CASE STUDY

PREPARING FOR THE FUTURE

As threats evolve and change, cybersecurity standards and requirements—whether imposed by governments or other organizations—also need to be adjusted. As a testing lab, all of the requirements that the client company's product must follow are flowed down the line to each of the third parties they work with, including testing services. It doesn't matter that some of these regulations won't go into effect for years, the lab's customers were already asking for their products to be certified according to the new standards.

After learning about HYAS through a report on the importance of protective DNS issued by the NSA and CISA,

> **From a competitive advantage perspective, the more we meet the requirements, the more often they (clients) call us. So when we start missing out on a contract, that's going to affect others down the line. Even if they don't tell us right now, it's in our best interest to be ready when they are.**

STEVE BOYLE, INFORMATION SYSTEMS MANAGER, EXPERIOR LABS

Boyle reached out and ultimately tried out a proof of concept demonstration, which impressed him enough to sign on. Of particular interest was the fact that Protect utilizes heuristic-based DNS protection—which actively monitors traffic for suspicious behavior—in addition to the more reactive rule-based protection, which blocks domains associated with an attack once it has already broken out. Unfortunately, by the time the block and allow lists have been updated, a business may already have been affected by the threat.

COMPANY AT A GLANCE

Since its founding in 2003, Southern California-based Experior Labs has become one of North America's fastest growing third-party testing laboratories, providing certification and qualification laboratory services. The company caters to a wide variety of industries, including telecommunication, military, aerospace, space, industrial, rail, medical, automotive and others. It offers testing in rugged conditions, including vibration, shock, temperature, and environmental, and can fulfill a wide variety of standards from organizations like ISO, UL, and many government agencies.

CHALLENGES

- Because Experior Labs needs to be compliant with a wide variety of standards to be eligible for certain contracts, it has to proactively prepare for upcoming requirements.
- Despite the limited size of its IT team, the company needed to roll out HYAS Protect to cover their corporate network and more than 200 end devices.
- IS Manager had worked with a larger competitor in the past and disliked the experience. Wanted a company that would provide personalized support.

RESULTS

- Better prepared to defend against threats.
- Provide the confidence needed to allow them to focus on growing their business.
- Rollout was incredibly smooth. Simple as changing to HYAS DNS resolver.
- All support tickets were handled quickly and to the customer's satisfaction.

EASY ROLLOUT

Experior Labs has experienced steady growth in recent years and has approximately doubled in size over the past four years. As a result, their network environment has also grown considerably, so any additional cybersecurity solutions needed to be able to be easily implemented on all end devices across their network. This turned out to be as simple as pointing the company's internal resolver to HYAS's DNS resolvers. Other than that, the only other step was deactivating any browser-based DNS services to make sure every device was pointing to HYAS. Better yet, once deployment was complete, Boyle found that he could effectively manage it himself.

INCREASED NETWORK VISIBILITY

One of HYAS Protect's core features is the ability to proactively block attacks before they get started by tracking adversary infrastructure as it is being built out. Protect even goes one step further by providing constant monitoring of your DNS traffic within your network. This provides another layer of security by alerting admins to suspicious activity, allowing them to block communication between malware on the network and the command and control (C2) structure that directs its actions after infection. It also gives users more practical visibility into their network. One of the Experior Labs team's favorite features was the way Protect aggregates DNS traffic in one spot, making reporting easier. While monitoring their traffic, the IT manager noticed that a number of internal DNS names were leaking out through devices joining their guest network. He was able to remedy this by reconfiguring the firewall to capture this internal traffic and reroute it to an internal server. "I would not have figured that out if I was not running HYAS Protect," he said.

PERSONAL TREATMENT AND SERVICE

HYAS also prides itself on its superior customer service and care, so we worked closely with Boyle to implement HYAS Protect and address any questions that came up. He had previously worked with one of HYAS's large protective DNS competitors and had not been a fan of the experience. So a large factor in his decision making was finding a partner that didn't just treat him like a number. "I appreciate that you are a younger, hungrier company," Boyle said. "I feel like I mean something to HYAS."

Since signing on with Protect in the spring, Experior and the HYAS team have maintained an ongoing dialogue to best understand what features they would most like to see added to the product in the future and how to implement new features as they roll out. "I've gotten to see the product evolve over time," Steve notes

CONTACT US FOR A DEMO

sales@hyas.com

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.

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