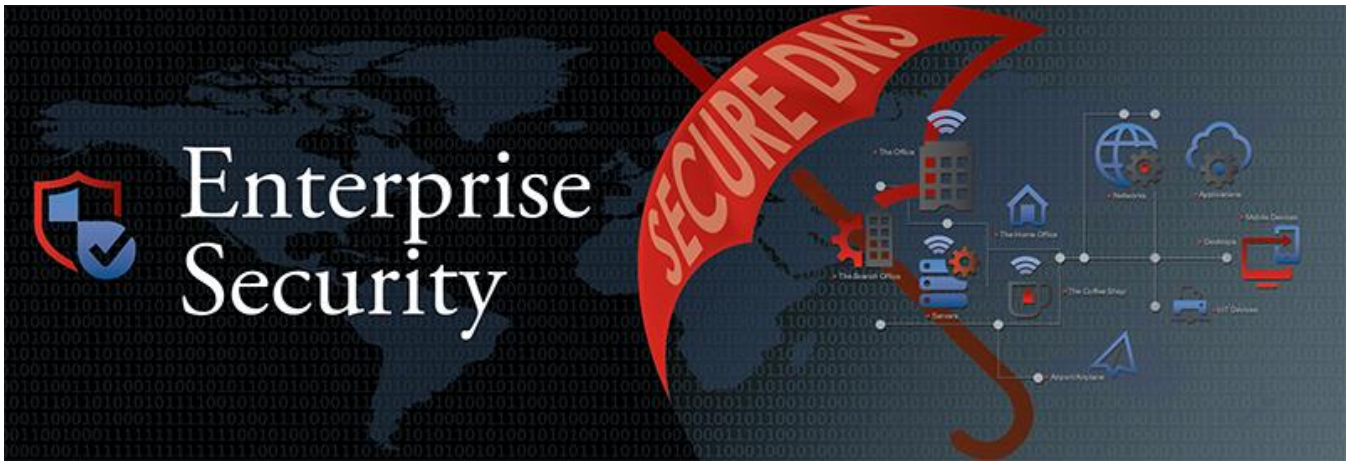



# What Would an Umbrella Approach to Security Look Like for Your Enterprise?

## Part 1: Leveraging DNS to Improve Your Security

*Ron Temske, Vice President, Security Solutions, Logicalis US*

The starting point for enterprise connectivity to anywhere is the Domain Name Services or DNS. Why not start there for cybersecurity? The purpose of DNS is to resolve names, which humans can remember, into IP addresses used by computers and other connected devices. Comparing DNS to a phone book (*Ed. For those of you old enough to remember them!*), or your contact lists in Outlook or your phone, is a good analogy.

It's difficult to remember phone numbers for all your family, friends, work colleagues, suppliers and customers, but you certainly remember their names. So, while none of us we would think to type http://54.239.25.208/ into our browses, we would have no problem remembering and typing http://www.amazon.com/ when we want to go shopping.

DNS is involved any time a domain name is accessed from a device. This isn't specific to just browser or http traffic, but includes any resource call to a domain from any connected device. And for that reason, DNS is both an asset and a liability.

**Truths About DNS**

As the central internet phone book, DNS can be involved in attacks in several ways. I'm going to take a few technical liberties and skip a lot of details about authoritative versus recursive, versus caching DNS servers and the role of the localhosts file. But all the concepts I will discuss are accurate. Here are a few ways that DNS can become a vulnerability to your enterprise:

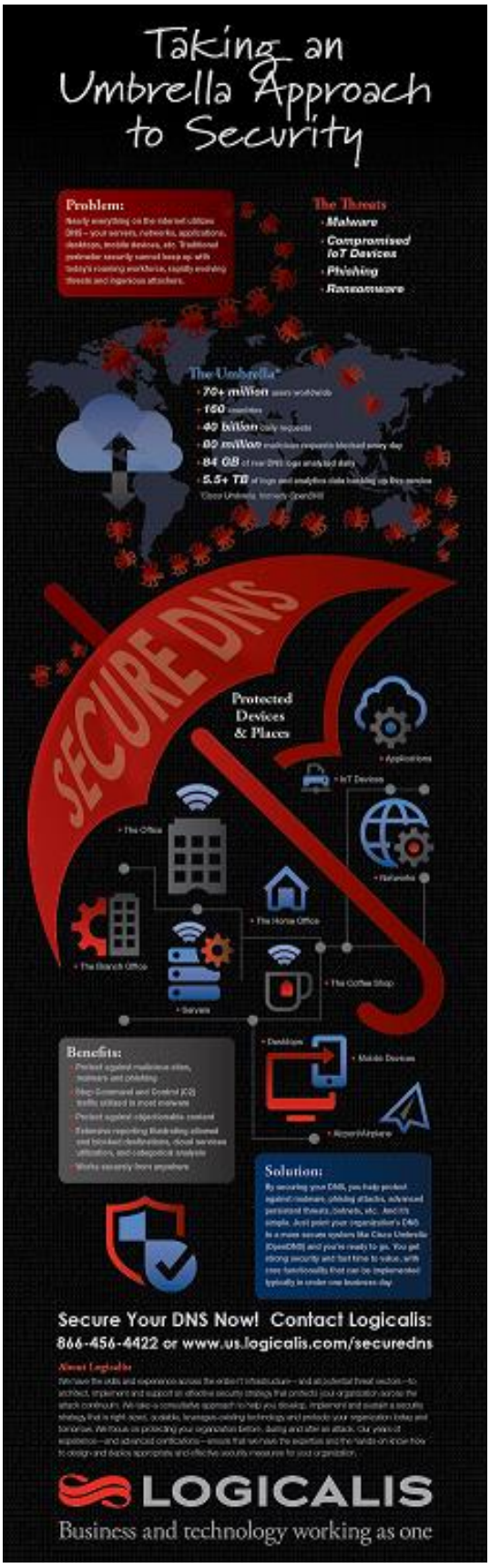
- **DNS caches can be "poisoned."** The DNS cache can be corrupted to misdirect queries to incorrect sites. In this case, a user types www.example.com in his browser, but since the DNS cache was corrupted, he gets sent to www.reallybadsite.com instead.

- **DNS can be used for typo cons and domain squatting.** These attacks use domain names that appear similar to a valid domain name, hoping users won't notice. For example www.1inkedin.com. Also common is using a legitimate domain name, but adding an extra character or word.

- **DNS can be used in phishing attacks.** Any attempt to lure a user to a malicious site can combine the typo con/domain squatting method described above to make the user believe they're going to a proper site. It's also common to mask a malicious domain or IP address behind a trusted domain address. These are easy enough to spot – hover over any website domain address before clicking on it and see where the hyperlink resolves. The link and text should be the same – or at least it should take you to the domain that you expected!
- **DNS can be leveraged for Command and Control (C2) malware.** DNS is used in many forms of malware, as most have some type of "call home" function to advise that the malware is in place.
- **DNS doesn't discriminate.** Users don't always know that a site is malicious and neither does DNS. A user may visit a "rogue" site intentionally, often in conjunction with a phishing attack, a "free" offer or another compelling link. This can might be accomplished by setting up a malicious site with a helpful sounding name (e.g. www.reallyhelpfulsitehere.com).

These types of attacks are focused on the end users, but there are also attacks directed against the DNS infrastructure which can result in a Dedicated Denial of Service (DDoS) attack among others. This has potentially devastating consequences: If DNS services are broken or unavailable, this effectively shuts down the entire network for affected users.

In Part Two of my article, we will take a look at a potential solution to these challenges: A Secure DNS that acts as an umbrella to protect places, spaces and devices from threats via the DNS services.




*Click for a larger image* ►

## Part 2: A Secure DNS

We have discussed what seems like an insurmountable obstacle. While we require DNS to resolve IP addresses, this also allows it to be leveraged for a variety of malware and attacks. It's estimated that 97 percent of all attacks involve DNS in some capacity, so the ability for DNS to play a role in security is extensive.

That's the premise behind Cisco Umbrella, formerly OpenDNS, which replaces the default DNS servers accessed by your enterprise (typically provided by a corporate server or your ISP) with a secure DNS backed by an entire intelligence community.

By using threat intelligence and cloud scale analytics, and leveraging how the DNS protocol operates, the Cisco approach succeeds in protecting users from being exposed to attacks and malware – no matter where the user or the malware is located.

Here are just a few of the ways this umbrella approach to DNS can protect your enterprise environment:

- Keeps a continuously updated record of malicious sites, so if you click on that link for www.1inkedin.com, the DNS prevents you from being sent to the site.
- Keeps a continuously validated database of site addresses which prevents a DNS cache poisoning attack from succeeding.
- Provides filtering ability for undesirable content (for example blocking all requests for adult content).
- Blocks the "call home" request from many forms of malware, effectively minimizing the impact of that malware.

- Works whether a device is on the corporate network or even while on guest networks when using AnyConnect or roaming client.

- Provides an extensive reporting dashboard that can provide a view into details such as SaaS consumption. For instance, you could view not only that SalesForce.com is being used, but who on your network is using it.

- Provides an Investigate Console to protect users and enable IT staff to understand the threat landscape with details such as phishing site vs adult content site.
- Integrates Cisco Umbrella/OpenDNS with Cisco AMP ThreatGrid and other technology partners such as Check Point to enable other solutions' threat intelligence into the platform.

There are few solutions that can provide this level of impact to security with as rapid a time to value. I am frequently asked about how to better protect home networks, so I am happy to note that a basic version, Cisco Umbrella Personal is free for personal use. You can view details at https://www.opendns.com/home-internet-security/