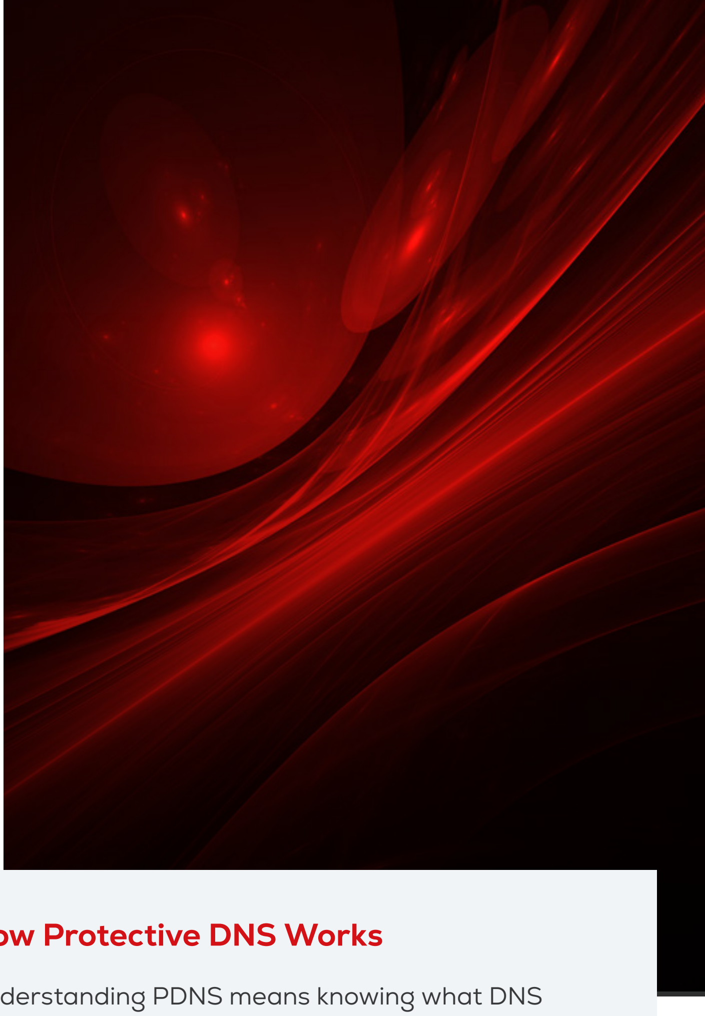
HYAS

The Role of

Protective DNS to Identify & Defend Against Cyber Threats



What Is **Protective DNS?**

The Domain Name System (DNS) is a critical but only marginally understood piece of the internet's infrastructure. Much like electricity, everyone knows that it works, but not necessarily how it works. Even though DNS is one of the most essential building blocks of the internet, it is often the most overlooked and exploited.

DNS is one of the most powerful and flexible protocols on the internet, which couldn't exist without it. If DNS is the phonebook of the internet, Protective DNS (PDNS) is what enables businesses to block the bad callers.

DNS routes users blindly and indiscriminately among 350+ million domains around the world, without "caring" whether it is sending users toward phishing, malware or a Trojan virus. What this means is that bad actors can easily use – and have been using – DNS to conduct cyberattacks. After all, no one is checking, right?

Protective DNS asks whether machines inside a network should actually talk to the domains they're trying to talk to. PDNS doesn't stop computers from using IP addresses to get where users (think) they want to go. But it will warn users if specific routes or IP addresses present security risks.

PDNS is like an inside-out firewall. A firewall prevents bad traffic from coming into the network. But networks inside enterprises can still talk to external domains they shouldn't. And this is exactly where threat actors hit hard.

How Protective DNS Works

Understanding PDNS means knowing what DNS consists of. There are three primary layers involved in DNS:

1. The **recursive layer** asks the DNS resolver where to go (domain or IP address, depending on whether a human or computer is asking).
2. The **authoritative layer** provides the answer to get the requester to these locations.
3. The **root servers** control top-level domains and hand off data.

The recursive layer asks if the requested IP address is okay to visit. If so, the authoritative layer provides the correct answer. If not, users are redirected to a page explaining the security risk and rationale, and can choose whether to proceed.

Threat Adversary **Infrastructure**

Just like legitimate businesses set up websites to sell their products, threat actors have to set up infrastructure to launch their attacks. That might be a phishing website that looks exactly like a bank's website with one extra letter in the domain, or the infrastructure to house malware.

Once a threat actor lands a digital spy inside an organization's network, this external infrastructure becomes the command-and-control (C2) center that the spy "beacons out to" for instructions about what to do.

Threat actors use DNS to communicate with C2. Effective Protective DNS paralyzes malware by identifying and severing this line of communication.

Why Organizations of Every Size **Need PDNS**

Many products claim to include DNS security, but this is often just a list of bad domains (aka allow-and-deny lists) that quickly fall out of date.

The persistent attacks against major corporations and the U.S. federal government – almost all of which rely on DNS – show that basic DNS security isn't good enough. If bad actors want to get into an organization, they will get in. Without Protective DNS, no security stack, no matter how strong it seems, can withstand modern cyberattacks.

When threat actors get into the network, Protective DNS identifies nefarious attempts to use DNS to communicate with command-and-control infrastructure and lets organizations head it off at the pass.

When You Do Not Have **Protective DNS**

A security stack without PDNS is like a tower without foundations: It's only a matter of time before it crumbles. Endpoint (EDR), managed (MDR) and extended detection and response (XDR) solutions are necessary but not sufficient.

Just like a home with external cameras and guard dogs, organizations with EDR, MDR, and XDR seem protected – and they are, but only from the outside. But if bad actors find an exploit in an organization's defenses (and we posit that they always will), the organization is immediately vulnerable because they don't have the same level of protection deployed internally.

Only Protective DNS asks whether an organization's machines should be talking to the domains they're trying to reach. PDNS eliminates threats before the rest of the security stack kicks in. As threat actors continue to successfully exfiltrate data and deploy ransomware, there is a clear need for this extra layer of protection inside networks.

Without PDNS, the number and severity of attacks will continue to grow. With a strong Protective DNS solution in place, DNS is no longer an easy gateway for attackers to infiltrate an organization.

What (the Right) **Protective DNS Solution Provides**

Protective DNS stops threat actors that have infiltrated organizations from communicating with external command-and-control infrastructure to execute a variety of exploits, from data exfiltration, encryption, lateral motion, privilege escalation, the list goes on.

With such a solution, gone are the days when threat actors are able to hide inside target networks for hundreds of days at a time – let alone up to five years. The internet changes every second in millions of ways. That's just the way it functions, and organizations need a way to keep track of the bad actors to protect themselves.

The true goal of cybersecurity is to drive the time between detection, remediation, and resolution as close to zero as possible. Because attackers are always creating new malware and new ways to attack organizations, the time between infection and detection is increasing. But businesses can no longer afford to let this be the case.

> **“The true goal of cybersecurity is to drive the time between detection, remediation, and resolution as close to zero as possible.**

Without a Protective DNS solution:

- ✘ If bad actors get inside an organization (and they will), they can do whatever they want
- ✘ Environments aren't secured against threat actors beaconing out of systems to C2 infrastructure
- ✘ There's no early warning signal of anomalous communication to malicious domains
- ✘ Threat actors can deploy damaging ransomware and exfiltrate data
- ✘ Businesses may take huge financial, operational, and reputational hits

With a Protective DNS solution:

- ✔ Helps target organizations understand what's going on in order to stop malware early in the kill chain
- ✔ Stops ransomware attempts by disabling efforts to steal and exfiltrate data from the target organization
- ✔ Prevents threat actors who infiltrate organizations from encrypting data or deploying ransomware
- ✔ Helps avoid difficult conversations with the board, negative financial fallout and reputational damage

HYAS Protective DNS **Vs. the Rest**

Traditional DNS protection typically adds newly published malware based on third-party data feeds. These lists are increasingly less effective in getting ahead of threat actors because by their very nature, they are reactionary. In order for malware to appear on a deny list, there already needs to have been an attack involving that malware.

This means organizations have to rely on someone being "popped" in order to get information about any given piece of malware, which means increased rate of threats. And it means threat actors spend more time inside organizations than they should be able to.

HYAS was founded with the mission to learn all we could about adversary infrastructure and then - how to use that knowledge to identify, predict, and ultimately dismantle the attacks associated with that infrastructure.

The HYAS Protective DNS solution, HYAS Protect, is powered by a vast graph database that maps what was nefarious yesterday to what is nefarious today to what is being created for nefarious purposes tomorrow. This happens before attacks are launched, enabling organizations to mitigate the damage.

HYAS Protect

- Looks at domains throughout their whole lifecycle: from birth to abandonment to rebirth
- Has real-time insight into meaningful, myriad movements and changes across the internet at any second that legacy solutions lack
- Has powerful underlying data that backs up the quality of its solution
- Characterizes and separates good and bad communication more accurately

HYAS Protect offers efficacy never before seen from a Protective DNS solution. A thorough evaluation conducted by the esteemed German third-party testing house, AV-TEST, found that HYAS Protect performed significantly better than any other Protective DNS offering on the market. (Source: AV-TEST)

Don't Be Another Statistic

$12 Trillion

The amount cybercrime will cost the world by 2025.
(Source: Cyber Crime Magazine)

99 Days

The median number of days attackers reside within a victim's network before detection.
(Source: Microsoft)

33%

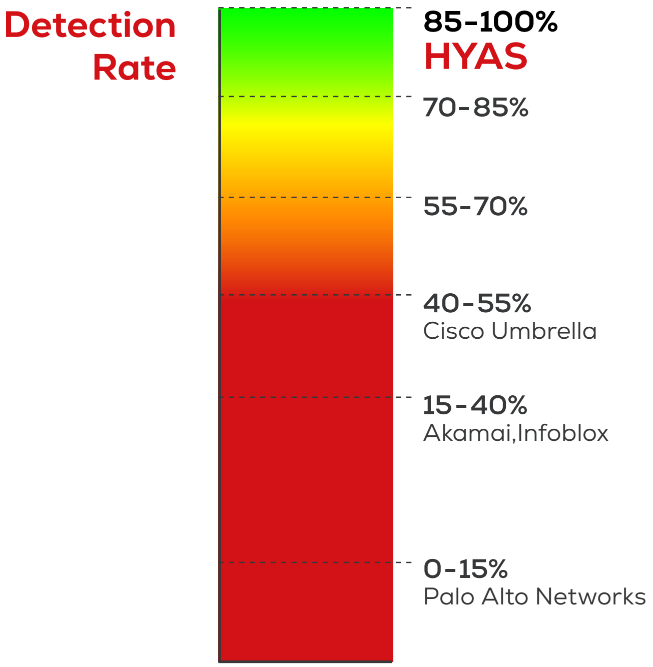
Percentage of cyber attacks that can be mitigated or stopped with DNS protection.
(Source: Global Cyber Alliance)

43%

Percentage of organizations that do not use a security solution built into a DNS server.
(Source: Help Net Security)

Efficacy Is **Everything**

When it comes to your network coverage, wouldn't you want to have more protection than less?



Protective DNS is only helpful if it fits into an organization's security architecture and deployment model – which can be very different depending on the organization.

All of the HYAS solutions are built to complement and integrate with any security tools an organization already has. With HYAS Protect, security teams get a next-gen PDNS solution that solves security needs now and for the future.

HYAS Protect is easy to manage and deploy. It's built to integrate so that:

- Organizations choose whether HYAS acts as their enforcement agent
- It fits into existing stacks, which include EDR or XDR
- Whatever SIEM, SOAR or firewall being run, HYAS works with it
- Organizations don't need to stop using any of the tools currently used

Monitoring Domains from Birth to Abandonment to Rebirth

Protective DNS is all about identifying and monitoring domains from when they are initially created to when they are no longer used. It's about establishing how they are correlated across the internet, accounting for changing records, host posture and remote machines.

If a domain never existed, it must be created: When it's bought and registered, it is in its infancy. But it can also be used and not renewed, and so it goes back to a "parking lot" of domains for someone else to use. Even domains once used for legitimate purposes can eventually be used by bad actors after being parked.

Legacy DNS filters and older solutions are not able to identify what HYAS is clocking in real time. There are over 15,000+ top-level domains with unlimited namespace to create any domain someone could want, which means an exponential amount of potentially malicious activity.

By tracking domains from birth to abandonment to rebirth and mapping and linking bad domains, IP and email addresses, and phone numbers, HYAS solutions accurately map what will turn malicious.

The HYAS **Portfolio**

HYAS Protect
identifies and preempts external and internal network attacks, giving clients maximum threat visibility to avoid ransomware, phishing and supply chain compromise – all in an integrated manner.

HYAS Insight
provides threat intelligence and investigation capabilities derived from unique datasets, providing advanced attribution tools, integration, data enrichment backed and incident response assistance for maximum ROI and efficacy.

HYAS Confront
offers visibility into production traffic, cleanup success rates, security controls, and API integration, highlighting anomalous communications for clients to respond appropriately.

HYAS Intelligence Services
helps augment security teams to better understand and defend against the cyber threats they face.

Protect your organization against cyber threats from the inside out. See how identifying and blocking adversary infrastructure levels the playing field for your organization.

CONTACT US
hyas.com/contact

INVESTIGATE ATTACK
INFRASTRUCTURE FURTHER
AND IDENTIFY FRAUD FASTER

PROTECTING BUSINESSES AND SOLVING INTELLIGENCE PROBLEMS
THROUGH DETECTION OF ADVERSARY INFRASTRUCTURE AND ANOMALOUS COMMUNICATION PATTERNS

HYAS is a world-leading authority on cyber adversary infrastructure and communication to that infrastructure. HYAS is dedicated to protecting organizations and solving intelligence problems through detection of adversary infrastructure and anomalous communication patterns.

We help businesses see more, do more, and understand more in real time about the nature of the threats they face. HYAS turns meta-data into actionable threat intelligence, actual adversary visibility, and protective DNS that renders malware inoperable.