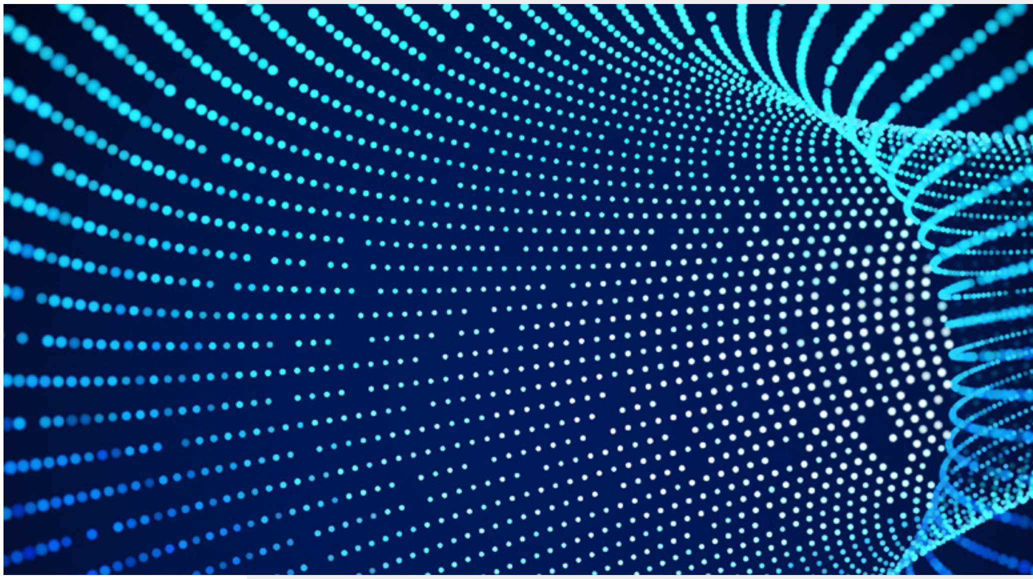
HYAS



SOLUTION BRIEF
HYAS Protect

Comprehensive Defense Against DNS Tunneling Attacks

Cyber attacks that exploit the fundamental Domain Name System (DNS) have grown in frequency and sophistication, and organizations can struggle to safeguard their networks. DNS tunneling has emerged as a favored method for cybercriminals, which allows them to covertly exfiltrate data and establish command-and-control channels.

To effectively counter these threats, HYAS Protect protective DNS not only detects and blocks DNS tunneling but also fortifies overall network security across IT and OT environments.

HYAS PROTECT
Protective DNS

- Real-time protection with the HYAS Protect Decision Engine
- Unrivaled intelligence from the HYAS Adversary Infrastructure Platform
- Enforce appropriate use policies with flexible content filtering
- Flexible deployment options adapt to your environment
- Get visibility on blocked and suspicious traffic
- Robust API for custom automation

The Challenge: DNS Tunneling in Critical Environments

DNS tunneling is a covert attack method where data is embedded within DNS queries and responses, enabling the stealthy transfer of information across network boundaries. This technique is particularly dangerous in Operational Technology (OT) environments, where safety and availability are paramount, often at the expense of security. A successful DNS tunneling attack can lead to severe consequences, including data breaches, operational disruption, and compromised critical infrastructure.

HYAS Protect: A Comprehensive Defense

HYAS Protect is the leading protective DNS solution that offers real-time detection and prevention of DNS-based threats, including DNS tunneling. Leveraging advanced threat intelligence and machine learning, HYAS Protect ensures that malicious DNS traffic is identified and blocked before it can cause harm. This solution is designed to enhance the security posture of both IT and OT environments, providing a robust defense against evolving cyber threats.

Key Features and Differentiators

Proactive Threat Detection and Blocking: HYAS Protect continuously monitors DNS traffic, utilizing advanced analytics to detect signs of malicious activity, such as DNS tunneling. The solution automatically blocks suspicious queries, preventing attackers from establishing communication channels or exfiltrating data, thereby protecting the network from potential threats.

Seamless Integration with IT and OT Environments: HYAS Protect is designed for easy integration into existing network infrastructures, whether in IT or OT environments. This ensures that the solution can be deployed without disrupting critical operations, providing comprehensive protection across all areas of the organization.

Enhanced Threat Intelligence and Attribution: Powered by HYAS's deep threat intelligence capabilities, HYAS Protect not only detects and blocks malicious DNS traffic but also traces it back to its source. This enables security teams to understand the full scope of an attack, facilitating a more informed and effective response.

Comprehensive Visibility and Control: HYAS Protect provides granular visibility into DNS traffic, allowing security teams to monitor, analyze, and control all DNS queries and responses. This level of oversight is crucial for identifying anomalies, such as those associated with DNS tunneling, and enforcing security policies across the network.

Zero-Touch Configuration and Management: HYAS Protect offers zero-touch configuration and management, minimizing the operational overhead for security teams. This feature ensures that the solution can be deployed quickly and efficiently, with minimal impact on resources and no need for extensive manual intervention.

Flexible Deployment Options: HYAS Protect is a cloud based, SaaS platform with a multitude of flexible deployment options, including EDR integrations, agentless, and agent-based options that can be tailored to meet the unique requirements of any organization.

Active Adversary Infrastructure Identification: HYAS Protect excels in identifying active adversary infrastructure through its real-time threat intelligence analysis. This capability allows organizations to stay ahead of emerging threats, blocking malicious domains and IPs before they can be used in attacks.

Use Case: Detecting and Blocking DNS Tunneling in OT Environments

In a recent deployment, HYAS Protect was utilized in a critical OT environment where traditional security solutions had failed to detect DNS tunneling. HYAS Protect's advanced decision engine quickly identified the malicious DNS traffic and blocked the tunneling attempts, safeguarding the network from potential data exfiltration and operational disruptions. This successful deployment not only reinforced the security of the OT environment but also showcased HYAS Protect's effectiveness in diverse and challenging scenarios.

Conclusion

As cyber threats targeting DNS become more sophisticated, organizations require intelligent and powerful solutions to protect their networks. HYAS Protect delivers unparalleled protective DNS capabilities, effectively countering DNS tunneling and other DNS-based threats while providing comprehensive visibility, control, and operational efficiency. Whether deployed in IT or OT environments, HYAS Protect is the cornerstone of a robust cybersecurity strategy, ensuring the safety and resilience of critical infrastructure.

HYAS Protect Key Features

- HYAS's real-time decision engine evaluates each outbound DNS request on your network or endpoint to determine whether it should be permitted. Utilizing over 50 meticulously refined rules and processes, our engine instantly responds to user requests, enabling access to safe sites while blocking malicious or inappropriate ones.
- The HYAS Decision Engine is powered by infrastructure intelligence sourced from the HYAS Adversary Infrastructure Platform. This platform processes billions of data points daily, utilizing unique and proprietary, restricted, commercial, and open-source intelligence sources. It profiles the latest malware infrastructure, suspicious domain registrations, and various other risk indicators to ensure robust protection.
- Set appropriate use policies by configuring specific internet categories that employees are prohibited from accessing. You can also establish allow and blocklists and create custom rules for additional protection. Integrate your Microsoft Entra ID (Azure AD) groups with custom policies for streamlined, enterprise-wide enforcement.
- Dashboards, custom filters, and alerts provide visibility into blocked, malicious, and suspicious traffic, helping you stay proactive and enhance your organization's resilience.
- HYAS Protect APIs give you the power to build automation that supports your operational goals, whatever they are.

Fortify and Future-Proof Your Network

The threat landscape is constantly changing, so cybersecurity tactics must evolve as well. By incorporating these threat intelligence best practices, any security team can build a robust defense against malware, phishing, DDoS attacks and whatever comes next. But it's critical to review and update your threat intelligence processes and tools regularly. Stay informed about new threats, technologies and the latest lines of defense — and adapt your strategies accordingly.

With HYAS solutions, including HYAS Protect (our PDNS solution) or HYAS Insight (our leading-edge threat intelligence and investigation platform), organizations of any size can integrate award-winning cybersecurity technology into their existing stacks. We make it seamless, simple and scalable, so your network stays safe — and you can focus on what you do best.

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 →

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.