CASE STUDY

Why a Silicon Valley Startup **Chose HYAS for DNS Protection**

For a Silicon Valley software company that serves major global corporations, security and compliance are key.

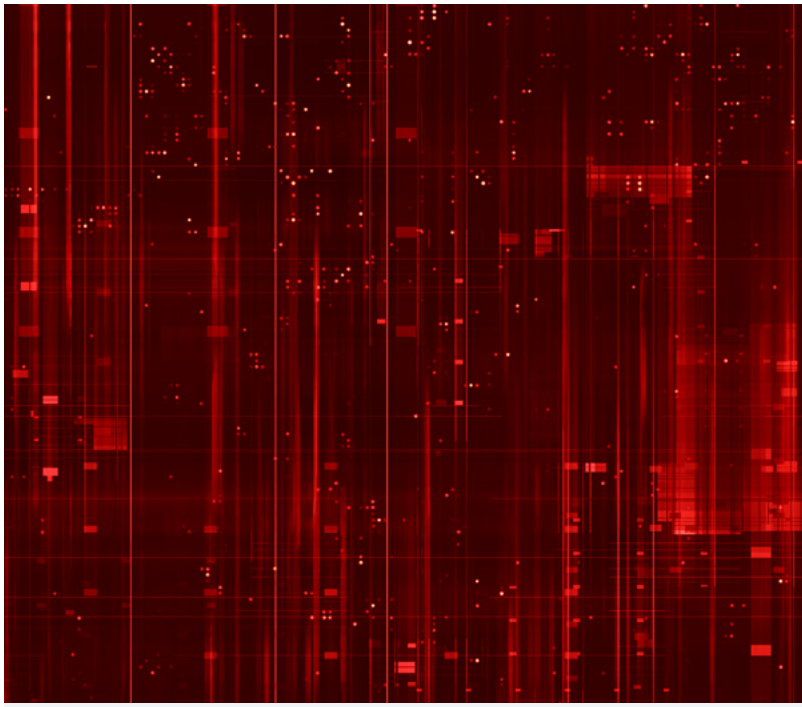
The startup builds technology that helps organizations improve their cyber resilience – so having its own strong cybersecurity posture is non-negotiable. With customers around the world that operate in sectors like financial services, telecommunications and retail, the company must also comply with many different regulatory regimes.

The company's cloud security architect chose HYAS Protect as its protective DNS solution. HYAS complements the company's existing cybersecurity infrastructure, providing greater visibility into indicators of compromise (IOCs) and better protecting endpoints that its other capabilities can't cover.

The Challenge: Protecting the Internal Data Center

The company, which has a headcount slightly north of 100, has employees around the world. Its cloud security architect is responsible for protecting both its public cloud – which uses Amazon Web Services, Google Cloud Platform and Microsoft Azure – and its internal data center. He also serves as the technical resource for many security concerns within the company, as well as issues related to governance, risk and compliance (GRC).

The company has historically relied on Suricata as its intrusion detection system (IDS) and intrusion prevention system (IPS) for its internal data center. It also uses SentinelOne for endpoint protection.



HYAS: The Experts on Adversary Infrastructure

Every HYAS solution is powered by the company's adversary infrastructure platform: a large, dynamic data lake that constantly ingests data from a variety of exclusive, private and commercial sources.

HYAS customers benefit from the company's unparalleled knowledge of attackers – and that's exactly why one Silicon Valley startup chose HYAS Protect to help it monitor for indicators of compromise (IOCs). "HYAS has actually done the IOC research," the company's cloud architect says.

HYAS Protect was added to the security stack to gain visibility that existing protections couldn't provide. "We've got some fairly robust endpoint protection," the cloud security architect says, "but it doesn't catch everything where we can't install it."

HYAS Protect enables the company to better understand its traffic patterns and monitor for IOCs. "We actually get a lot better DNS visibility than we would with a bare Suricata instance," the cloud security architect says. "Because everything in our data center is already using our internal DNS server, which uses HYAS as a forwarder, we get a lot more coverage in a much easier way."

Why HYAS: Meeting Global Compliance Standards

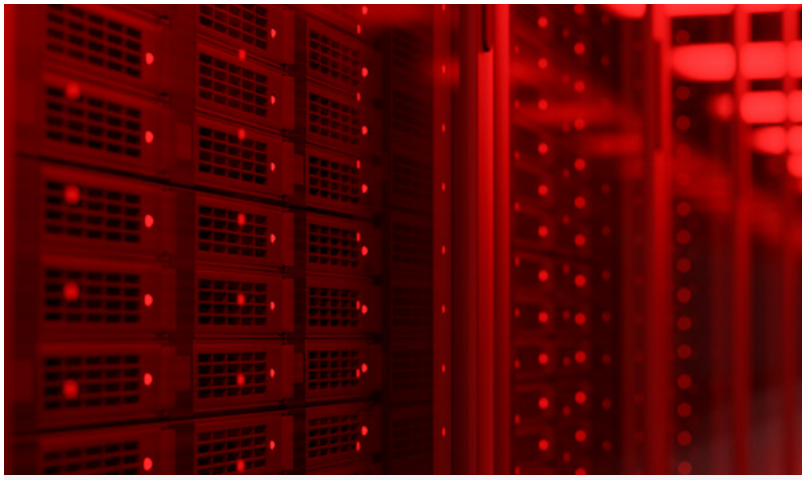
One of the main reasons the company turned to HYAS was to help its GRC team cover compliance requirements. With customers around the world in a variety of highly regulated industries, the company needs a reliable and flexible security posture that can adapt to new and changing requirements. "GDPR and CCPA are actually relatively easy," the cloud security architect says. "We've had a pretty robust process in place for years." But ISO27001 has posed greater challenges as a larger-scale framework with a broader range of requirements: while GDPR and CPPA focus on protecting personal data, ISO27001 is intended to help businesses protect against all information security risks.

To address needs related to ISO27001, the cloud security architect assisted the GRC team in identifying and implementing the necessary tools to fulfill various compliance requirements, including HYAS Protect.

Customer requirements are another area to address. Many of the startup's customers need to understand its compliance posture as part of their vendor due diligence. With HYAS Protect, the company can assure its clients that DNS monitoring is part of its security information and event management (SIEM) stack.

> **"HYAS has already done all the IOC research. So, you're pulling in that threat intelligence and blocking stuff straight away."**

HYAS Protect allows organizations to proactively enforce security by detecting and blocking communication by malware, ransomware, phishing and other types of cyber attacks. It covers devices inside and outside of a network, which is crucial for companies with remote employees.



HYAS in the Security Stack

HYAS is designed to augment and amplify existing cybersecurity infrastructure. It provides easy-to-use APIs that connect to SIEM, SOAR, firewalls, endpoints, and other security components.

The startup uses HYAS in combination with:

- Elasticsearch for security information and event management
- Suricata for intrusion detection and prevention
- SentinelOne for endpoint protection
- Google as a backup DNS forwarder

Integrating Seamlessly Into a Security Posture

HYAS Protect is only one component of the company's approach to cybersecurity. It uses Elasticsearch as its SIEM solution and has maintained its Suricata and SentinelOne deployments.

For architecture, primary and secondary domain controllers are used as DNS servers. HYAS Protect serves as the primary forwarder, with Google as a backup.

Right now, HYAS is deployed as a standalone, but the company is reworking its logging and plans to start ingesting HYAS Protect into the SIEM infrastructure soon. The company is also preparing to implement blocking as it works toward moving development into the public cloud.

The cloud security architect looks forward to the benefits of blocking for its security infrastructure. In particular, he's excited to capitalize on HYAS's unparalleled knowledge of adversary infrastructure.

Once the company can pull blocking data into its SIEM, it can correlate blocking with known issues: "I think HYAS data will greatly enrich the incident response process."

Building a Foundation to Scale Progress

Though the company is early in its HYAS journey, the cloud security architect looks forward to continuing to partner with the HYAS team.

"Everyone at HYAS been great to work with," he says, noting that the team's willingness to talk him through what they're seeing has helped him see how the product applies to the company's environment.

He also has praise for the platform itself. "It's a very easy platform. The UI is very easy to use and very easily understood," he adds. For a team of just three people, ease of use is critical – especially for a company whose clients rely on its software to make their organizations safe.

With significant growth on the horizon, the company needs trustworthy security partners. And it knows it's in good hands with HYAS.

> **"It's a very easy platform to use. The UI is clean and easily understood. And everyone at HYAS been great to work with."**

HYAS Grows With Your Enterprise

The startup's cloud security architect chose HYAS in part because of the possibilities it offers for future growth. In addition to DNS protection, HYAS offers solutions for:

- Providing proactive insight into potential threats
- Investigating incidents and locating the sources of attacks
- Determining whether cleanup after an incident was successful
- Establishing a baseline of normal DNS traffic to improve detection of anomalies

CONTACT US FOR A DEMO
hyas.com/contact

IDENTIFY AND BLOCK
ATTACKS BEFORE THEY HAPPEN

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.