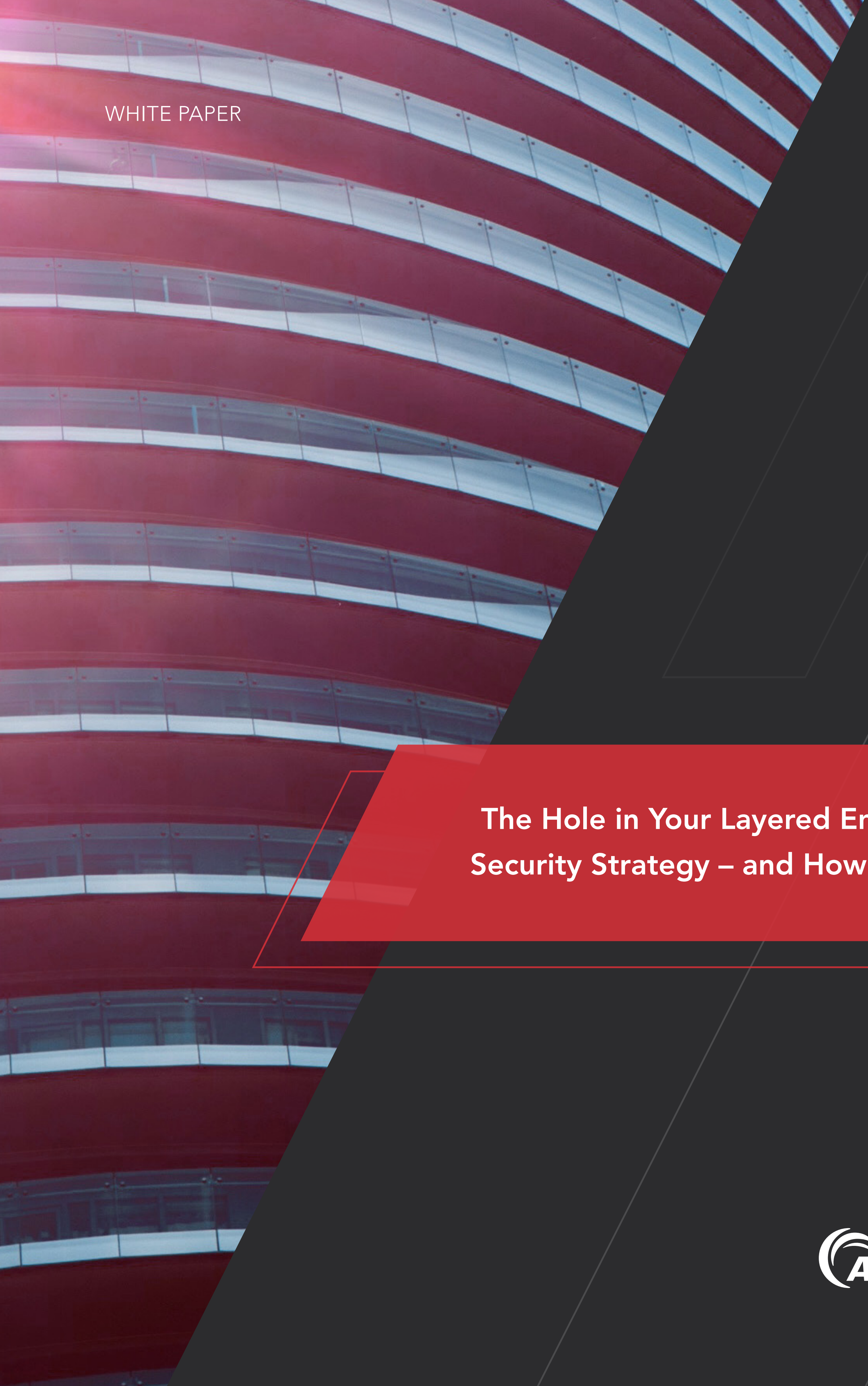
WHITE PAPER



The Hole in Your Layered Enterprise Security Strategy – and How to Fix It

Executive Summary

The challenges that IT security professionals face are growing more complex by the day. Security threats are constantly evolving. The volume and rate of targeted threats, such as malware, ransomware, DNS-based data exfiltration, and phishing, are increasing. And the fact that companies no longer consist of employees who work a standard, full workday in the same, central location (employees are onsite and remote, full-time and part-time, and located all around the world) further complicates enterprise security. When you consider that most enterprises also extend network access to contractors, partners, and suppliers, the situation becomes even more convoluted.

To confront these challenges, best-in-class enterprises are scrapping traditional approaches like perimeter security and "trust but verify," knowing they aren't comprehensive enough to deal with today's sophisticated attacks. Instead, businesses are moving toward a zero trust security model, which jettisons the notion of a trusted "inside." This architecture assumes that every user and device is equally untrusted, and that "inside" and "outside" boundaries have dissolved.

An integral component of zero trust is deploying a layered enterprise security (LES) strategy, which relies upon multiple levels of defense to safeguard against threats, instead of a single tier of protection. Most security professionals agree that no single product provides 100% resistance against all threats, nor is it possible to achieve complete resilience against today's incessant and incentivized cyberthreats. Therefore, it's a best practice to employ an LES strategy to help ensure a depth of defense.

However, many companies that have migrated to an LES strategy still fail to protect their Domain Name System (DNS) infrastructure, a critical Internet protocol that was never designed with security in mind. The open nature of DNS — and recursive DNS (rDNS) specifically — makes it a primary and relatively easy target for attacks, including malware campaigns and data exfiltration. It's crucial that companies build out and shore up their LES strategy to include and better defend DNS.

In this paper, we'll examine the particulars of layered enterprise security, the critical reasons why DNS should be monitored and protected, and the key benefits of DNS-based security — including how quick and easy it is to deploy.

Layered Enterprise Security + Zero Trust = Your Best Defense

WHAT EXACTLY IS LAYERED ENTERPRISE SECURITY?

When considering why layered enterprise security is critical, it's helpful to think about securing a physical environment. Imagine there was a constant threat of break-ins by sophisticated criminals to a property you own. Would you rely solely upon an alarm system? Probably not. You'd likely have myriad protections such as an alarm system, motion detectors, guard dogs, maybe even armed guards. Perhaps you'd keep your most valuable items in several advanced safes, and doors to each room might have complex locks. Essentially, you'd employ many types of protection at various locations on premises to keep your property secure.

The same concept applies to your enterprise's IT security; experts agree that utilizing diverse layers of fortification is the best way to detect bad actors and repel attacks. Since cybercriminals probe for weaknesses in enterprises' defenses, you can't put all of your confidence in a single security solution. And as previously mentioned, there is no one solution that can safeguard your company against every manner of cyberattack, making an LES approach critical.

A defense-in-depth strategy helps ensure that, in the event of a threat evading one security mechanism, other layers of protection might still identify and block the threat. IT security expert Jerry Shenk explains:

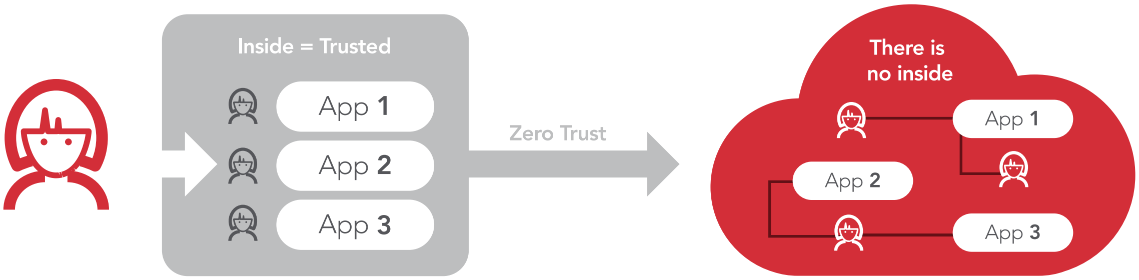
> There is no such thing as a silver bullet, and it takes many technologies and processes to provide comprehensive risk and security management … today's attackers strike across multiple layers. That means that our security must also be layered.[1]

Let's consider a common IT security approach: Anti-virus software. Installing it on laptops and desktops will definitely protect a company against some malware attacks. However, today's malware is so advanced that relying on that single mechanism will leave a company vulnerable to those threats specifically designed to evade endpoint anti-virus.

With a tiered approach to security, any failure of endpoint anti-virus to discover and deflect malware may not mean a breakdown in the entire security system. At a minimum, utilizing multiple defense techniques will slow an attacker and improve time to detection; at its best, layered enterprise security will completely thwart an attack, stopping its progression through enterprise systems before any damage is done.

LES: An Essential Part of a Zero Trust Approach

WHILE NOT A NEW IDEA, ZERO TRUST HAS INCREASINGLY GAINED TRACTION, AND FOR GOOD REASON.



Originally championed by Forrester Research, a zero trust architecture assumes that there is no "inside" and that everyone and every device is equally untrusted. This security framework considers every user and device that could touch your network to be hostile and potentially compromised, and dictates that you are always authenticating and authorizing. Instead of "trust but verify," the rule is to "verify and never trust." And the more layers of security you have, the stronger your zero trust security model will be.

> CIOs must move toward a Zero Trust approach to security that is data-and identity-centric — and in our view is the only approach to security that works.[2]

In its report, Zero Trust Security: A CIO's Guide To Defending Their Business From Cyberattacks, Forrester Research asserts that all enterprises must be "working on the assumption that all traffic is threat traffic until you've authorized, inspected, and secured it, regardless of whether an internal or external party is accessing your systems and regardless of whether the data is located within your data center or in the cloud."[3]

If all traffic must be considered threat traffic, why are enterprises leaving recursive DNS — which resolves millions of queries per day — completely unprotected?

Your Unprotected Recursive DNS is a Win for Malicious Attackers

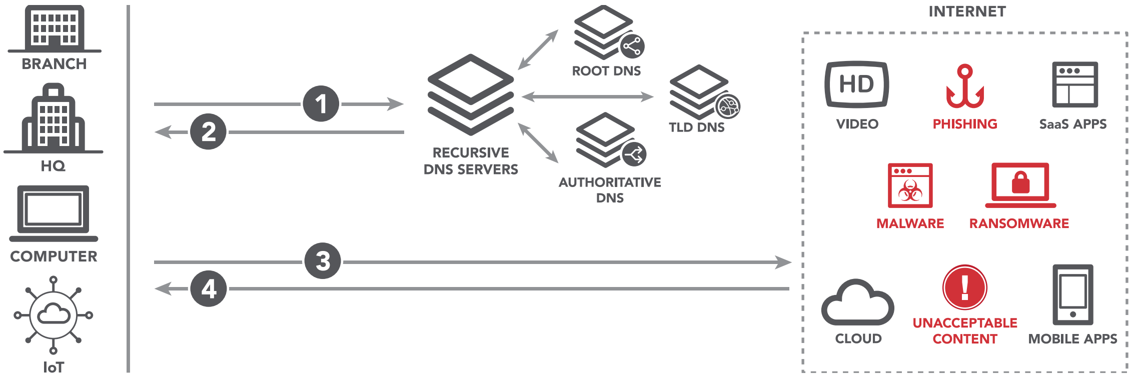
Many organizations recognize the value in adopting a layered enterprise security approach and, as such, are deploying multiple security solutions, including firewalls, secure web gateways, sandboxing, intruder prevention systems, and endpoint anti-virus. Yet, malicious actors are persistent and continue to gain access to enterprises by exploiting security weaknesses. One such gap: the vulnerable back door that is recursive DNS.

> The Internet of Things (IoT) is composed of billions of Internet-connected devices around the world that are constantly making DNS requests. As the number of IoT devices skyrockets — projected to reach 20.4 billion in 2020[4] — your exposure to cybercriminals will also climb. Currently, 80% of IoT devices are not tested for security vulnerabilities,[5] making the IoT a prime target for bad actors looking to exploit the security holes inherent in DNS.

Why is DNS such an appealing target for bad actors?

- **INHERENTLY VULNERABLE:** Though it makes the Internet fast, efficient, and navigable, DNS is innately open, utilizing unfiltered ports 80 and 443. As previously discussed, this exposure is exacerbated by the fact that individuals and corporations alike often leave it unprotected.
- **UBIQUITOUS:** Almost every action taken on the Internet begins with a DNS request that maps domain names to IP addresses. This means that any time your enterprise's users or network-connected devices (including IoT devices) perform an Internet request — from web browsing to email to online retail to cloud computing —they use DNS.
- **UNDISCERNING:** DNS itself has no intelligence, so it will blindly resolve requests for both good and malicious domains.

DNS: THE STARTING POINT OF EVERY INTERNET REQUEST



Bad actors develop malware that is specifically tailored to exploit these qualities as well as evade existing security layers — such as firewalls, secure web gateways, anti-virus programs, and threat intelligence services — that don't typically use DNS as a control-point. As a result, the DNS infrastructure often provides an avenue through which cybercriminals can launch targeted threats against enterprises, including phishing attacks, malware and ransomware campaigns, and data exfiltration.

> Since a large percentage of compromises start with user interactions, it's necessary to observe and orient network defenses to quickly thwart attack activities that originate at the user level.[6]

It's clear that in order to have a layered enterprise security approach that accomplishes the mission of zero trust, you must proactively monitor and control your DNS. If it is left unchecked, it's only a matter of time before one of the millions of daily Internet requests made from your network resolves to a malicious download. The potential scenarios are daunting:

- **ONE COMPROMISED DEVICE** can quickly become a gateway for companywide infections that can slow or crash your network, spy on business activities, steal information, delete data and files, turn devices into "zombie computers" that host illegal content, are used for crypto mining, engage in DDoS attacks, and more.

- **MOST MALWARE** will send a request back to its command and control (CnC) server from your network for further instructions. Given the unfiltered and open nature of DNS traffic, these malicious communications will go undetected, bypassing all network-level security.

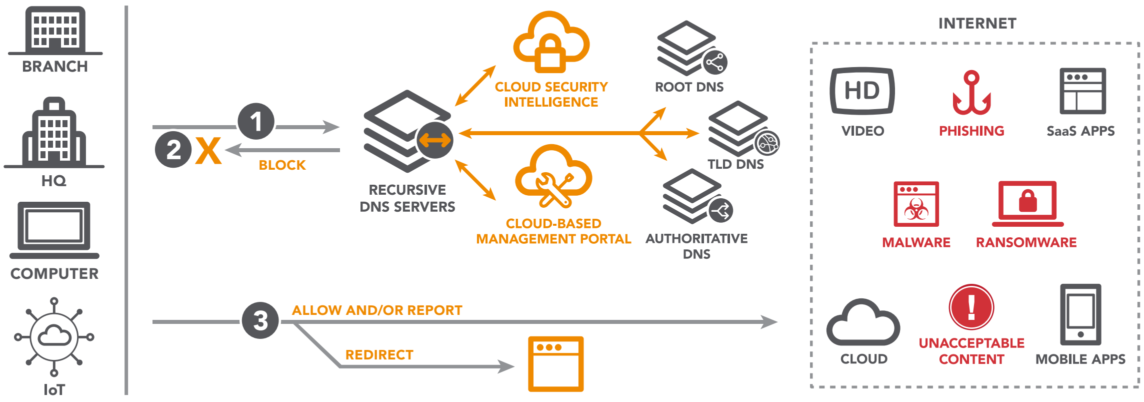
- **THROUGH DNS,** bad actors can exfiltrate financial records, social security numbers, credit card information, intellectual property, and other sensitive data. These data packets are encrypted, compressed, chopped, and then transmitted outside of your network.

How a DNS-Based Security Solution Helps Protect Your Enterprise

So, how exactly do you fortify your enterprise security, with an eye to better protecting the security gap that DNS presents? You turn DNS into your initial line of defense.

IT organizations are employing third-party DNS-based security solutions that act as an enterprise's recursive DNS server, examining every DNS request to determine if it's querying a safe or a malicious domain. These solutions can transform DNS into a control-point and valuable security asset that proactively protects your network.

EMPLOYING A DNS-BASED SECURITY SOLUTION



DNS resolvers perform one core function: They take a human-readable domain name and find the corresponding IP address of the server where the resource is located. The resolver will either find the IP address in cache or will use a recursive DNS server to search through a hierarchy of DNS name servers and authoritative DNS servers. Through utilization of a DNS-based security solution, your organization will no longer resolve these DNS requests blindly.

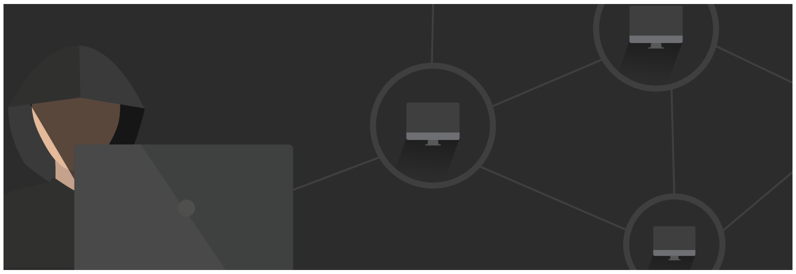
The DNS-based security solution will act as your enterprise's DNS server, checking domain names against comprehensive and up-to-date threat intelligence before resolving the IP address. It's crucial to understand that your DNS-layer security solution is only as good as its threat intelligence.

Therefore, your solution's raw, high-quality threat data should be supplemented by continuous evaluation, research, and validation by dedicated security experts. This intelligence should be augmented by external feeds from security partners as well as public data, such as WHOIS and registrar information. The combined data set should be analyzed using advanced, real-time, and offline behavioral analysis and proprietary algorithms on a rolling basis.

The threat intelligence that your DNS-based security solution is built on should be able to:

- **DELIVER** intelligence that is focused on threats that are current and relevant, as opposed to domain coverage.
- **DRAW** from a broad and comprehensive volume of DNS and IP traffic so it is able to quickly identify global threat trends and detect threats before they are widely active.
- **DIFFERENTIATE** between dedicated domains that have been created specifically for malicious use and legitimate domains that have been compromised.
- **PROVIDE** a very low rate of false-positive security alerts so that your security team isn't wasting time and effort investigating them.

Your DNS-based security solution should constantly monitor and dissect your DNS logs in real time, checking them against this robust data set, and should therefore quickly identify anomalies. Suspicious, odd, and superfluous requests will be flagged and blocked — take, for example, a single printer suddenly making thousands of rDNS requests or an employee's laptop issuing hundreds of queries at 3:00 in the morning — mitigating an issue or intrusion before it inflicts damage to the corporate network.



The intelligence, monitoring, and filtering provided by a DNS-based security solution are not activities that an organization can effectively achieve on its own. This is due to volume and visibility. One device makes several thousand recursive DNS queries per day — now multiply that by every user and device. Volume often prohibits DNS log entry into a security information and event management (SIEM) system. Exporting logs and cutting in data from multiple sources to view DNS traffic in aggregate is onerous, and digging through this data to identify anomalous requests is incredibly time consuming.

Even if you overcome these aggregation issues and allocate resources to constantly monitor and dissect your DNS logs, it's highly unlikely you'll identify and mitigate an intrusion because you're deriving insights in a vacuum. Your company's sample size is too small to identify Internet-wide trends and threats. The more traffic and intelligence you have access to, the easier it becomes to flag irregular DNS traffic; you must understand global trends and patterns to efficiently and consistently identify threats.

The best DNS-based security solutions can be deployed and configured in less than 30 minutes, are 100% cloud-based, and can instantly add protection without complexity or hardware, with no disruption for users. Your DNS security measure should allow you to almost instantly administer security policies and updates from anywhere to protect all locations. It should also help you quickly and uniformly enforce compliance and your acceptable use policy (AUP) by blocking access to objectionable or inappropriate domains and content categories. The best solutions enable you to enforce your security measures and AUP when laptops are used off of your corporate network and when a laptop's VPN is not active.

Why Three Popular Security Solutions Benefit from an Additional Layer of DNS-Based Security

Let's take a look at three security technologies that enterprises commonly employ, their strengths and weaknesses, and how a DNS-based layer of security complements them while shoring up a company's defense against malicious actors.

ENDPOINT ANTI-VIRUS SOLUTIONS

Endpoint anti-virus solutions detect, block, and remove malware from end-user devices such as laptops and desktops. A detection engine scans requested web pages and files, and compares the results against a frequently updated list of malware signatures.

Strength: Endpoint anti-virus solutions provide decent, quick protection against known threats.

Weaknesses: By the time a threat hits an endpoint anti-virus solution, the software is the last layer of defense. If the software has not had a signature update, that single compromised device can be enough to cause significant damage. Endpoint anti-virus also provides limited protection against unknown/zero-day threats and file-less malware. Additionally, signature databases become very large and can be out of date on many devices, especially laptops that may seldom be connected to the corporate network.

How a DNS-based security layer helps: If a known malicious domain delivers new malware or a new malware variant, a DNS security solution can proactively protect the enterprise as a result of the solution's real-time threat intelligence — no signature updates are necessary.

If a device is already infected with malware and brought into the enterprise's network, a DNS-based security solution can detect that compromised device before it can inflict damage. This is because the vast majority of malware will use DNS to reach its CnC server. When the device attempts this contact, it is identified. Additionally, since a DNS-layer security solution uses DNS as a control-point, evading that control-point across the security kill chain is unlikely.

ENTERPRISE FIREWALL SOLUTIONS

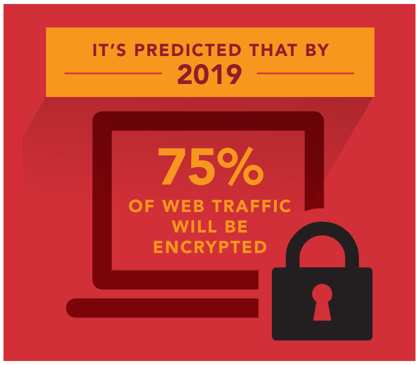
Also called next-generation firewalls (NGFWs), these deep-packet inspection firewalls move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and intelligence from outside the firewall. Increasingly, NGFWs are adding sandboxing, advanced threat protection, URL filtering, and data leakage prevention.

Strengths: NGFWs provide protection against inbound malicious attacks and are effective across all ports and protocols.

Weaknesses: They are complex and time consuming to manage and, as a result, can easily be configured incorrectly, leading to vulnerabilities. NGFWs are not strong solutions for off-network laptop protection, and the majority don't use DNS as a security control-point.

How a DNS-based security layer helps: A DNS-layer security solution blocks threats at an early stage, before the IP connection. It also frees up IT resources by managing whitelists, blacklists, and access control lists (ACLs) — a time-consuming process. By mitigating more attacks at the DNS level, organizations see fewer events that need to be addressed by other security systems on the network, making the IT security team's job more manageable.

It's predicted that by 2019, 75% of all web traffic will be encrypted.[7] As a result, encrypted traffic will become the go-to method of distributing malware and executing cyberattacks. Inspecting encrypted traffic is very processor-intensive because it requires organizations to decrypt and inspect the SSL traffic. By using



a DNS-based security solution to monitor suspicious and block malicious DNS traffic, you reduce the amount of HTTPS traffic that needs to be inspected, placing less load on your firewall.

SECURE WEB GATEWAY SOLUTIONS

A secure web gateway (SWG) protects Internet-connected devices from infection and enforces corporate and regulatory policy compliance. An SWG includesURL filtering, malicious-code detection and filtering, and application controls for popular web-based applications such as instant messaging and Skype.

Strengths: A secure web gateway works at the URL level, giving more granular control. It looks at both the resource being requested and the payload, integrates with identity systems, and allows very flexible policies to be created.

Weaknesses: SWGs are complex to manage. Their anti-virus engines have the same limitations as endpoint anti-virus. A secure web gateway is also expensive to deploy at all sites if you need local breakouts, and they are not an ideal solution for off-network device protection. Unfortunately, SWGs are not effective against malware that does not use HTTP/HTTPS on ports 80/443. Additionally, SWGs offer limited protection against DNS-specific threats, such as malware CnC traffic, and their static blacklists are easy to evade using Domain Generation Algorithms (DGAs) and fast fluxing.

How a DNS-based security layer helps: Coupled with a secure web gateway, a layer of security at the DNS control-point plugs a security gap. Working with a cloud-based SWG (as opposed to an on-premise NGFW), a DNS security solution stops threats early, before the IP connection stage.

Another benefit of a DNS security solution: It's cloud-based. This means there is no need for on-premise controls that must be monitored by IT at all times. Plus, whitelists, blacklists, and ACLs are managed automatically. And by mitigating more attacks at the DNS level, there are fewer security events that need to be dealt with by other security systems on the network.

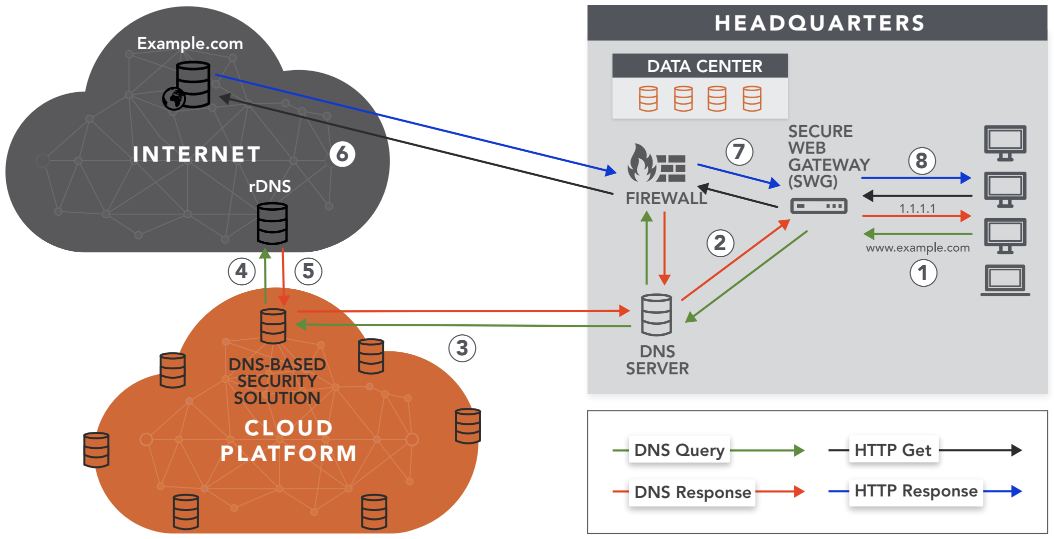
A Common Configuration: DNS-Based Security Layer + Secure Web Gateway + Enterprise Firewall

Now let's examine how an organization could accomplish a layered enterprise security model that adheres to the concepts of zero trust. A common configuration that large enterprises deploy is a DNS-based security solution with a secure web gateway and an enterprise firewall. Here's how the flow works when a user makes a request to access an external resource:

1. The user makes a request for example.com. The request hits the secure web gateway.
2. The SWG checks the requested URL against the filtering policy assigned to the user of the device. If the URL is not allowed, the request is dropped and the user receives a block page. If it is allowed, the SWG sends the DNS request to the DNS resolver.
3. The DNS resolver sends the DNS request to the DNS-based security solution, which checks the domain against the policy configured for the HQ. If the request is for an internal resource, the DNS resolver responds with the IP address of the internal resource.
4. If the domain is allowed under the DNS-based security solution's policy, the request is sent to the recursive DNS servers.
5. The rDNS servers respond with the IP address of the server where example.com is hosted, and the IP address is sent back to the device.
6. The device browser then makes the request to the IP address of the resource.
7. The response payload is received by the SWG and the content is inspected by inline anti-virus.
8. The requested web page is sent back to the device.

Below is an example of how an enterprise's setup could look.

DNS-BASED SECURITY SOLUTION EMPLOYED



It's worth highlighting that the overall architecture is the same as it was before a layer of security was added at the DNS management point. The only change is that the DNS resolver is now configured to send DNS requests for external resources to the DNS security solution, which is a quick and simple change for the IT organization to make.

Conclusion

Most IT professionals will agree that the time for a zero trust model for security is here, and the only way to achieve it is through a layered enterprise security approach. As DNS is an attractive and easy-to-exploit target for malicious attacks, it's critical to employ a DNS-based layer of security.

Best-in-class DNS security solutions can be deployed in minutes and deliver continuous, proactive protection against ever-evolving threats. They complement your existing IT security solutions and provide a host of benefits that not only better protect your enterprise against cybercriminals, but also free up IT resources to focus on other business-critical priorities.

To learn more about using DNS as a vital security control-point, as well as integrating a DNS-based solution with layered enterprise and zero trust security strategies, visit www.akamai.com/etp.

SOURCES

1) Jerry Shenk, *Layered Security: Why It Works* (SANS Institute, 2013), 2, 12.

2) Martha Bennett, *Zero Trust Security: A CIO's Guide To Defending Their Business From Cyberattacks* (Forrester Research, 2017),

3) Bennett, *Zero Trust Security*, 4.

4) "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016," Gartner.com, February 7, 2016, accessed April 10, 2018.

5) Ponemon Institute LLC, *2017 Study on Mobile & IoT Application Security Whitepaper* (Arxan Technologies, 2017), 12.

6) Chase Cunningham, *Develop Your Zero Trust Workforce Security Strategy* (Forrester Research, 2017), 5.

7) "NSS Labs Predicts 75% of Web Traffic Will Be Encrypted by 2019," NSS Labs, November 9, 2016, accessed March 22, 2018.

As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media & entertainment providers, and government organizations trust Akamai please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 06/18.