HYAS

PROTECTIVE DNS:

THE CYBERSECURITY ESSENTIAL **YOU DIDN'T KNOW YOU NEEDED**

TABLE OF CONTENTS

THE EVOLVING WORLD OF CYBER THREATS

IN CYBERSECURITY, THE ONLY CONSTANT IS CHANGE.

The number of threats from powerful, well-funded and well-educated bad actors armed with an ever-more sophisticated array of tools and techniques increase exponentially, and businesses around the world are significantly under-prepared and under-protected against them.

The solution is actually very simple.

At HYAS, when everyone else is looking at what is coming into an environment, we are focused on what is going out. Cyber threat actors rely on special infrastructure to deploy their attacks. This attack infrastructure is hidden to people who do not know how (or why) to look for it. Rather than chasing specific attacks, HYAS technology identifies the infrastructure the attackers are attempting to use to deploy any attack.

We harness a powerful understanding of threat actor infrastructure and anomalous communication to help organizations proactively protect themselves against pervasive threats. The aim is to level the playing field – regardless of bad actors changing their techniques – and stop threats outright.

So, how do we go about doing that?

Shields Up!

CISA is funded by the federal government and works alongside the NSA and other intelligence organizations – both public and private – to build more secure, resilient infrastructure. CISA makes recommendations for small companies and large enterprises to secure critical infrastructure and defend themselves against cyber threats.

CISA released a joint memo with the National Security Agency following the SolarWinds and Colonial Pipeline attacks several years ago. Monitoring all outbound DNS traffic is paramount to understanding which traffic is nefarious, and thus what communications need to be shut down. As part of the Shields Up initiative, CISA recommends Protective DNS as a critical component of a modern, comprehensive cybersecurity solution.

DNS 101

In the wake of several major cyberattacks, there's been a lot of recent talk about protective Domain Name System (PDNS) services. In 2020, the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) released guidance on choosing protective DNS services.

> **Protective DNS is a policy-implementing, recursive DNS resolver service built as the successor to the capability currently being delivered by E3A DNS Sinkhole. Protective DNS is deployed upstream of agency networks. The service filters DNS queries - by comparison to a range of unclassified threat intelligence - to prevent resolution for known malicious domains and/or IP addresses. Protective DNS supports emerging DNS technologies including encrypted DNS protocol support (DoH/DoT) and IPv6 resolution. DNS log data is made available to users of Protective DNS to dramatically increase visibility. Additionally, users are able to heavily customize alerts, data extraction, and other system features.**
>
> -CYBER SECURITY & INFRASTRUCTURE AGENCY (CISA)

But what is the Domain Name System (DNS) and why does protecting it matter so much to business?

WHAT DNS IS

DNS is often called the "phonebook of the internet." But unlike phones without phone books, the internet as we know it can't function without DNS.

> **"DNS is often called the 'phonebook' of the internet."**

DNS is a fundamental internet protocol that was built for efficiency and scalability – but not necessarily security. The system is designed to fulfill lookups as quickly as possible, with recursive resolvers passing the request along to DNS servers higher up the chain of authority if the information is not stored in their cache.

Recursive resolvers will contact root servers, which will then pass the request to the TLD nameserver responsible for the queried domain's extension (.com, .net, .uk, etc.). Finally, the request will be routed to the authoritative nameserver for the requested domain, consulting the domain's A Record to return an IP address.

This is an elegant system with built-in redundancies to ensure that all requests are fulfilled quickly without overloading any one particular server. Because it works so seamlessly, for most users, it might as well function like the electricity coming out of their wall plug, it just works – which means it is often overlooked.

When it comes to understanding the content and intention of the lookups it performs, the system is fairly passive – after all, its primary job is to be accurate and speedy. This has led to the development of several types of attacks that take advantage of features of the protocol to initiate attacks.

If someone wants to create an e-commerce website, they need to be able to register a domain with a domain name registrar. DNS maps domain names to IP addresses (the numeric addresses that allow computers to talk to each other). When you register a domain the registrar will ask you for the IP address of the nameserver where the DNS record resides. Meanwhile, domains allow people to find other people, goods and services online. **DNS translates what humans read into what computers can read.**

There's just one problem: Just as legitimate business owners benefit from the openness of DNS, bad actors can also take advantage of its inherent anonymity. In fact, it's their primary communication tool.

WHY WE NEED PROTECTIVE DNS

When malware infects a system, it doesn't act independently. Before it does anything, it needs to talk to an external agent that lies outside of the infected system. It must "beacon out" for instructions.

Bad actors need to lay the groundwork before infiltrating systems with malware. Creation of domains to act as command and control (C2) infrastructure effectively directs the malware on how to carry out operations within the compromised systems. Even when criminals change their tactics, techniques and procedures (TTP), they're still using the same DNS and C2 infrastructure to instruct and deploy malware. This adversary infrastructure is what enables an attack to initiate within an organization. Lateral motion, data exfiltration and encryption – all begins with outbound communication to threat actors.

This is where Protective DNS comes in.

Protective DNS blocks access to malicious websites, detects and disrupts malicious communication, which can prevent data exfiltration, filter unwanted content, and provide early threat detection capabilities.

We must assume an organization is already breached – or will be imminently – so the job of Protective DNS is to identify and block communications from adversary infrastructure. It's not necessarily important to know what is being communicated in order to shut it down. We only need to know that this communication shouldn't be happening so we can take action.

ADVERSARY INFRASTRUCTURE AND A MEGA GRAPH DATABASE

The internet is awash with data. There's so much data that it's difficult to know how to analyze it, let alone how to apply it to protecting critical systems and infrastructure.

But it is possible to identify good and bad with a robust analytical framework – even with the sheer amount of data flowing through the world. This is the key to identifying, mapping, and attributing adversary infrastructure.

A UNIQUE EDGE

A massive graph database underpins HYAS technology, gathering information from authoritative sources across the internet, including exclusive, private, bespoke, and commercial datasets. This analysis runs automatically 24/7/365, and the interconnected nodes that result reveal a picture of the cyber threat ecosystem unlike any other.

This graph database facilitates a cybersecurity solution with both a very high efficacy rate and a very low false-positive rate.

This solution hasn't been easy to establish. Anyone can benefit from DNS anonymity to easily create multiple domains, and there are hundreds of millions of registered domains. Moreover, bad actors constantly create new C2 structures.

But by understanding what this adversary infrastructure entails, we can differentiate good from bad. We can build correlations and understand how new, nefarious domains fit into the database. Real-time, nonstop monitoring and analysis of this infrastructure – and threats emanating from it – facilitate the most up-to-date knowledge about what we should (and should not) communicate with across the internet.

HEAVY LIFTING TECH

When the best human-crafted technology meets the best machine learning technology, we can lift heavier, so to speak. The more data connected, the better the decision-making. And the better the data, the greater the power.

The HYAS database ingests billions of data points a day, working in tandem with various methodologies to create the nodes that fuel its foundational power.

As a static model, a legacy-based "allow and deny" list isn't fit for purpose in today's world of cyber threats. The internet is constantly changing, and protection against cyber threats has to evolve along with it for the best chance of protection.

Isolating and eliminating each case of malware – and understanding the infrastructure behind them – is inadequate. If we add one bad domain to a deny list so malware is unable to communicate with it, bad actors simply need to update their malware every 36 hours so it can talk to different C2 structures. Bad actors always stay ahead of their targets.

HYAS works to identify adversary infrastructure at inception. This means that – in tandem with interconnected data – even if threat actors change domains every 36 hours, new nefarious domains are still blocked before the malware is updated to communicate with new attacker infrastructure. Now, regardless of how a threat enters an organization or which threat vector it leverages, organizations can finally stay ahead of their attackers by relying on identifying the protocol, not the specific threat.

MISSION: **DIGITAL RESILIENCY**

Digital (or cyber) resiliency and business continuity plans are à la mode for organizations honing their cybersecurity strategies. **Enterprises need to understand how, if breached, they'll be able to effectively deal with any fallout.** They may need to alert board members and shareholders as well as address potential impact of the breach on clients, employees, as well as brand reputation.

Better yet, they want to stop attacks from happening in the first place.

KEEP THEM OUT? THEY'RE ALREADY INSIDE

Historically, cybersecurity strategy has been preventative for most organizations – especially for large-scale enterprises with established brands to protect. Keeping bad actors out of their systems and critical infrastructure has been and remains a number one priority for chief information security officers (CISOs) who understand the potential damage and catastrophic business and financial implications.

But in the wake of major breaches over the last few years – which have included critical American infrastructure and the U.S. federal government – most CISOs' concerns have shifted. **Now, the fear is not of bad actors trying to infiltrate: They're already inside.**

A truly modern business resiliency strategy responds to these worries with confidence.Of course, it is important to identify the cause of any breach, but when it comes to protective DNS as a proactive defense, it doesn't matter how bad actors infiltrated a system. Protective DNS is laser-focused on identifying and blocking any malicious, anomalous communications coming out of it.

DISRUPTING THE 'KILL CHAIN'

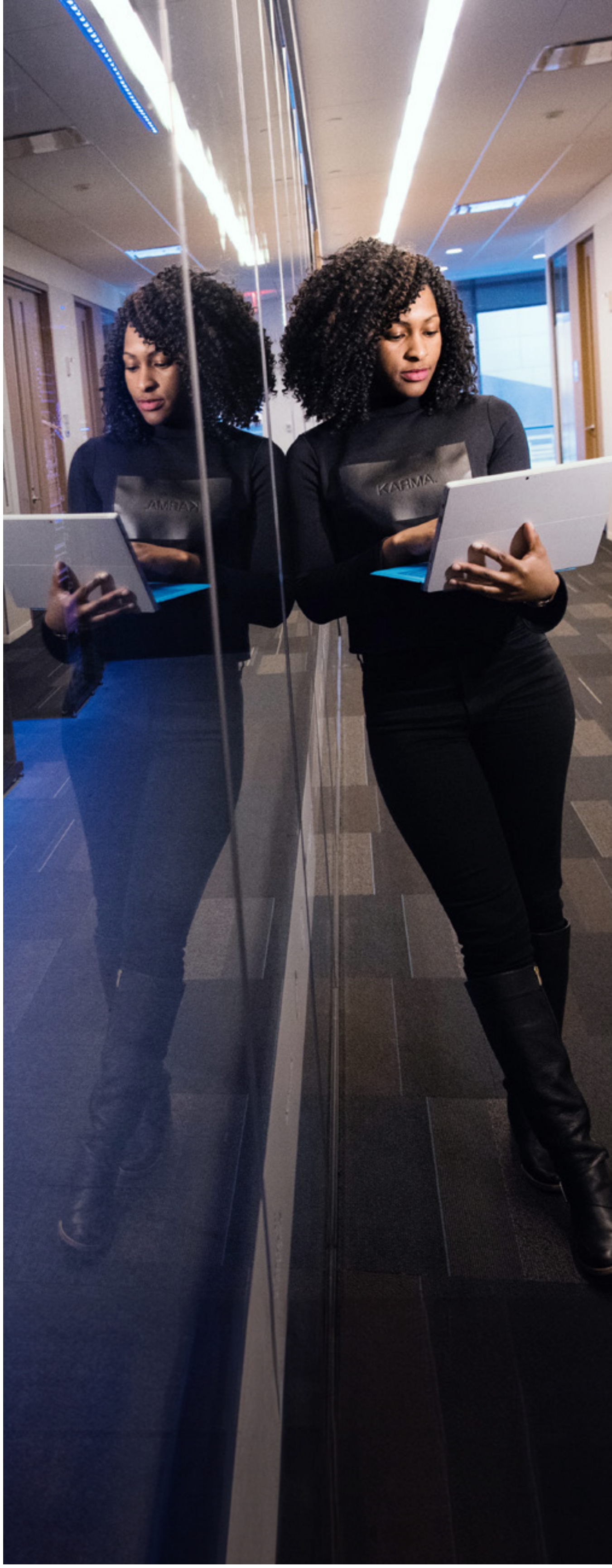
A break-in doesn't need to turn into ransomware or encryption events. It doesn't automatically lead to data getting stolen by bad actors. **Detecting anomalous communication results early enough in the cyber 'kill chain' means that we can stop these things from escalating.**

Protective DNS acts as an early warning system declaring an imminent threat. Even if a threat is already inside a network, Protective DNS provides an edge – the damage is not yet done, and a security team can be alerted to investigate the threat in a timely manner.

Early investigation means organizations can identify and manage threats long before those threats mutate into devastating breaches – breaches that necessitate notifying boards and customers and tend to generate negative publicity, loss of trust, and untold financial implications.

Beyond being an early signal of impending danger, Protective DNS also serves as a last line of defense. If malware penetrates insider risk detection and attempts communication with C2 infrastructure, PDNS allows organizations to shut down that communication – and the kill chain – before threats evolve into something malicious.

> **"Protective DNS is the thing that's going to allow you to stop malware early in the kill chain and shut it down before it gets started in the attack."**
>
> **DAVID RATNER**
> CEO, HYAS



SOLUTION INTEGRATION

The time has never been more ripe for bold, ambitious solutions in cybersecurity. Diverse approaches toward securing modern networks are gaining traction. Organizations are using new and different frameworks and technologies to tackle truly next-gen security challenges.

The success of this cybersecurity renaissance relies on ensuring that existing, legacy network and security layers continue to function as required while we adapt to new frameworks with Protective DNS protection as part of a holistic cybersecurity solution.

A standalone endpoint security system or firewall may protect against rudimentary threats. Security information and event management (SIEM) systems should be able to alert organizations to the biggest dangers their infrastructure faces. A solid security orchestration, automation and response (SOAR) system must deal with threats efficiently without human intervention.

The right Protective DNS solution amplifies the capabilities of these systems. They become much more powerful. SWGs, EDRs, FDRs, and firewalls are fortified. SIEM and SOAR systems are enriched. Efficacy skyrockets.

HIGH EFFICACY

Ideally, Protective DNS can be layered on top of existing security stacks.But depending on the provider, that is often not the case, and vendors mandate which solutions their technology will and will not accommodate.

In contrast, the HYAS Protective DNS solution, HYAS Protect, is specifically designed to integrate into and and all existing security stacks. This means minimal friction when deploying Protective DNS.

> “The deployment was easy. All you do is go into all of your DNS servers and point all external traffic at HYAS Protect as the primary resolver and move our previous public DNS service to be the secondary. We’ve never had an issue with HYAS so we have never used the secondary.”

CHRIS BATES
CHIEF INFORMATION SECURITY OFFICER, SENTINELONE

Every organization builds a defense that is as strong as it can be, given its human and financial resources. Usually, these defense systems are built incrementally over years. They typically include firewalls, secure web gateways (SWG), endpoint detection and response (EDR), and file detection and response (FDR). To rip them up and start over with the most high-tech and modern solution would be counterproductive. Moreover, it’s unnecessary.

If bad actors should penetrate a network’s walls, Protective DNS lies in wait to signal suspicious activity before a breach occurs, allowing IT and security teams to swiftly mitigate the threat. **Deployed correctly, Protective DNS is a direct, high-efficacy way to proactively identify and block threats across environments that works in concert with (and complement) existing security stacks.**

The ideal Protective DNS solution extends and increases the efficacy of even decades-old defenses. It enhances a business resilience strategy. Enterprises can defend themselves against bad actors regardless of how infiltration techniques change. Protective DNS is highly effective both in terms of thwarting unwanted communications as well as working in harmony with existing stacks.

HYAS Protect: Easy to Use, Easy to Manage, Easy to Deploy

Security teams deploying HYAS Protect Protective DNS are up and running almost immediately. The User Interface (UI) is intuitive and easy to navigate, making the solution straightforward and simple to use.

Once implemented, security teams are able to directly monitor all current traffic and make comparisons that may point to trends from the previous day. They can note already-blocked traffic – including less serious cases that were precautionarily flagged – and take action to block additional traffic if required. Alternatively, if certain traffic is required by other teams, de-escalation is a very straightforward process.

FAST-GROWTH BUSINESS REASSURANCE

Large corporate and government institutions aren't the only entities that can benefit from Protective DNS. Smaller businesses also need protection against the same threat tactics and techniques that can be used against them. Most small to mid-sized businesses do not have as much protection as they should. Inevitably it is a fraction larger organizations, but the risks and likelihood of cyber attacks against them are nearly the same.

Under Attack

Small and mid-sized businesses (SMBs) are a prime target for cyber attacks. Here's a look at the numbers:

- Nearly 50% of all cyber attacks are aimed at SMBs
- 82% of ransomware attacks target SMBs
- 83% of SMBs are not financially prepared to recover from a cyber attack.
- 61% of SMBs experienced an attack in 2022
- 43% SMBs do not have any cybersecurity plan in place

Businesses ready to scale are usually aware that threat levels naturally increase as they increase in size. But that shouldn't be an obstacle to growth. With Protective DNS in place, small organizations can utilize technology normally reserved for large enterprises.

> **"If you have a system like HYAS in place, you can detect and shut down threats before they run rampant throughout your organization."**
>
> **DAVID RATNER**
> CEO, HYAS

FROM GARAGE OPERATION TO ALL-ENCOMPASSING BRAND

Portland Leather Goods began its life in a garage in 2015 and has grown rapidly ever since. With the opening of its sister company, Patina, the company is now shifting focus to a greater range of high-end luxury goods beyond leather.

With such successful growth comes a greater focus on cybersecurity. Protective DNS steadily moves from a desirable feature to a necessity. A Protective DNS solution that integrates harmoniously with an existing security stack provides a proactive defense that would not have been there in the first place.

Scaling businesses require their cybersecurity partners to be knowledgeable and adaptive. In growth stages, businesses must also contend with careful, intentional resource allocation. So it's important to choose a Protective DNS solution that aligns with one's brand while offering the very best protection. And it's critical to find a vendor that understands its own systems inside-out as well as the specific requirements of growing companies.

THE VALUE OF VISIBILITY

Portland Leather Goods implemented the HYAS Protective DNS solution, HYAS Protect, which integrated easily into the organization's security stack. The security team at Portland Leather Goods immediately gained access to a whole new level of visibility into their network. Not only can they monitor and block potential malicious domains via HYAS Protect's easy-to-use interface, the platform also provides insight into legitimate network traffic.

The discovery of certain employee traffic habits, for example, led to the implementation of new company policies, which both hardened their security posture and increased overall productivity.

> **"HYAS Protect shined a light on the fact that we had no protection or any insight into what was happening, and our traffic was not monitored."**
>
> **PORTLAND LEATHER GOODS**

> **"HYAS [is an] early warning signal that something anomalous is going on to investigate right now."**
>
> **DAVID RATNER**
> CEO, HYAS

HYAS Protect brings a level of sophistication and preparedness – "big business defense" – at an affordable price. HYAS Protective DNS is easy to use and manage, can operate on its own (i.e., "set it and forget it"), and integrates with any existing security stack, making it ideal for smaller security teams who need to do more with less.

CYBERSECURITY PRIORITIZATION

If security teams seem comparatively small in large corporations, they're even smaller in growing businesses. We prize individual competence in organizations of all sizes, which can work wonders for a modest team. But can that competence be maintained or replicated if one of the star players leaves the company?

Even if cyber attacks aren't a visible threat, a cautious approach pays off in the long run. When investigated more closely, unintentional employee errors and faulty technology can often highlight significant vulnerabilities and risks.

No matter the size of the business, without a razor sharp focus on cybersecurity, companies are always one accidental misstep from a major breach. Shining a light on a lack of protection, insight and traffic monitoring in the short term can help transform internal cybersecurity policies and lead to better outcomes for businesses in the long term.

PROTECTIVE DNS: NECESSARY NEXT-GEN SECURITY

Every cybersecurity solution plays a different role in a security stack. To succeed against today's cyber attacks, they need to be interoperable, smart, and dynamic. Cyber threats are more advanced, more frequent, and more damaging. It pays to ensure that your organization is as protected as you can be against these potential attacks.

Agencies like CISA and the NSA already recommend Protective DNS as part of a modern cybersecurity approach as part of its Shields Up initiative.

Cyber insurance companies are starting to ask potential customers whether they have a Protective DNS solution in place. It may not be long before Protective DNS becomes a compliance framework requirement for companies to claim cyber insurance benefits after a breach.

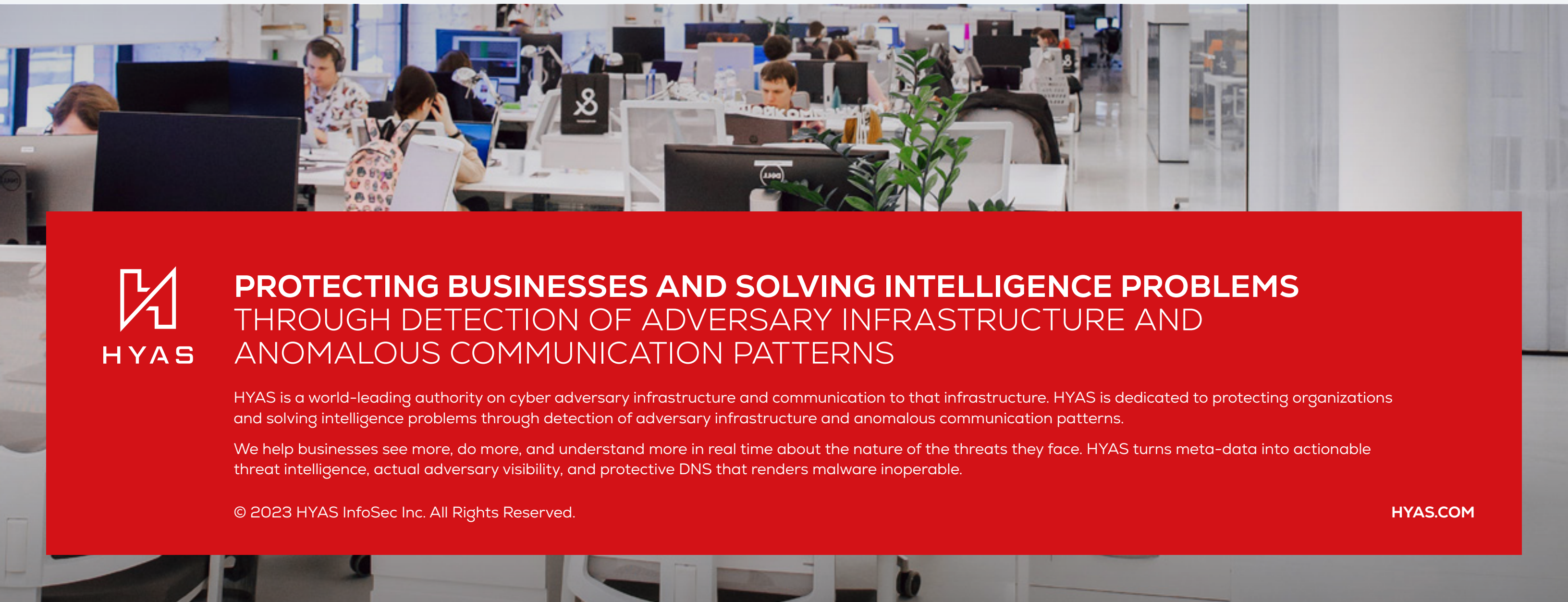
HYAS didn't invent Protective DNS. We invented how to identify and defend against adversary infrastructure and anomalous communication with unique technology and unprecedented data sources. We understand that solutions that don't work well together create vulnerabilities bad actors exploit.

Protective DNS that not only harmonizes with, but also increases the efficacy of, an organization's security stacks will drive true digital and business resilience, safeguard vital assets, and ensure operational continuity.

HYAS PROTECT

HYAS Protect enforces security and blocks command and control (C2) communication used by malware, ransomware, phishing, and supply chain attacks. All the while, it delivers on-demand intelligence to enhance your existing security and IT governance stack.

Let's connect and discover what HYAS Protect Protective DNS can do for you.



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.

HYAS.COM