HYAS
FULL FORWARD

BLOCK ATTACKS **BEFORE THEY BEGIN**

Proactively Protect Your Organization and Mitigate Threats in Real Time with HYAS Protect and Microsoft Defender for Endpoint

Microsoft Security

TABLE OF **CONTENTS**

HOW SECURE **ARE YOUR ORGANIZATION'S ENDPOINTS?**

The More You Go Digital, the More Doors You Must Guard Against Cyberthreats

With an increasing number of organizations embracing digital transformation and shifting to a remote workforce, the opportunity for cyberattacks has increased as well. More devices means more endpoints, and as this trend continues, threat actors will take advantage of this proliferation of vulnerable new endpoints – making them more difficult to constantly outmaneuver. Security teams will also have to contend with the increased speed at which businesses now operate, making maintaining legacy block and allow lists an even heavier burden.

- **An average of 360,000 malicious files were detected per day globally in 2020.[1]**
- **In 2021, a consumer or business suffered a ransomware attack every 11 seconds.[2]**
- **By 2025, it is estimated that the global cost of cybercrime will reach $10.5 trillion.[2]**

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

DEPLOY ANYTIME, ANYWHERE

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

IDENTIFY AND PREVENT ATTACKS

Gain unrivaled visibility into risk before communicating to any domain.

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

Today's threat actors keep organizations under constant fire. In fact, on average, businesses suffered a ransomware attack every 11 seconds in 2021.[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.

HYAS Protect is a cloud-native infrastructure-as-a-service, recently 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.

"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 for Microsoft Defender*

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

From 2020 to 2021, the average time it took organizations to identify and contain a data breach increased from 280 to 287 days.[3] On top of that it takes these organizations 80 days on average to contain a breach, this poses a clear problem.[4]

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.

HYAS
FULL FORWARD

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.

With HYAS Protect and Microsoft Defender for Endpoint, you finally have an instant source of truth to help you focus less on bad actors and more on driving your business forward.

SCHEDULE **A DEMO**

VISIT **THE WEBSITE**

FIND US **ON THE MICROSOFT COMMERCIAL MARKETPLACE**

[1] The number of new malicious files detected every day increases by 5.2% to 360,000 in 2020, Kaspersky

[2] 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics, Cybersecurity Ventures

[3] Cost of a Data Breach Report, 2021, IBM

[4] Cost of a Data Breach Report, 2020, IBM

Microsoft Security