HYAS

Member of
Microsoft Intelligent
Security Association

Microsoft

HYAS Protect and **Microsoft Defender** for Endpoints

Secure Your Endpoints

Changing digital landscapes, a remote and hybrid workforce, proliferating network environments all continuously increase the risk of cyberattacks. More devices mean more endpoints, and threat actors will always seek out the most vulnerable new endpoints. Security teams must contend with the increased speed at which businesses now operate, which makes maintaining legacy block and allow lists an even heavier burden.

- 68% of organizations have experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastructure (Expert Insights, 2023)
- In 2022, 76% of organizations were targeted by a ransomware attack, out of which 64% were actually infected. Only 50% of these organizations managed to retrieve their data after paying the ransom. Additionally, a little over 66% of respondents reported to have had multiple, isolated infections. (CSO Online)
- 74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering. (Verizon 2023 Data Breach Investigations Report)

Now, organizations can confidently mitigate future attacks without the labor of maintaining block and allow lists. Attackers continue to adapt, and HYAS adapts right along with them in real time, safeguarding your data from threats and clearing a path for your business to move forward.

Preempt Attacks and Proactively Assess Risk in Real Time with HYAS Protect

1. **Deploy Anytime, Anywhere**

   Enable easy deployment and simplify security management requiring no additional agent.

2. **Identify and Prevent Attacks**

   Gain unrivaled visibility into risk before communicating to any domain.

3. **Cut Malicious Connections**

   Stop connections to malicious infrastructure before adversaries carry out their attacks.

Deploy **Anytime, Anywhere**

QUICK AND EASY DEPLOYMENT ENHANCES THE VALUE OF YOUR EXISTING ENDPOINT SOLUTIONS

Organizations are under constant fire. In 2022, organizations detected nearly 500 million ransomware worldwide[1]. On average, the most common entry point for ransomware is phishing and 93% of ransomware is Windows-based executables[2]. In this endless barrage of attacks, businesses do not have the luxury of time when it comes to deploying new security solutions. And unfortunately, deploying a Protective Domain Name System (PDNS) solution is not always efficient, as it can require installing another agent.

> **"The integration of Microsoft Defender for Endpoint with HYAS Protect allows us to work together to help customers navigate the security landscape."**

ROB LEFFERTS
CORPORATE VICE PRESIDENT, MICROSOFT DEFENDER

HYAS Protect is a cloud-native infrastructure-as-a-service, recognized by the NSA and CISA, that scales infinitely and deploys in minutes. When you layer it with Microsoft Defender for Endpoint you build a stronger security solution to protect your corporate network and endpoints from cyber threats, detects advanced attacks and data breaches, automates security incidents, and improves security posture.

Since Defender for Endpoint is included with Microsoft 365 E3 and E5, adding HYAS Protect is quick and easy with no additional agent required. HYAS will walk you through the setup process and will be your trusted Protective DNS partner.

Use Case: Protective DNS

Identify and prevent attacks before they happen, independent of protocol, for devices inside and outside your network. Our fast and flexible deployment supports WFH/hybrid work models and protects all kinds of devices (IoT, servers, mobile, stationary, and more).

Identify and **Prevent Attacks**

DETECT AND BLOCK COMMUNICATION WITH MALICIOUS URLS AND DOMAINS

As organizations embrace digital transformation, the speed at which they do business and the number of endpoints they operate increases as well. Security teams need to be able to identify potential risks and act quickly to mitigate threats coming from all angles. Unfortunately, conventional DNS firewalls are blind and must rely on slowly updated global block and allow lists, rendering them essentially ineffectual as new threat campaigns are launched and enough targets are successfully breached.

At HYAS, we have collected years of exclusive historical domain data and execute real-time communication pattern analysis to create the HYAS Protect data lake, providing our clients with unrivaled visibility into risk before communicating with any domain.

The HYAS Protect integration with Microsoft Defender for Endpoint improves enterprise security by analyzing Defender for Endpoint sensor data to detect communication with malicious URLs/domains and blocking them. Combining machine learning with authoritative knowledge about attacker infrastructure and unrivaled domain-based intelligence, HYAS Protect not only proactively secures organizations, it also augments and improves the efficacy of existing components. Our combination of infrastructure expertise and multivariate pattern analysis provides an immediate, reliable, and high-fidelity source of truth to mitigate threats in real time.

Use Case: 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 hiding in your network.

Cut **Malicious Connections**

BREAK COMMUNICATION WITH MALICIOUS INFRASTRUCTURE BEFORE ADVERSARIES COMPROMISE YOUR DATA

IBM reported that it takes businesses an average of 277 days to identify and report a data breach, and on top of that, the average cost of a data breach is nearly 4.5 million dollars[3]. This poses a clear problem.

HYAS Protect combines infrastructure expertise and multivariate communication pattern analysis to render reputational verdicts for any domain or infrastructure, allowing Microsoft Defender for Endpoint to preempt attacks at the network layer. We stop connections to malicious infrastructure before adversaries can use it.

And since attackers constantly adapt their infrastructure, HYAS also adapts in real time, safeguarding you from advanced mechanisms such as DGA. HYAS also eliminates confidence scores and minimizes false positives and false negatives, ensuring you have access to an instant source of truth.

Use Case: Security Compromise

Stop attacks before they get started, ensuring that users, devices, or servers don't accidentally communicate with adversary infrastructure to avoid ransomware, phishing, and supply chain compromise.

Solution **Overview**

ATTACKERS ONLY HAVE ONE WAY OUT

While attackers have many potential access points to exploit when attempting to harm your business, they have only one way out – the internet.

Regardless of how the bad actor initially gets inside the network, most attacks require communication between the program or malware inside the organization and the bad actor's command and control (C2) infrastructure outside the enterprise for instructions, lateral motion, potential data exfiltration, and next steps. Whether an attack originated because of a modern architecture library, a supply chain vulnerability, or a new IoT device, the fact that they all require external C2 communication is the Achilles' heel that enterprises can use for visibility, control, and prevention.

BLOCK ATTACKS AND CLEAR A SAFE PATH FOR INNOVATION WITH HYAS PROTECT AND MICROSOFT DEFENDER FOR ENDPOINT

- Automate security with easy deployment and simplified management requiring no additional agent.
- Reduce security operations center (SOC) noise with a high-fidelity threat signal, minimizing false positive alerts.
- Avoid phishing attacks and render malware inert by blocking communication to phishing domains and stopping communications to malware command and control infrastructure.

UNDERSTANDING PROTECTIVE DNS

Protective DNS is an important layer of threat mitigation that is gaining the attention of private enterprises and government organizations as a critical next-generation security control, and should be the base-layer of any modern security stack. Its utility for preventing attacks augments regularly deployed network and endpoint security tools.

Benefits include better availability of resources and higher levels of compliance, as well as security advances such as greater visibility, faster mean time to detect threats, and proactive prevention of inbound malware and outbound connections to infected entities.

Focus Less on Threats **and More on the Future**

It takes the most proactive security possible to support today's rapid pace of business. The HYAS Protect integration with Microsoft Defender for Endpoint improves enterprise security by analyzing Defender for Endpoint sensor data to detect communication with malicious URLs/domains and block them.

Using authoritative knowledge of attacker infrastructure and unrivaled domain-based intelligence, HYAS Protect augments your existing security solutions to proactively protect your organization.

[1] Statista.com

[2] AAG-IT.com

[3] IBM.com

HYAS Protect and Microsoft Defender for Endpoint help ensure business resiliency, no matter what comes at you. Users gain an instant source of truth with full visibility and control so you can focus on driving your business forward.

Schedule a Demo

Visit the Website

Find Us on the Microsoft Commercial Marketplace

Member of
Microsoft Intelligent Security Association

Microsoft

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.

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.

HYAS.COM