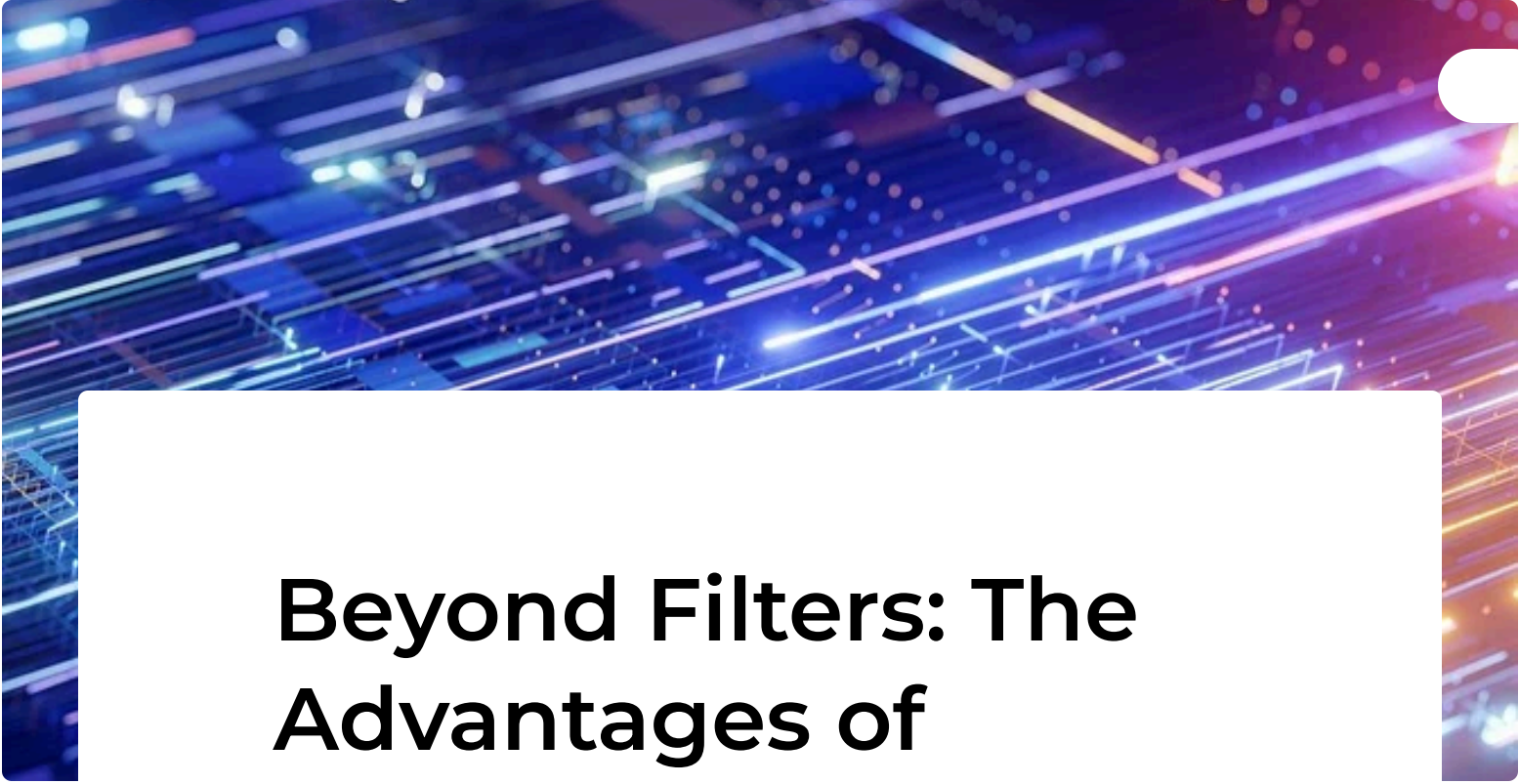




Beyond Filters: The Advantages of Protective DNS

Published by **Dan White** on Dec 02, 2024

- Protective DNS (PDNS) uses the Domain Name System (DNS) to provide an additional layer of protection against cyber threats such as malware, phishing attacks, and other malicious activities.
- Because DNS is foundational to the internet, it's one of the best places to begin when developing cybersecurity safeguards and overall business resiliency. DNS maps domain names to IP addresses; PDNS adds a security layer, protecting the user, device, network, and organization from malicious actors and nefarious activity.

- How does PDNS work and how does it fit into an existing cybersecurity stack? Here's an overview of the tech and why the HYAS solution is a value-add for security operations.

Remember phonebooks? You either vividly do, or you just have a dim recollection of these massive makeshift doorstops, abandoned in dusty vestibules. Maybe you've never even seen one.

Regardless, in the digital world, the DNS protocol is fundamentally the internet's phonebook, translating human-readable domain names (like "example.com") into the numerical IP addresses that computers use to communicate with each other. Leveraging this protocol is the ultimate solution for early detection and intervention. Quite simply, it's one of the first — and best — lines of defense for organizations in every industry and of any size.

Since DNS is a foundational component of the internet in and of itself. Protective DNS (PDNS) can act as a gatekeeper — it guards against dangerous threats, malware, ransomware, phishing and the like, and it alerts security teams in real time. Furthermore, PDNS gives those teams better visibility into their networks and systems and, ultimately, empowers them to take a proactive stance against the criminals who would try and break in, steal data, or otherwise cause damage.

Think of it as an enhancement to your cybersecurity posture that can add value right out of the gate. Let's take a look at how Protective DNS works, what it can do for security operations, and why the HYAS PDNS solution offers the best ROI on the market.

How Does PDNS Work? It's All About Proactive

Protection

Virtually every internet communication starts with at least one DNS query. That's why PDNS is a pivotal component of cybersecurity infrastructure — or it should be. But PDNS isn't just a "filter." Filters are generally apps or controls that blocks the bad stuff — and sometimes the good and innocuous. (Gmail's spam folder is a filter, for instance.) Instead, PDNS is a comprehensive solution that functions like a transparent layer of protection, seamlessly integrating into the overall security stack while offering real-time visibility and defense against cyber threats.

PDNS solutions screen DNS queries to detect and block the communication used by criminals and their malicious activity. When a user, device, or process attempts to access a remote domain (for instance, by clicking on a link in an email), the user's device generates a DNS query to resolve the domain name to an IP address. Usually, this query is sent straight to the organization's standard DNS servers. But this process is a bit different when PDNS is involved.

When PDNS is in play, every DNS query is routed through a service like HYAS instead of sending the query to standard servers. (Alternatively, depending on the deployment architecture and needs of the organization, some other process like an EDR may directly invoke the PDNS service, or the PDNS system may otherwise receive a fork or copy of the DNS communication). Then the PDNS service compares the DNS query against a comprehensive, up-to-the-minute database of domain reputations — flagging domains that are under the control of criminals, or are otherwise known to be utilized for malicious activities and overall "command and control", and stopping the communication flow before it even gets started.

The PDNS Advantage

Because PDNS flags malicious and suspicious traffic immediately, it provides a barrier, which among other benefits prevents users from inadvertently visiting “spoofed” websites and falling for fraudulent emails. PDNS can also help prevent users from falling prey to social engineering — using psychological manipulation to trick people into making security mistakes or giving away sensitive information, often by tricking them into falling for a form of a **phishing attack**.

With PDNS as a sentry, security teams can “passively listen to what’s going on in the environment — who a client is potentially talking to and what infrastructure they’re talking to as well. We’re actively blocking and stopping some of that proverbial bleeding right away,” explained HYAS’ Adam Lopez in a recent webinar.

Here are four advantages that can be game changers for your security operations.

1. Protection Away from the Office

Whether users are on or off your organization’s network, early and widespread detection protects remote-first and hybrid organizations. PDNS software continuously monitors networks at the DNS layer, both when employees are in the office and when they’re anywhere else in the world.

2. Less Is More: Cost-Effectiveness

As the overall cost of security programs skyrockets, budgets are tightening. All security teams are being asked to do more with less. PDNS is a very cost-effective security layer you can add to augment your current network stack, and deploy quickly, often in a matter of minutes.

3. Ensure Compliance

PDNS security has an additional upside. It can help ensure your organization adheres to specific compliance standards, whether or not you are beholden to various requirements from a federal [or industry] perspective or based on your vertical.

4. Increased Visibility, Threat Intelligence Sharing, and True Business Resiliency

Because PDNS gives organizations significantly improved visibility into their networks, security teams can react to potential threats before they become attacks. This ability to be proactive is one of the cornerstones of **protective DNS**.

This increased visibility includes logging DNS queries, which is key to identifying trends and unusual communication access patterns. Having the ability to detect, analyze, prevent, and mitigate threats that are active on a network is crucial to limiting organizational damage. PDNS is a way to make sure you have the elements in place to properly recover from security incidents, and in this way provides true business resiliency.

What's more, PDNS software can analyze those DNS query logs across multiple networks, which means it can identify emerging threats more quickly and accurately, further enhancing visibility into potential threats.

Why HYAS Protect?

Looking for a **protective DNS solution**? **HYAS Protect** offers unique PDNS capabilities and an innovative approach to cybersecurity. Here are some of its critical features:

Unique Threat Intelligence

HYAS Protect is powered by proprietary threat intelligence that's more robust than conventional **DNS protection services**. That means HYAS can leverage data on attackers' infrastructures and methodologies to identify and neutralize threats others might miss. HYAS Protect is on the forefront of providing real-time analysis based on unique threat actor infrastructure information.

Real-Time Analysis

The cybersecurity space moves at warp speed — and so does HYAS Protect. Analyzing DNS queries in real time means instantaneous threat identification and mitigation. This immediate response is crucial for preventing costly breaches and disruptions. Solutions that detonate malware or rely on intelligence feeds to decide what's malicious are always one-step behind; HYAS, in contrast, is always one step ahead.

Unrivalled Preemptive Visibility

HYAS Protect offers unmatched visibility into a network's DNS traffic beyond monitoring. By understanding normal traffic patterns, HYAS Protect can detect anomalies right away. This visibility extends beyond an organization's immediate network, incorporating global threat intelligence to predict and prevent attacks everywhere — before they even reach your "gates."

An Easy Solution

HYAS was designed to be easy to deploy, easy to manage and easy to integrate. It's also lightning-fast, both to implement *and* in its unrivalled real-time analysis speed.

HYAS Protect Architecture

Designed with flexibility and efficiency at its core, HYAS Protect's architecture consists of a decision engine that runs advanced algorithms against its proprietary threat intelligence database and the overall HYAS Adversary Infrastructure Platform.

IT environments can be as diverse as security pros themselves. HYAS Protect can seamlessly integrate with your existing platform and security stack for streamlined security ops. The HYAS solution also offers both agent-based and agentless options.

The agent-based approach allows for detailed, device-level protection and visibility, which enables users to secure endpoints directly. The agentless option provides broader, network-wide defense — requiring no installation software on individual devices. This dual approach empowers organizations to tailor their security posture to match their specific requirements, and the two approaches can even be combined.

Revolutionizing PDNS for Robust Threat Defense

HYAS Protect can safeguard your network from the cyber threats of today and prepare you to withstand whatever challenges the future holds. It's a powerful blend of real-time analysis, exclusive threat intelligence and network-wide visibility.

That's next-level cybersecurity. That's HYAS Protect: a versatile and powerful PDNS solution.

*Are you ready to protect your growing business from cyber threats? **Get in touch with HYAS today.***