HYAS PROTECT

Understand and Preempt Attacker Infrastructure in Real-Time

HYAS™ Protect is a generational leap forward utilizing authoritative knowledge of attacker infrastructure including unrivaled domain-based intelligence to proactively protect enterprises from cyberattacks.

HYAS Protect is deployed as a cloud-based DNS security solution or through API integration with existing solutions. HYAS Protect combines infrastructure expertise and multi-variant communication pattern analysis to deliver reputational verdicts and actions for any domain and infrastructure, allowing enterprises to preempt attacks while proactively assessing risk in real-time. HYAS Protect can enforce security, block command and control (C2) communication used by malware, ransomware, and botnets, block phishing attacks, and deliver a high-fidelity threat signal that enhances an enterprise's existing security and IT governance stack.

Virtually all malicious software uses domain names in attacks, either for payload delivery, C2, or data exfiltration. Conventional network security approaches can fail to keep up with new, rapidly evolving threat infrastructure. By combining HYAS's proprietary threat attribution knowledge, analysis of C2 communication patterns for hundreds of thousands of daily new malware samples, and proprietary multivariate algorithms, HYAS Protect provides unparalleled visibility into attackers' assets and infrastructure, which can be utilized to uniquely and definitively answer key questions for analysts, supercharge and enhance existing assets in the security stack, and even provide an added and critical layer of protection. Even before a bad actor launches an attack involving communication to a malicious domain, HYAS Protect knows a domain's reputation and can provide a verdict that both enhances existing toolsets and preempts attacks, enabling a fundamentally more secure environment.

HYAS Protect delivers a high fidelity threat signal by leveraging machine learning and intricate logic gates to identify suspicious DNS queries. 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 historic intelligence inputs accumulated by HYAS. Using query patterns, query deltas, and other behavior across all HYAS Protect customers, the Watch Engine can move a suspect 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.

BENEFITS

Rapid & Precise
HYAS attribution data collection eliminates confidence scores, minimizes false positives and false negatives, and provides a source of domain truth on the Internet in real-time.

Comprehensive
Years of historical domain data combined with real-time analysis of communication patterns aggregated in the HYAS Protect data lake ensures a complete and thorough view of questionable and malicious domains.

Preemptive Protection
Block connection to malicious infrastructure before adversaries utilize it, and preemptively mitigate against future attacks without using conventional block and allow lists.

Cloud-Native, Rapid Deployment
Leverage global, scalable infrastructure-as-a-service for optimal scalability; deploy in minutes, anywhere in the world, with high availability and redundancy.

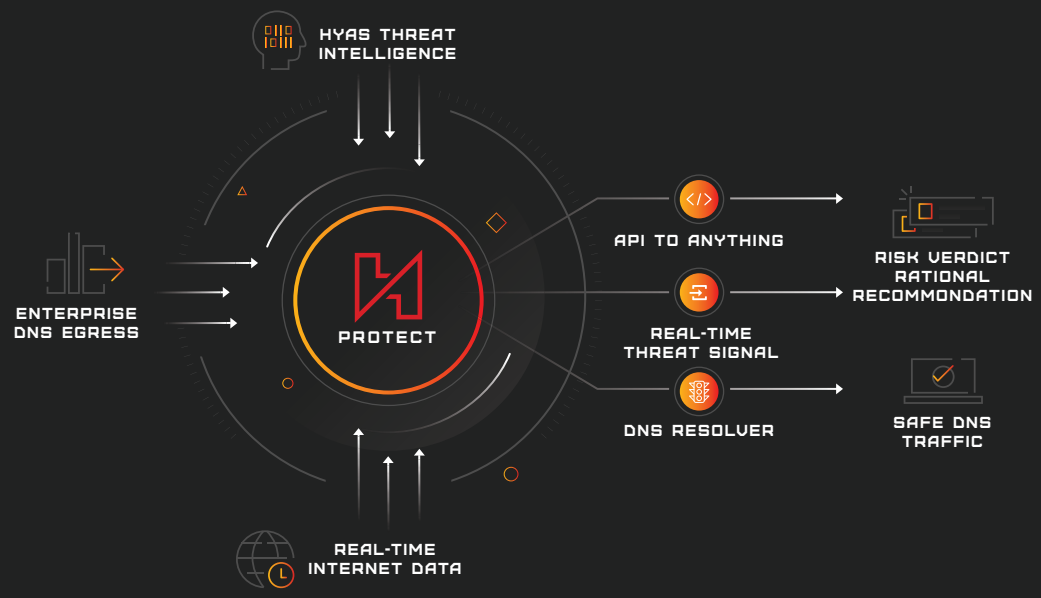
API-driven Flexibility
HYAS Protect amplifies the intelligence of your existing security stack through a new layer of protection; use HYAS Protect as a DNS resolver, integrate HYAS Protect intelligence into your SIEM, SOAR, Firewall, or other security component via easy to use APIs.

DATASHEET: HYAS PROTECT

3.3B+
Data Points Processed Every Day

~200K+
Malware Samples Analyzed Daily

<5MINS*
New Domain Ratings



*Rating for new domains registered within the past 24 hours

USE CASES

Proactive Security - Identify and prevent attacks before they happen, independent of protocol, for devices inside and outside your network. Flexible deployment supports WFH/hybrid work models and protects IoT devices.

Augment Existing Investments - Integrate via APIs with existing SIEM, SOAR, firewalls and other systems with reputation, rationale, and related data from HYAS Protect.

Dissect DNS to Augment Existing Investments - Understand your DNS traffic, sort and filter for high risk behavior, and feed that knowledge via APIs into existing SIEM, SOAR, firewalls and other systems with risk, rationale, and related data.

Threat Visibility - HYAS Protect provides a high fidelity threat signal to reduce alert fatigue and improve your network intelligence. Detect and block low-and-slow attacks, supply chain attacks, and other intrusions that are hiding in your network.

Avoid Ransomware, Phishing and Supply Chain Compromise - Stop attacks before they get started by blocking malicious domains and ensuring that users don't accidentally communicate with adversary infrastructure

DEPLOYMENT OPTIONS

DNS Resolver - HYAS Protect operates as your DNS resolver to block bad domains, IPs, and nameservers with superior security, reliability, and performance; deploy in minutes across your entire infrastructure; built-in support for DNS over HTTPS and DNS over TLS.

Real-Time Threat Signal - Verdicts and analysis of your DNS traffic augment existing security systems via API integration into your SIEM, SOAR, Firewall, or other component in your security stack.

Investigation and Static Analysis - Enable security operations center (SOC) teams investigating incidents to evaluate suspect domains or perform a static analysis of DNS egress traffic.

ABOUT HYAS

HYAS, a First Nations word meaning "great and powerful," is the world's leading authority on cyber adversary infrastructure and communication to that infrastructure. HYAS has constructed what is arguably the world's largest data lake of attacker infrastructure including unrivaled domain-based intelligence. HYAS leverages its infrastructure knowledge to deliver a generational leap forward in cybersecurity. HYAS provides the industry's first security solution that integrates into an organization's existing security technology stack to proactively detect and mitigate cyber risks before attacks happen, and to identify the infrastructure behind the attacks. Threat and fraud response teams use HYAS to hunt, find, and identify adversary infrastructure while enterprises can proactively block both known and not-yet-launched phishing and ransomware attacks at the network layer.

HYAS.COM / INFO@HYAS.COM