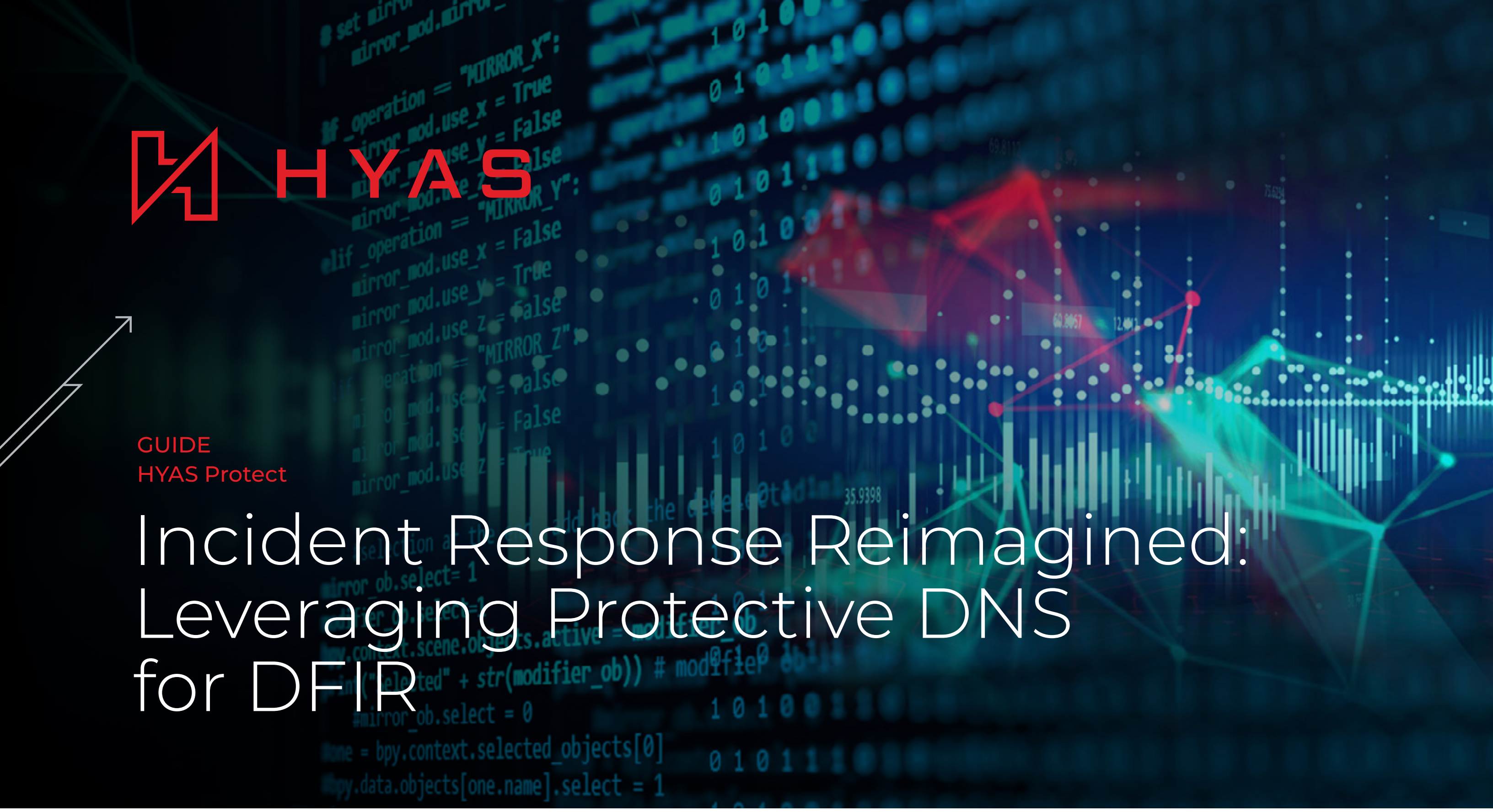

GUIDE
HYAS Protect

Incident Response Reimagined: Leveraging Protective DNS for DFIR

The Power of Protective DNS

DNS, or domain name system, is often referred to as the "phonebook" of the internet. But while a phone book lists names with phone numbers, DNS translates domain names (like www.hyas.com) into IP addresses (like 123.0.4.1) — which are the numerical labels computers use to identify and communicate with each other on a network. While domain names are easy for people to remember, networked devices rely on IP addresses to route data.

Here's another way to think of DNS: The internet is a massive library, each web page is a book, and DNS is a librarian who knows the exact location (IP address) of what a person seeks. When entering a URL into a web browser, we're asking DNS to point to the right place, just as a librarian assists with finding a book in the library.

In the cybersecurity space, we can leverage DNS to create a first line of defense against malicious attacks. PDNS is like a vigilant, security-minded librarian who not only helps us find books but also ensures we steer clear of sections that are unsafe or contain harmful content — like avoiding trouble in the library, akin to how Slimer in "Ghostbusters" might cause chaos.

A librarian might check books for inappropriate content before they put them in circulation. PDNS does something similar: It scrutinizes domain names against a continuously updated list of harmful sites. And if someone attempts to access a dangerous site, the vigilant PDNS prevents them from reaching it, protecting the user and the entire organization.

PDNS is a pivotal component of cybersecurity infrastructure — not just a kind of filter blocking harmful content. It is a comprehensive solution that seamlessly integrates into an organization's network to offer real-time defense against cyber threats.

PDNS, Meet DFIR

Protective DNS is a cornerstone of cybersecurity that enables Digital Forensics and Incident Response (DFIR). PDNS provides vital capabilities for detecting, analyzing and mitigating cyber threats.

Digital forensics can be defined as the collection, preservation, analysis and presentation of digital evidence related to cyber incidents. Incident response focuses on promptly addressing security breaches to mitigate damage and recover, maintaining continuity of operations.

PDNS provides vital capabilities for detecting, analyzing, and mitigating cyber threats by monitoring DNS queries and responses for signs of malicious activity. And as attacks become increasingly sophisticated, maintaining a robust DFIR process has become essential.

Here's a brief overview of how PDNS works in digital forensics and incident response.

Detection and Analysis

- PDNS systems log DNS queries and responses
- The resulting data from these logs can reveal:
  - Compromise vectors
  - Communication with command and control (C2) servers
  - Attempts at data exfiltration
- Analyzing PDNS data can expose anomalies that signify malicious activity, such as:
  - Repeated queries to unknown domains
  - Excessive DNS requests (indicative of network compromise or malware)

> “We thoroughly tested HYAS Protect and stand by the results. As attacks evolve, increases in the efficacy of protection are clearly critical, and HYAS has demonstrated a very high level of efficacy with their new solution.”
>
> – **Andreas Marx,** CEO of AV-TEST

AV-TEST

AV-TEST is an independent research institute based in Magdeburg, Germany, that specializes in conducting comprehensive and rigorous tests of security software and products.

In a test of HYAS Protect commissioned by HYAS, AV-TEST found that the HYAS solution blocked:

- Over 87% of portable executables (PEs) malware
- Over 84% of non-PE issues (e.g., links pointing to other forms of malicious files)
- Over 80% of phishing URLs
- Incredibly low false-positive rates averaging 2%

Compared to other Protective DNS solutions tested by AV-TEST, HYAS Protect achieved the highest efficacy ratings of all protective DNS solutions providers tested to date. The test results indicate it affords substantially greater protection.

Containment and Eradication

Once a threat is identified, PDNS can help contain the breach by:

- Blocking traffic to malicious domains
- Disrupting attackers' control over compromised systems
- Stopping further data exfiltration attempts
- Limiting the spread of malware
- Preventing additional systems from being compromised

Recovery and Post-incident Analysis

PDNS data is invaluable for understanding the sequence of events before and during a security incident. The data allows analysts to:

- Reconstruct the attack timeline with precision
- Identify affected systems
- Understand the tactics, techniques and procedures (TTPs) used by attackers

These Insights are Critical for:

- Restoring systems and data
- Reinforcing defenses
- Preventing future breaches

Importance of PDNS in DFIR at Every Step

PDNS (as part of DFIR) is critical at every step of the security incident identification and response process.

Preparation: PDNS can proactively identify potential vulnerabilities and misconfigurations with a potential for exploitation in an attack. Think outdated DNS records and unsecured DNS configurations, which can make an organization's infrastructure susceptible to attacks like spoofing and cache poisoning.

Identification: PDNS highlights suspicious DNS activity in real time, right as it happens.

Containment: PDNS enables immediate blocking of DNS requests to known malicious sites. HYAS Protect's proprietary threat intelligence feeds can keep one's network from "talking" to these domains before bad actors can launch malware or another attack.

Eradication: Insights from PDNS data pinpoint the origins and methods of attacks and add them to HYAS' threat intelligence feed, which prevents the same hackers and/or attack techniques from striking the same network again.

Recovery: It's critical to ensure that all backdoors and malware are truly eradicated from the network, which can be achieved through PDNS analysis of the attack vector.

Lessons Learned: PDNS logs are the basis for post-incident analysis, which helps security teams strengthen their security postures and prevent similar attacks.

Go On Offense With HYAS Protect

HYAS Protect is designed to proactively defend organizations against a multitude of cyber threats by leveraging the power of Protective DNS. At its core, HYAS Protect aims to intercept and neutralize threats before they can reach an organization's network, thus significantly reducing the risk of malware infections, phishing attacks, and other cyber threats.

Key Features Include:

1. **Real-time threat intelligence**
HYAS Protect integrates real-time intelligence to identify threats and block access to malicious domains, URLs and IP addresses. The HYAS advantage is a blend of proprietary data, open-source databases and industry partnerships. It all adds up to comprehensive, leading-edge protection against threats that are known — and those that are emerging.

2. **Customizable policies and whitelisting**
Understanding that each organization has unique security needs, HYAS Protect allows for the customization of filtering policies. Administrators can tailor these policies to block specific categories of websites, such as those known for phishing or hosting malware, while whitelisting trusted domains to ensure uninterrupted access to necessary resources.

3. **Enhanced visibility and reporting**
HYAS Protect offers detailed visibility into DNS traffic, enabling organizations to monitor and analyze queries in real time. This feature aids in identifying suspicious patterns and potential security breaches, providing valuable insights for threat hunting and incident response efforts. Comprehensive reporting tools also allow for the easy generation of reports, facilitating compliance and audit processes.

4. **Scalable and secure architecture**
Designed to meet the demands of both small businesses and large enterprises, HYAS Protect's architecture is highly scalable, ensuring reliable performance under varying loads. It employs robust security measures to safeguard DNS queries and responses, including DNS over HTTPS (DoH) and DNS over TLS (DoT), encrypting DNS traffic to protect against eavesdropping and tampering.

5. **Deploy anywhere, anytime**
Time is not a luxury that businesses can afford. HYAS Protect is a cloud-native software-as-a-service that scales infinitely and deploys in minutes.

6. **Revolutionize existing security investments**
HYAS Protect's API-driven flexibility amplifies the intelligence of an existing security stack through a new layer of protective DNS. Easy-to-use APIs allow seamless leveraging of SIEM, SOAR, firewalls, or other security components.

HYAS Protect and RSM Defense: Client Success Stories

RSM (Risk Management Solutions) provides consulting and management services, including cybersecurity services, to hundreds of clients around the world.

RSM's dedicated Security Operations Center (SOC), known as RSM Defense, offers around-the-clock monitoring and threat mitigation services to customers who use RSM's cybersecurity services. This specialized division scans client networks for unusual activity and promptly responds to alerts by investigating and neutralizing potential threats.

As a company that promises leading-edge technology solutions, RSM needed cybersecurity applications that could integrate with its existing security stack — and scale as needed. HYAS Protect was the clear choice.

The French Connection

With HYAS Protect, RSM successfully intercepted suspicious DNS activity for a large retail client. The team at RSM uncovered a cybercriminal exploiting the legitimate remote access software Splashtop for unauthorized purposes, specifically to sustain unauthorized access within a network that didn't normally utilize Splashtop.

RSM analysts observed unusual DNS queries emanating from the system but realized that even though the access to the host was not compromised, it was still relevant to the identified threat, contradicting initial beliefs. This led to a broader investigation of the incident. The implementation of the HYAS Protect tool allowed the RSM security personnel to discern legitimate access by trusted agents (TA).

Moreover, the RSM team discovered that the malicious software used against their client was connecting to infrastructure outside of the U.S., notably to servers in France. Given the client's lack of international operations or connections, this was a clear indicator of suspicious activity.

By deploying HYAS Protect, RSM was able to halt the DNS transactions linked to the cybercriminal's infrastructure.

HYAS Protect is designed to permit the use of legitimate remote access tools such as Splashtop and TeamViewer in scenarios where their use is justified for business. But when cybercriminals manipulate such tools for malevolent purposes, HYAS knows what to expect, enabling security teams to differentiate between unconventional yet harmless activity and truly malicious actions.

Forensics and Phishing

RSM's digital forensics and incident response (DFIR) unit tackled a cybersecurity threat aimed at one of their clients in the professional services sector located in the Middle East.

A cyber attacker infiltrated the client's system via a phishing email. This malicious actor established the deceptive domain merely two days prior to launching the attack. The DFIR team swiftly revoked trusted agent (TA) access and implemented HYAS Protect to block further actions from the threat actor. While the team managed to contain the situation initially, cyber attackers often persist in their efforts to breach systems.

In an attempt to regain entry, the attacker resorted to the initial method of attack: another phishing email.

Thanks to HYAS Protect's capability to autonomously block communications based on a domain's newness and reputation for being associated with bad actors, subsequent phishing attempts were thwarted. This level of protection continued even though the client inadvertently engaged with the phishing link again, all because RSM had equipped their client with HYAS Protect. This system is adept at halting suspicious DNS activity even without predefined rules targeting such traffic, offering a safeguard against potential reinfection amidst ongoing remediation efforts.

When paired with HYAS Insight — HYAS' comprehensive threat intelligence service — businesses are well-equipped to defend against DNS-based cyber threats. The decision-making process within HYAS is informed by domain-specific intelligence, further enhancing threat detection and contextualization.

BY THE NUMBERS: CYBERSECURITY STATS

$10.5 trillion

The estimated global cost of cybercrime by 2025, which is growing by 15% annually.

— **Cybersecurity Ventures**

95%

of cybersecurity breaches are due to human error.

— **Cybint News**

44

records are stolen every second; more than 3.8 million since 2013.

— **Cybersecurity Ventures**

118 days

Average time it takes to detect a data breach.

— **ThoughtLab Group**

$4.45 million

Average cost of a data breach.

— **IBM Cost of a Data Breach Report 2023**

35%

of malware was delivered via email in 2023, making it the most common vector for malware.

— **Verizon 2023 Data Breach Investigation Report**

72%

The increase in data breaches since 2021, which held the previous all-time record.

— **Identity Theft Resource Center 2022 Data Breach Report**

4.1 million

The number of sites infected with malware at any given time.

— **SiteLock Website Security Report 2022**

Let's Optimize Your Security Solutions — Together

Is your organization fully equipped to defend itself? Learn more about how HYAS Protect can provide:

- Unmatched visibility
- Real-time domain truth
- Proactive defense
- Seamless deployment

Why Choose HYAS Protect?

Don't just ask us...

- **Germany-based independent software and cybersecurity valuator AV-TEST** validated our industry-leading PDNS
- **The National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA)** recognize HYAS as a leader in the space
- **Microsoft's M12 fund and S3 Ventures** invested in the company

HYAS Products

HYAS security solutions provide the visibility and observability needed to stay in control of your environment. HYAS solutions are easy to deploy, easy to manage, and integrate seamlessly into any security stack.

PROTECTIVE DNS

HYAS Protect

Protective DNS

Our protective DNS solution combines authoritative knowledge of attacker infrastructure and domain-based intelligence to proactively block malicious communication used by cybercriminals to conduct phishing, ransomware, and other forms of cyberattacks.

Explore HYAS Protect →

THREAT INTELLIGENCE & INVESTIGATION

HYAS Insight

Threat Intelligence & Investigation

HYAS Insights allows you to rapidly discover and investigate any IOC and related indicators. Identify and map out the complete cybercriminal campaign architecture and take a proactive stance against future attacks.

Explore HYAS Insight →

Recent Malware Infrastructure
Daily Detonation Volume by Malware Family
Distribution by Top Malware Tags
12161
Total
Distribution by Top C2 ASN Countries

Contact Us For a Demo
hyas.com/contact

HYAS

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.