# BISINGS SEVICES

- INDUSTRY **Business Services**
- NUMBER OF ENDPOINTS 1,600
- THE CHALLENGE This mid-sized international company needed to improve its security maturity and was uncertain how to start with an Al-based platform. Organizational gaps in personnel and skillsets prevented full compliance, remote work security, and protection against ransomware. Other solutions on the market were too expensive or difficult to learn.

### THE SOLUTION

A Cybereason package with EDR and MDR solutions filled their organizational gaps, simplified alerts, provided greater threat context, and addressed the issues of compliance, remote work security, and ransomware prevention.

### INTRODUCTION

This international business services provider employs 400 employees and manages more than 1,600 endpoints. As their business grew across several major industries, they realized it was time to strengthen their current posture with a best-in-class managed detection and response platform.

Previously relying on home-brewed solutions, the company investigated several other vendors before making their final selection. In their own words, they had "a long list of criteria that an EDR solution should meet," and they evaluated each subsequent competitor with those requirements in mind.

In the end, they made the decision to deploy the Cybereason platform.

"The MDR package was an important component since we desired a strong team who could 'have our six' if we got too far over our heads," the company's Cyber Security Analyst said.

## THE CHALLENGE

Because their organization was admittedly 'small and relatively new to the SOC/ EDR world', they decided to start simply.

"We had to pick a few priorities and start there, so we didn't have the immediate budget to hire crucial people like pen testers or engineers," the company's analyst said. "We had some help from the network company we started with, but our organizational gaps still created uncertainty in our future."

Those organizational gaps created uncertainty in their security posture, as well. The company lacked visibility into the processes running on most of their endpoints and to cover the load, they had been forced to "use one solution in as many places as possible." On the hunt for a better way, they found other platforms either too modular, too expensive, or too difficult for new SOC analysts to use.

Until they found Cybereason.







We had several 'weighted' criteria on our list, and we found that Cybereason offered a strong, proactive security solution.



Cybereason offers more visibility, automation, and prevention than other EDR tools.

**BUSINESS SERVICES INDUSTRY** 

# **SOLUTION**

- Combines advanced prevention and endpoint controls with rapid detection to leverage deep contextual correlations across all endpoints in real time.
- While the runners-up were described as 'close contenders', they ultimately chose Cybereason "because of affordability, usability, and capability." They also wanted a company that could have their back in the event that a threat scenario proved overwhelming, too complex, or indecipherable.
- It also addressed several of their growing concerns: Endpoint protection, remote workers, and ransomware.

# THE OUTCOME

The results were already being felt several months into the Cybereason MDR deployment. "The Cybereason platform has proven itself capable already," stated one of the company's SOC analysts.

"Cybereason has helped the analysts look into and across endpoints to see what's happening - good and bad," the analyst said. "Visibility and prevention have been two of Cybereason's strongest suits."

Using Cybereason EDR to monitor what happened at each endpoint, they could secure all access points into the network, including remote workers.

Another big win was helping the company stay compliant in the face of government and private sector data regulations. "The Cybereason platform helps meet regulatory compliance and does the job we need it to. Furthermore, it helps us do the jobs we need to," the Cyber Security Analyst said.

The company reports that incident investigations have become more responsive by simplifying alerts and investigations. "We are seeing more relevant alerts since Cybereason tells a concise story."

### **ABOUT CYBEREASON**

Cybereason is the XDR company, partnering with Defenders to end attacks at the endpoint, in the cloud and across the entire enterprise ecosystem. Only the Cybereason Al-Driven XDR Platform provides predictive prevention, detection and response that is undefeated against modern ransomware and advanced attack techniques. The Cybereason MalOptm instantly delivers context-rich attack intelligence across every affected device, user, and system with unparalleled speed and accuracy. Cybereason turns threat data into actionable decisions at the speed of business. Cybereason is a privately held international company headquartered in Boston with customers in more than 40 countries.

