




DELIVERING
THE CONFIDENCE
**TO MOVE FORWARD
WITH PROTECTIVE DNS**





EXECUTIVE SUMMARY:

Enterprises face challenges in moving business initiatives forward in the face of cyber threats.



Defense against malicious actors and their attacks has always been a cat-and-mouse game – attackers figure a way through existing defenses and when security approaches improve to stop the attack, the bad actors adjust their tactics to slip through again. Security teams routinely update antivirus signatures to counter a new strain of malware, but then the malware authors update their binary. Or, security teams employ artificial intelligence for protection only to see hackers adapt and find another way in. While the state of security has seen incremental improvements, a recent [Accenture](#) study indicated that most business leaders admit the risks are increasing, not decreasing.

Existing approaches to malware and ransomware detection and mitigation, protection against supply chain attacks, phishing, and other intrusions do not clear a confident path to progress for today's enterprises. Protective DNS analyzes DNS queries and takes action to mitigate threats. HYAS Protect provides a Protective DNS solution that enables enterprises to get in front of threats by blocking communication before damage can occur. While enterprises use layers of security that offer threat signals with varying levels of quality, HYAS Protect delivers a high fidelity threat signal to reduce the time to detect threats while avoiding security operations center (SOC) alert fatigue.

HYAS DOES NOT PLAY CAT AND MOUSE

THE GOAL IS TO CHANGE THE GAME

A paradigm shift often requires looking at a problem space differently, so rather than focus on the cyber attack itself, let's look at what happens before the attack. Before a malware or ransomware attack can be launched, bad actors need to pre-stage their command and control (C2), the infrastructure on the Internet that communicates with the malware and provides instructions on what actions to take. While today's malware authors are aware of detection technologies and typically design cyber weapons to be Fully UnDetectable (FUD) by existing protective layers, their malware still needs to communicate with C2.

Prior to a phishing attack, the fraudster needs to not only create a domain but also build a website that convincingly looks like the legitimate target website. All of these actions must occur before they can launch the very first attack, before they send the very first beacon, before they deliver the first phish, and before they can exploit any intrusion.



HYAS believes that focusing on the adversary infrastructure that is used in the attack not only provides a fundamental advantage in detecting attacks in real-time, but also provides a vital key to shift one's security defenses from reactive to proactive and to get ahead of the attacker.

NSA/CISA ON PROTECTIVE DNS

Protecting users' DNS queries is a key defense because cyber threat actors use domain names across the network exploitation lifecycle: users frequently mis-type domain names while attempting to navigate to a known-good website and unintentionally go to a malicious one instead (T1583.001); threat actors lace phishing emails with malicious links (T1566.002); a compromised device may seek commands from a remote command and control server (TA0011); a threat actor may exfiltrate data from a compromised device to a remote host (TA0010). The domain names associated with malicious content are often known or knowable, and preventing their resolution protects individual users and the enterprise.

3.7B+

DATA POINTS
PROCESSED
EVERYDAY

~200K+

MALWARE
SAMPLES
ANALYZED DAILY

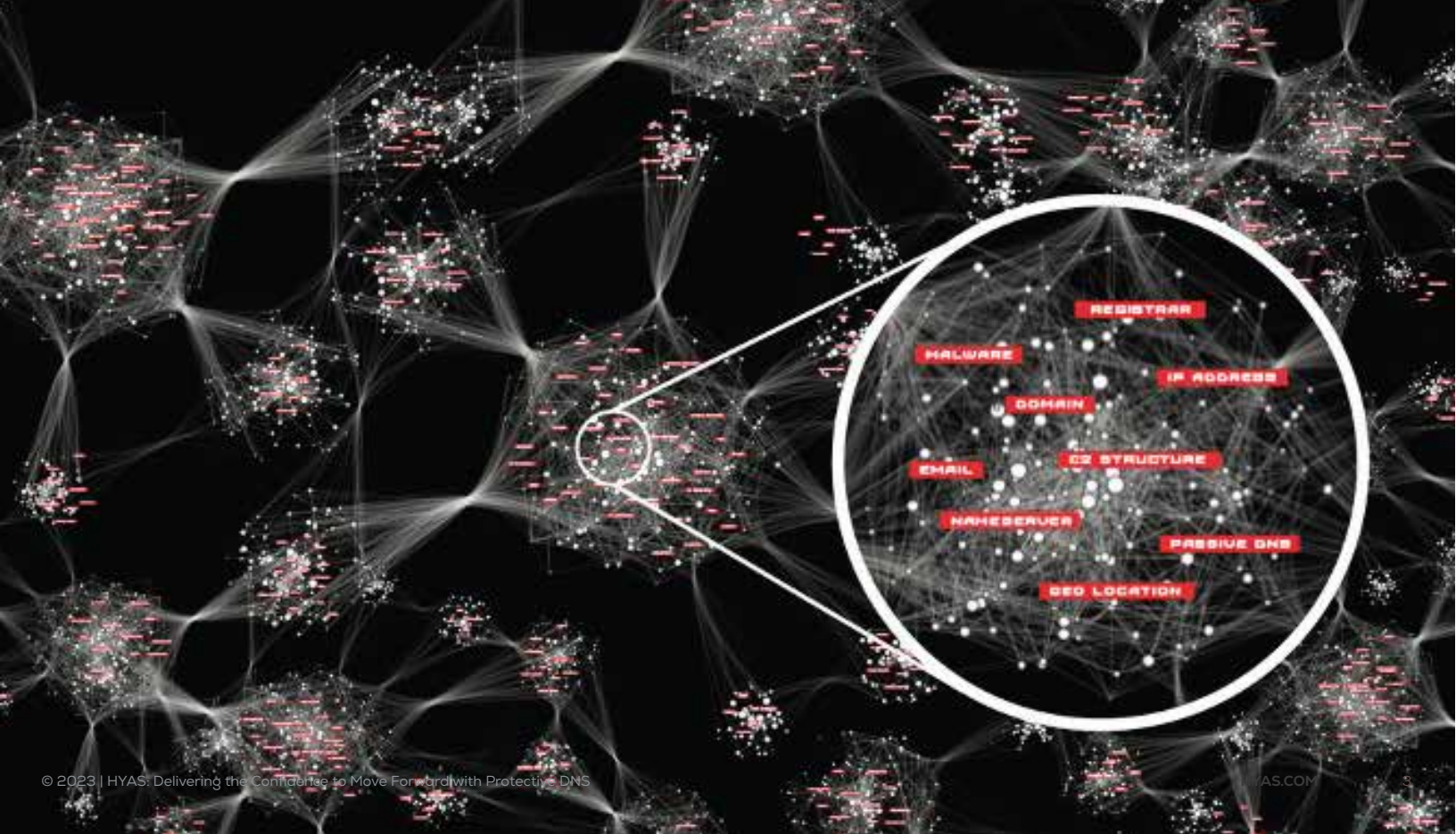
<5MINS*

NEW DOMAIN
RATINGS

HYAS IS THE LEADING AUTHORITY ON ADVERSARY INFRASTRUCTURE AND THE COMMUNICATION PATTERNS TO AND FROM IT

HYAS has built a data lake of attacker infrastructure, spanning multiple years. The ingestion of billions of data items per day, daily detonation of hundreds of thousands of pieces of malware to extract the C2 infrastructure, and the unique ability to understand correlations between diverse data points differentiates the HYAS solution set. The HYAS data lake, referred to internally as the HYAS Cerebrum because it is the main brain powering HYAS products, understands the relationships between diverse data points. These relationships allow the rapid and efficient correlation between multiple indicators, until the entire campaign infrastructure of the bad actor or actors is unveiled. While a simple allow/deny list solution may update a single data point, based on malware detonation or inclusion on an FBI Flash report, HYAS automatically updates everything in the relationship graph simultaneously, as soon as new knowledge is ingested. When new domains are published by government agencies or on security forums for companies to add to their allow/deny lists, HYAS doesn't need to manually update as our next-generation approach is fundamentally different, and the domains in question are already marked as suspicious even before their publication.

Figure 1: a visualization of the HYAS datalake



THE OPPORTUNITY TO DEAL WITH CYBER RISKS BEFORE THE ATTACK

Alert fatigue is a large challenge for most security teams. In a [recent study](#), respondents reported that over 50% of alerts were false positives and 35% said their SOC has either tried to increase staff by hiring more analysts or turned off high-volume alerting features.

HYAS Protect leverages both machine learning and an intricate decision engine to identify suspicious DNS queries. When a domain has been flagged as suspicious by the system, it is then moved into the HYAS Protect Watch Engine for ongoing monitoring (see sidebar). The goal of the Watch Engine is to significantly reduce alert noise while watching for stealthy threats that might evade conventional security approaches.

The modern enterprise security stack has a variety of components and layers and must cover an expanding attack surface. With risks continually increasing, it means that either (i) there are so many alerts generated that teams cannot distinguish fact from fiction to act efficiently and effectively, (ii) intrusions are escaping detection by the existing stack, or (iii) a combination of both. A successful paradigm shift needs to ensure that it can both find intrusions that are missed today as well as provide actionable intelligence.



HYAS Protect Watch Engine

When a domain has been flagged as suspicious, it is moved into the HYAS Protect Watch Engine. This unique engine monitors domains over time using hundreds of thousands of domain-relevant active and historical intelligence inputs accumulated by HYAS. Using query patterns, query deltas, and other behaviors across all HYAS Protect customers, the Watch Engine can move a suspicious domain into blocking and alerting or conclude that it is benign. Designed to detect sophisticated "low and slow" along with supply chain attacks, the Watch Engine minimizes false positives and false negatives to ensure consequential alerting from HYAS Protect.



Focusing on the communication patterns between an enterprise and adversary infrastructure and the threat signals that can be gleaned from these patterns of behavior provides a high fidelity risk indicator with a low false positive rate.

Additionally, looking at both the destination of communication (the “where”) and the communication pattern to it (the “how often”) provides a unique ability to provide a high fidelity threat signal that reduces alert fatigue. For example, a Google search on “Orcus Rat” may accidentally cause the browser to populate search results with prefetched contents from the malware’s C2 – it doesn’t mean that the enterprise is infected. No urgent alert needs to be generated in this case. The prefetch attempt should be blocked and marked as such on a dashboard for visibility, but it doesn’t require an immediate priority shift inside the SOC. However, a pattern of communication to the C2 clearly indicates something fundamentally different, and thus should generate an alert and an immediate response.

For example, consider the steps involved in a modern ransomware attack. While it often starts with a less sophisticated criminal finding exposed remote management services or phishing a single employee, generally this attacker will monetize the compromised machine by selling access to a more sophisticated criminal organization. The more sophisticated criminal enterprise will typically replace the initial “loader” malware that gained a foothold with second stage malware to provide remote access and use it to exploit the initial foothold. After understanding the target and performing data exfiltration as appropriate, the malware will finally be replaced with a ransomware binary and given the instruction to encrypt. All of the above steps involve communication between the enterprise and adversary infrastructure, which means that an organization that got encrypted by a ransomware attack didn’t detect any of the nefarious communications, had so many alerts that they couldn’t identify quickly enough what was actually occurring in their network, or a combination of both. Focusing on the paradigm shift – adversary infrastructure and the communication patterns to it – addresses both of these issues as well as provides other advantages to the enterprise.



FAST DEPLOYMENT MODES

BECAUSE TIME AND SURPRISE ARE ALWAYS ON THE ATTACKER'S SIDE

HYAS Protect is a SaaS solution that operates in the Microsoft Azure cloud and is “API forward” to facilitate easy integrations. It is purposely designed to be flexible and can be deployed in multiple modes depending on the requirements and existing architecture of the specific environment.

DNS Resolver

HYAS Protect can act as the external DNS resolver for a given organization. HYAS Protect is a full DNS resolver solution, complete with advanced security features such as DNSSEC, DNS over HTTPS (DoH), and DNS over TLS (DoT). However, more than a standard DNS resolver, HYAS Protect additionally inspects the target of the query, the recent communication patterns to it (i.e. whether it is a domain being monitored closely in the HYAS Protect Watch Engine), and other characteristics to make a determination of risk. If the risk is deemed too high, HYAS Protect can refuse to resolve the domain, keeping the enterprise safe. The requesting device may get a “No Such Domain” reply or otherwise be redirected to a walled garden that explains there has been a flagged security incident. Regardless of how malware enters an enterprise, it can't take any nefarious actions without communicating with its C2. Blocking the communication to the C2 thus renders the malware inert and ineffective, blocking the attack before it gets started. A key advantage of HYAS Protect as a DNS resolver lies in detection of this beaconing behavior and automatic blocking without requiring any human intervention.

HYAS Protect Agent

The HYAS Protect agent is a lightweight agent that allows devices to be protected regardless where the user is. At the office, at home, at a hotel or at Starbucks. It provides real-time verdicts, blocking traffic to threat actor infrastructure, while being transparent to the end-user. Using the HYAS Protect Agent allows for logging username with each DNS request. It also centralizes visibility and status of employee devices in HYAS Protect

Endpoint Detection and Remediation (EDR) Integration

Leverage your existing infrastructure by integrating HYAS Protect with either Microsoft Defender for Endpoint or with SentinelOne Singularity. Using the already installed EDR agents, HYAS Protect can analyze the logs from all endpoints to detect traffic to threat actor infrastructure. Optionally the integration can be configured to block subsequent communication to threat actor infrastructure. Since it uses the EDR agent, detection and blocking is possible regardless of where the user is.

Threat Signal

HYAS Protect doesn't need to be the external DNS resolver, it only needs to see the relevant network traffic. HYAS Protect can be deployed anywhere in the enterprise stack as long as it gets a mirror copy of the DNS traffic. When it detects something, it can alert the SIEM, SOAR, firewall, or other internal component. HYAS Protect can be a complete additional layer of protection that changes nothing in the enterprise stack but fundamentally acts as an enhanced and highly efficient responsive threat signal, finding the intrusions which escape or otherwise slip past the existing protection layers.

Investigation and Static Analysis

HYAS Protect can even be utilized in standalone mode. Whether as a tool for an analyst to get additional information about a given domain or an automated solution to scan messaging and social media channels and websites for the communication of and about nefarious infrastructure, HYAS Protect can easily adapt to these models given its flexible API.

MAXIMIZING SECURITY ECOSYSTEM INVESTMENTS THROUGH INTEGRATION

Although HYAS Protect is a SaaS solution with an advanced user interface custom designed by HYAS, it is purpose-built to be "API forward." Exporting a set of detailed JSON APIs allows the easy integration of HYAS Protect into any infrastructure in the security stack.

For instance, in today's hybrid work environment, protecting devices while outside of an enterprise's virtual four walls is more important than ever. HYAS Protect can integrate seamlessly with many endpoint security solutions, enabling an enterprise to add security without having to replace existing components, and fundamentally enhance and improve the effectiveness of the overall solution. Alerts can be configured to be sent to any security operations infrastructure including SIEM, SOAR, or XDR solutions. HYAS Protect can even be integrated into a firewall or other component to "super charge" the existing security investment.



SUMMARY

HYAS Protect delivers the confidence to move today's business initiatives forward. Protecting the enterprise, its users, and devices is a constant battle that requires the right processes, procedures, tools, and solutions. With changing hybrid work models, increasing concerns around detection and mitigation of supply chain attacks, the ever-increasing risks from malware, ransomware, and phishing attacks, and the sheer cost of addressing data breaches and "cleanup" post attack, HYAS believes a paradigm shift is required to effectively counter adversaries and address security in today's world. Focusing on attacker infrastructure, instead of each discrete exploit, enables a fundamentally new and next-generation approach to proactively identifying, countering, and mitigating attacks.



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. We help businesses see more, do more, and understand more about the nature of the threats they face in real time. HYAS turns meta-data into actionable threat intelligence, actual adversary visibility, and protective DNS that renders malware inoperable. HYAS's foundational cybersecurity solutions and personalized service provide the confidence and enhanced risk mitigation that today's businesses need to move forward in an ever-changing data environment. Visit HYAS.com for more details.