



CASE STUDY

PARTNERSHIP WITH HYAS

# HELPS PORTLAND LEATHER GOODS STAY BULLISH

## EXECUTIVE SUMMARY

- As a small but rapidly expanding business, Portland Leather Goods had limited resources to devote to cybersecurity and needed high-efficacy solutions.
- They settled on HYAS Protect because of its focus on proactive security and visibility.
- Deployment was easy and the UI intuitive.
- Traffic monitoring helped lead both security and productivity-boosting policy changes.

## SMALL BUSINESSES FACING BIG THREATS

No matter the size of the business, in today's cybersecurity landscape, every organization is a target worth exploiting. While attacks on giant corporations like Target, T-Mobile, and Uber grab the headlines, small and medium-sized businesses (SMBs) bear an unfair share of cyber attacks. With limited access to critical resources and advanced threat detection teams, SMBs tend to be both the least prepared to deal with attacks and also the least likely to be able to recover from one. The types of threats SMBs face are exactly the same ones (phishing, ransomware, data exfiltration, etc.) that companies with thousands of employees, robust security teams, and billion-dollar balance sheets face.

Despite the odds, SMBs need to employ enterprise-quality security solutions if they hope to stand a chance against this constantly evolving threat environment. They do not, however, have enterprise-level resources to devote to security, making the choice of which solutions to implement even more deliberative. Every piece of an SMB's security stack must carry its weight by providing the broadest, most accurate protection possible.



## SMB THREAT LANDSCAPE

- Nearly 50% of all cyber attacks are aimed at SMBs.
- 82% of ransomware attacks target SMBs.
- 61% of SMBs experienced an attack in the previous year.
- 50% of the SMBs that were successfully attacked reported recovery times of more than 24 hours.
- 43% SMBs do not have any cybersecurity plan in place.
- 83% of small and medium-sized businesses are not financially prepared to recover from a cyber attack.

## SKIN IN THE GAME

Portland Leather Goods is a rapidly growing lifestyle brand that was founded just seven years ago in a garage in Portland, Oregon. As the company expanded, so did its cyber risk profile. When some missing folders caused a

**“I feel like we’ve been validated in our decision time and time again.”**

ISAAC SPENCER

IT MANAGER, PORTLAND LEATHER GOODS

scare, the security team realized the company’s success had painted a bigger target on their back and needed to prepare accordingly. After looking into a number of other vendors, Portland Leather Goods chose the HYAS platform because they appreciated its proactive approach to cybersecurity and felt a kinship with HYAS’s company values and trajectory.

## FOUNDATIONAL SECURITY

By choosing HYAS Protect, Portland Leather Goods could safeguard users within their network from wittingly or unwittingly connecting to a malicious domain. The industry-leading protective DNS platform uses HYAS’s expert knowledge of adversary infrastructure and superior threat intelligence to constantly analyze and evaluate the likelihood that a given domain is malicious, even ones that haven’t yet been used in an attack.

If an attack of some kind does make it through a network’s defense perimeter, HYAS Protect can help detect the command and control (C2) traffic used by the malware and block it. Nearly all forms of malware use DNS at some point in their attack, so cutting off its ability to communicate with its command and control renders it effectively inert.

“My day starts with pulling up the HYAS Protect page and looking at what the traffic has been, looking at yesterday’s traffic to see if there have been trends, look at what we’ve been blocking, and elevate anything if I need to,” said Isaac Spencer, IT Manager at Portland Leather Goods.

## THE VALUE OF VISIBILITY

HYAS Protect integrated easily into the organization’s security stack, and the security team at Portland Leather Goods immediately gained access to a whole new level of visibility into their network. Not only can they monitor and block potential malicious domains via HYAS Protect’s easy-to-use interface, the platform also provides insight into legitimate network traffic. The discovery of certain employee traffic habits, for example, led to the implementation of new company policies, which both hardened their security posture and increased overall productivity.

**“HYAS has increased our overall productivity for both our company and our security team. We have been very happy partnering with HYAS.”**

ISAAC SPENCER

IT MANAGER, PORTLAND LEATHER GOODS

At HYAS, we understand the unique challenges small and medium sized businesses face. Our platform is easy to use and manage, can operate on its own (i.e., “set it and forget it”), and integrates with any existing security stack, making it ideal for smaller security teams who need to do more with less.

## CONTACT US FOR A DEMO

[sales@hyas.com](mailto: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.