HYAS

HYAS **CASE STUDY**

COMPANY AT A GLANCE

SentinelOne™

SentinelOne is the leading cybersecurity solution encompassing AI-powered prevention, detection, response and hunting across endpoints, containers, cloud workloads, and IoT devices in a single autonomous platform. SentinelOne has over 1,000 employees around the globe with major offices in the USA, Israel, the Netherlands, the Czech Republic and Japan.

CHALLENGES

- Identifying potential gaps in existing defensive layers
- Improving security hygiene

RESULTS

- Improved security operations through rapid identification and remediation of unprotected endpoints
- Risk reduction by identification of potential security blind spots
- Improved security detection and prevention capabilities by integrating Protective DNS with existing security infrastructure

SENTINELONE DEPLOYS HYAS PROTECT FOR PROACTIVE SECURITY AND CONTROL IN AN EVER-CHANGING ENVIRONMENT

CYBERSECURITY LEADER IMPROVES SECURITY HYGIENE AND LOCATES GAPS WITH PROTECTIVE DNS FROM HYAS

Protecting Cybersecurity Innovation with Defense in Depth

SentinelOne delivers leading cybersecurity solutions for enterprises around the world. Its autonomous endpoint protection prevents, detects, and responds to attacks across all major vectors. Innovating and delivering an industry-leading security solution requires a security strategy to protect the company, inspire customer confidence, and fulfill compliance requirements to enable the business. The SentinelOne security team fulfills compliance mandates including ISO 27001, SOC2 Type II, Sarbanes-Oxley, and FedRamp.

SentinelOne employees work in the office as well as remotely. Security for the entire infrastructure is monitored using Vigilance, SentinelOne's managed detection and response (MDR) solution in concert with the SentinelOne security operations team.

"We believe in security in depth and security layers. HYAS Protect can block potential threats at the DNS layer, and we also correlate the alerts with other telemetry we are ingesting. Any time we encounter an alert or an interesting domain from HYAS Protect that we haven't seen before, we are able to compare against other existing telemetry. Combining HYAS Protect with other data allows us to identify security holes that we can plug."

> **HYAS Protect has helped us to reinforce our policy guardrails. We have policies and procedures in place to maintain security hygiene, but HYAS Protect helps us monitor and investigate risk. Alerting from HYAS Protect gives us another layer of visibility to ensure we react quickly.**

CHRIS BATES
Chief Information Security Officer, SentinelOne

Improving Security with Protective DNS

SentinelOne had been using a public DNS service to resolve DNS queries and wanted to get the security value by adding a Protective DNS service to its technology stack. Explained Bates, "DNS is one of the aggregating functions within your environment that provides a great chokepoint. HYAS Protect monitors that chokepoint to find things that other tools might have missed."

After identifying the need to monitor DNS traffic, the SentinelOne team researched the space and arrived at the leading options: Cisco Umbrella and HYAS Protect. Upon comparing the features and quality of the results that both solutions generated, SentinelOne decided to go with HYAS Protect. Commenting on the decision, Bates said, "We chose HYAS because the results it provided were good, we liked the HYAS focus on adversary infrastructure and how it mines and grabs intelligence, we liked the POC experience. Using the HYAS Protect API has been very helpful. There is room for this partnership to grow in the future."

Good Security Decisions: Quality Data & Context

Making good security decisions requires a combination of good data and establishing context for the security team. Bates observed, "Everyone has data. It is about context. You need good quality data, but also applying data in a meaningful context. We take the high-quality data that comes from HYAS Protect and enrich the data that comes from SentinelOne. Together with our proprietary technology and HYAS Protect, I get the depth, breadth, and context from my data. My team can take a look and understand if it is something we expect or don't expect. The added intelligence around the DNS enhances the context already in SentinelOne allowing for quicker decisions to be made."

HYAS Protect is deployed in Protection Mode at SentinelOne to act as the DNS resolver to block malicious domains and IPs. HYAS Protect alerts are used by the SentinelOne security team to identify security issues and potential gaps in coverage. Explained Bates, "HYAS provides an indicator of a potential issue. It shows me something that I need to go investigate. It may be something that gets raised to a critical level or something that is modest."

Smooth HYAS Protect Deployment Integrates with Security Infrastructure

HYAS Protect has been employed as the primary DNS resolver for about half a year with alerts being sent into SentinelOne's security information and event management (SIEM) system. The scalability and reliability provided by HYAS Protect have matched SentinelOne's rigorous requirements. In commenting on the deployment, Bates shared, "The deployment was easy. All you do is go into all of your DNS servers and point all external traffic at HYAS Protect as the primary resolver and move our previous public DNS service to be the secondary. We've never had an issue with HYAS so we have never used the secondary."

In describing the assistance provided by HYAS to ensure SentinelOne's success, Bates commented, "It has been a great relationship with the HYAS team. They have been responsive and collaborative from a smooth POC to the production roll-out."

Reducing Risk & Improving Security Operations

HYAS Protect is integrated with SentinelOne's existing processes and administering HYAS Protect has required minimal resourcing from the SentinelOne security team. Observed Bates, "Our security operations are automated, and HYAS Protect fits well into our existing processes. If there is an alert within HYAS Protect, it sends the information to our SIEM, and then APIs pull the information into SentinelOne, and we use APIs to update the HYAS Protect Allow list. There is little to no maintenance or administrative overhead with HYAS Protect."

Deploying HYAS Protect has enabled SentinelOne to improve security operations. Explained Bates, "We use [HYAS Protect] for additional intelligence to identify something abnormal that may be going on, but we also use it to also go back and validate that we have visibility everywhere. We compare HYAS Protect alerts against our other tooling to identify potential compromises and holes in coverage."

> **"HYAS Protect provides an important additional layer for our defense in depth strategy. It helps us to identify where people are doing things they should not be doing, both for our end-users as well as the engineering environment."**

Deploying a Protective DNS solution has helped this security leader sharpen its security posture. Commented Bates, "HYAS Protect provides an important additional layer for our defense in depth strategy. It helps us to identify where people are doing things they should not be doing, both for our end-users as well as the engineering environment."

CONTACT US FOR A DEMO

confidence@hyas.com

INVESTIGATE ATTACK INFRASTRUCTURE FURTHER
AND IDENTIFY FRAUD FASTER

HYAS INSIGHT

An efficient and expedient investigation is the best way to protect your enterprise. HYAS Insight provides threat and fraud response teams with unparalleled visibility into everything you need to know about the attack. This includes the origin, current infrastructure being used and any infrastructure likely to be used in future attacks.

HYAS

WE'RE NOT HERE TO PLAY CAT AND MOUSE
WE'RE OUT TO CHANGE THE GAME

HYAS is a valued partner and world-leading authority on cyber adversary infrastructure and communication to that infrastructure. We help businesses see more, do more, and understand more about the nature of the threats they face, or don't even realize they are facing, on a daily basis. Our vision is to be the leading provider of confidence and cybersecurity that today's businesses need to move forward in an ever-changing data environment.