

American Hotel Company

INDUSTRY

Hospitality

NUMBER OF ENDPOINTS

9,200

USE CASE

A major American hotel company looked to replace their existing on-premises security platform with a SaaS solution for endpoint protection and threat intelligence.

THE CHALLENGE

- » A Lack of a SaaS security solution made it difficult to gain full visibility across more than 9,000 hotels and resorts.
- » The Advanced Threat Team spent all their time manually processing threat intelligence and applying fixes to their security stack.
- » The company split into two separate business entities, leaving only half the security team to cover the same number of locations.

THE SOLUTION

- » Cybereason provided a cloud-based solution for unified protection across all the company's endpoints and attack surfaces.
- » Cybereason MDR supported the internal security team with a full team of security experts to detect and remediate threats and free up time for the company's threat team.
- » Cybereason provided full visibility into endpoints with advanced prevention and endpoint controls as well as rapid detection and response.
- » Cybereason enabled the company's security team to leverage custom detection rules and define new logic for triggering MalOps™ (malicious operations).

CYBEREASON SUPPORTS THREAT INTELLIGENCE FOR A GLOBAL HOTEL FRANCHISE

One of the largest hotel franchising companies in the world manages more than 20 hotel brands, 15,000 employees, and 9,000 locations across 80 companies. For the global hospitality brand, protecting their customers and infrastructure against cybercriminals and state-sponsored threat actors was a primary concern.

When the company split its hotel and vacation ownership businesses into two separate companies, the hotel company took the opportunity to reevaluate its current security solution. They looked for a cloud-based security platform to support their locations all over the world. They also planned to improve threat intelligence and automate manual processes.

The hotel franchise chose Cybereason. After comparing multiple solutions, Cybereason met the company's needs and fit the direction their security team was heading.

"Cybereason had a view around how cyber operations act and how to defend against them," said the Manager of the Advanced Threat Team. "Our philosophy around defense, resilience, hunting, and instant response just meshes so well with Cybereason's vision."

THE CHALLENGE

Before switching to Cybereason, the company used a disconnected, non-SaaS tool. This left their threat team to manually analyze new threat intel and build it into their defensive stack. Using up resources on manual tasks did not allow the company's threat detection and response to grow and improve.

As a global brand with more than 9,000 endpoints, visibility and asset management were significant challenges. Without a SaaS solution, their team needed to be on-premises to gain visibility into specific servers. This made it difficult to have a full understanding of what was built on each server, where it came from, who updates it, and whether or not it is still supported.

In 2018, the brand split into two separate business entities. The new hotel and resort company was left with half of its existing cybersecurity

personnel. This increased the problems of manual threat intelligence and asset management, but it also presented an opportunity to reevaluate their security stack.

"One of the decisions we made was to replace our current product with something that was more cloud-focused. Our incumbent product required you to be on-prem or required you to be on VPN," said the company's Senior Director of Threat and Vulnerability. "We needed a product that would fit our disconnected model where not every hotel needs to come back on a wire to our data centers."

THE SOLUTION

The company performed a 30-day proof of concept with four different vendors - Cybereason, CrowdStrike, SentinelOne, and RSA Security. They used an internally developed scorecard to evaluate the various aspects most important to their security needs, including dashboarding, GUI, reporting, threat detection, and performance in penetration testing.

"What we noticed with Cybereason was that it popped. It fired right away," said the company's Senior Director of Threat and Vulnerability. "It told us exactly what it found, behavioral detection. Sometimes it even identified the malware family right away, which was cool."

The company initially deployed Cybereason EDR to gain better visibility, detection, and response at their endpoints. This provided contextualized and correlated insights from the MalOptm detection engine. After a short period of time, they turned on the full Cybereason for unified protection across their endpoints and extended attack surfaces as well as security operations optimization and incident management.

The threat hunting capabilities of Cybereason enabled their security team to leverage custom detection rules and define new logic for triggering MalOps. This has helped their team mature and evolve into a full-time threat intelligence organization. Cybereason's streamlined GUI also enabled the advanced threat team to mature their SOC organization and get that team involved in more advanced threat techniques without requiring prior technical knowledge.

The hotel company's internal security team is also supported by Cybereason Managed Detection and Response (MDR). Managed detection and response provides a global SOC team of security experts to help improve the company's security posture and streamline operations.

THE OUTCOME

"Cybereason MDR definitely allows me to sleep better at night," said the company's Senior Director of Threat and Vulnerability. "I don't have to worry



"Cybereason's performance in pen testing was what won us over compared to other products. The technology was great. In the end, this was the right product for us."

SENIOR DIRECTOR OF THREAT AND VULNERABILITY

Hospitality Industry



about every single thing that may fire in the organization overnight. I know I have that 24/7, eyes on glass kind of coverage."

Moving to a SaaS platform provides advanced prevention and endpoint controls across their 9,000 locations without requiring on-site access. They gained full visibility to automatically uncover attacks, gained a full understanding of advanced threats, and can now execute prevention and remediation automatically.

"From a proactive standpoint, it does a lot of heavy lifting for us. Going to a platform like Cybereason where you guys have threat hunting and threat intelligence built-in on the back end has helped automate a lot of that hunt," the Senior Director of Threat and Vulnerability said.

Due to the ease of deployment and efficient resource usage, the Threat and Vulnerability team gained buy-in and support from their CISO. Being able to upskill members of the SOC has allowed the company to direct funds to other areas. The top priority for the company's Advanced Threat Manager was to increase threat intel and Cybereason's ability to reduce the time needed for manual threat hunting allowed the company to focus more effort on this initiative.



