




SOLUTION BRIEF  
HYAS Protect

# HYAS Protect & Splunk Enterprise: Proactively Defend Against Cyber Threats with Infrastructure Intelligence

**Gain Real-Time Protection  
and Visibility Within  
the Splunk Environment**

Today's threat landscape demands more than reactive security. Organizations need proactive, infrastructure-aware solutions that identify threats before damage is done — and the integration of HYAS Protect with Splunk Enterprise delivers just that.



HYAS Protect is a next-generation Protective DNS solution powered by infrastructure intelligence — leveraging authoritative knowledge of adversary infrastructure to provide real-time reputational verdicts and block malicious activity before it can impact your organization.

By integrating directly with Splunk Enterprise, HYAS Protect empowers security teams to enhance threat visibility, enrich investigations, and enforce stronger policies — all from within the analytics platform they already use.

## Key Benefits of the Integration

### Proactive Threat Prevention

HYAS Protect analyzes communication patterns in real time to assign dynamic reputational scores to domains and infrastructure, enabling early identification and blocking of threats like malware, ransomware, phishing, and botnets — regardless of how they enter the network.

### Native Splunk Integration

The HYAS Protect app plugs directly into Splunk Enterprise, allowing analysts to run verdict lookups and threat intelligence queries from dashboards or the Splunk search bar — streamlining workflows and eliminating context switching.



“HYAS Protect is a next-generation Protective DNS solution powered by infrastructure intelligence.”

### Real-Time Verdict Lookups

Analysts can quickly determine the threat reputation of an IP, domain, FQDN, or nameserver using HYAS Protect’s Verdict Lookup Dashboard — giving SOC teams immediate insights into indicators of interest.

### Automated Enrichment and Response

Custom search commands and adaptive response actions let security teams automate verdict lookups during alert triage or incident investigation, accelerating time to response.

## Core Capabilities

### HYAS Protect Verdict Lookup Dashboard

A user-friendly Splunk dashboard that enables fast and efficient threat verdict queries:


- Select indicator type: IP, Domain, FQDN, or Nameserver
- Enter the value
- Submit to retrieve a live verdict from HYAS Protect
- Results are displayed in Splunk for further analysis and correlation

### Custom Search Commands

Run HYAS Protect queries directly from Splunk’s search bar to enrich data and streamline investigations

### Splunk ES Adaptive Response Integration

Security teams using Splunk Enterprise Security can enrich alerts on the fly via adaptive response actions:

- Select a notable event in Incident Review
  - Run the HYAS Protect verdict lookup
  - View enriched threat data directly in the Splunk UI — no pivoting required
- 



## Example Use Cases

### Threat Prevention

Preemptively block access to high-risk domains and infrastructure using real-time reputation verdicts — stopping threats like phishing or C2 communication before they execute.

### Alert Triage

Use HYAS Protect's adaptive response actions to add context to alerts in Splunk ES, reducing noise and enabling faster decisions.

### Incident Investigation

During an active investigation, quickly query domains, IPs, or FQDNs from within Splunk to uncover threat context and map malicious behavior.

### DNS Visibility

Gain a deeper understanding of DNS traffic and infrastructure communications across your environment, enhancing detection and forensic capabilities.

## How to Get Started

### 1. Download the App

Find the HYAS Protect App for Splunk on Splunkbase.

### 2. Install & Configure

Deploy the app in your Splunk Enterprise environment and configure your HYAS Protect API credentials.

### 3. Start Querying

Use dashboards, search commands, or adaptive response actions to begin enriching indicators and proactively defending against threats.

## Supported Indicator Types

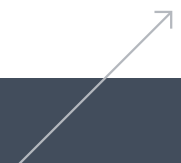
- IP Addresses (IPv4, IPv6)
- Domains
- FQDNs
- Nameservers

## About HYAS

HYAS is the world's premier provider of infrastructure intelligence, enabling organizations worldwide with unparalleled visibility, protection, and the necessary proactive intelligence to address cyber attacks, fraud, and all forms of digital risk. Independently tested with proven efficacy, HYAS Protect delivers business resiliency against all forms of cyber attacks, regardless of the attack vector or how the organization was breached.

### Want to see it in action?

Contact us at [info@hyas.com](mailto:info@hyas.com) or visit [www.hyas.com](http://www.hyas.com) to learn more or schedule a demo.



# 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 [→](#)



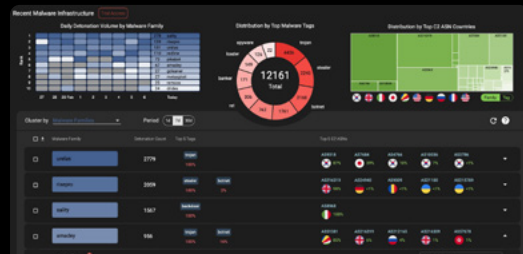
## THREAT INTELLIGENCE & INVESTIGATION

### HYAS Insight

Threat Intelligence & Investigation

HYAS Insight 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 [→](#)



Contact Us For a Demo  
[hyas.com/contact](https://hyas.com/contact)



## 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.