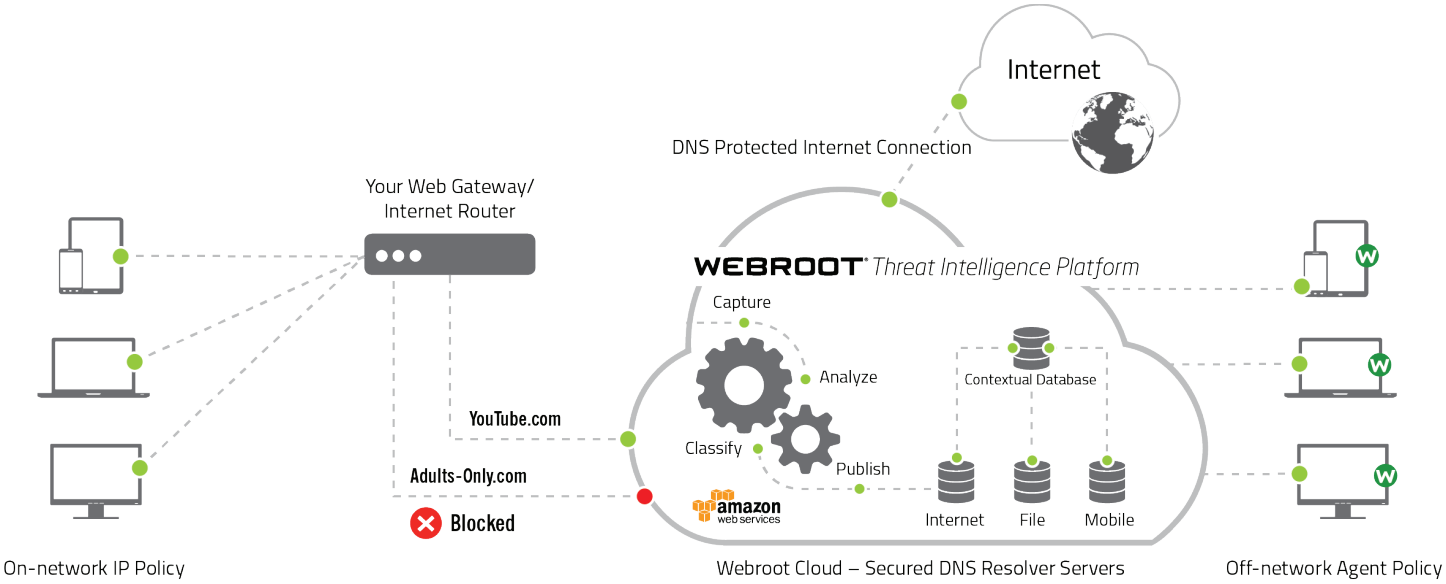
DNS Protection also enables administrators to finely tune web access policies using both global and site-based policies. By using the intuitive drop-down menu to fill in a few client and site IP address details, then performing an easy command line service validation test, the service is live and operational right away. Each client IP address can be given a different policy, so securing a client's guest WiFi networks or applying more granular site policies is smooth and straightforward.

Webroot SecureAnywhere® DNS Protection is powered by the Webroot® Threat Intelligence Platform— an advanced, cloud-based security platform, which is enhanced by a contextual analysis engine to correlate information for deep insight across the digital landscape. This advanced self-learning platform continuously scans the internet and incorporates inputs from millions of sensors, making it possible to quickly and accurately identify previously unknown threats at an unprecedented scale.

Webroot's DNS Protection provides an additional layer of web filtering protection from sites that host malware or spyware, and also enables partners to offer far more granular control over the types of accessed at client sites. The service enhances our partner's network security solutions by increasing real-time protection against known malicious threats, unauthorized network access, and Distribution Denial of Service (DDoS) attacks, and drastically improves their visibility and control over internet access.

In particular, DNS Protection's URL filtering is supported by Webroot BrightCloud® Web Classification data. This URL database is the largest of its kind, and the service continually classifies over 600 million domains to update the database in near-real time. Webroot analyzes and categorizes websites at the rate of over 5,000 URLs per second. In fact, the service scans the entire IPv4 and in-use IPv6 space and classifies over 95% of the internet at least three times per day. It continually analyzes and classifies over 4 billion IP addresses, 27 billion URLs and uncovers more than 45,000 malicious URLs, 6,000 new phishing sites, and over 100,000 new malicious IP addresses per day. (These threat intelligence services are utilized by over 65 leading network and security vendors worldwide.)

Part of what makes Webroot threat intelligence so powerful is that, instead of focusing on a single type of threat data, Webroot analyzes the connections between disparate internet objects. This contextualization ensures that no internet object is reviewed in a vacuum, but instead in the context of its relationships, in a "guilt by association" model, to understand not only the level of risk it currently poses, but also its potential for future malicious activity. For example, if a user runs a mobile app that tries to access the



How Webroot SecureAnywhere® DNS Protection works

contact list and transfer it to an IP address, the malicious behavior of the app would impact the reputation score of the IP address. This, in turn, would affect the reputations of any URLs that are connected to that IP. This ability to correlate current associations among objects with history on how millions of objects have behaved over time is why Webroot threat intelligence can predict future sources of emerging threats.

Webroot offers 80 URL categories to allow service providers to determine the right usage policies for their clients. By leveraging industry-leading Webroot intelligence and services to automatically block malicious websites and filter undesirable website types, you can drastically reduce the number of malware threats that infect your clients' networks and endpoints.

Established in 1997, Webroot has a long track record of delivering high integrity IT security solutions to the global market. With any Webroot service, customers and partners benefit from over 20 years' experience in cybersecurity and threat intelligence.

Conclusion

As the threat landscape becomes increasingly sophisticated, it's clear that a layered approach to cybersecurity is key to delivering superior results. By deploying cloud-based, domain layer security that extends endpoint protection into the network, MSPs can ensure that most internet threats are blocked before they even reach their clients' endpoints. With DNS protection at the network edge and endpoint protection for network-connected devices, MSPs can provide powerful, comprehensive security to clients that is easy to manage and cost-effective.

[1]Arbor Networks. "Insight into the Global Threat Landscape: 13th Annual Worldwide Infrastructure Security Report." (January 2018)

[2]EfficientIP. "The 2017 Global DNS Threat Survey Report." (June 2017)

[3]Webroot Inc. "Quarterly Threat Trends, June 2017." (June 2017)

About Webroot

Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.

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