CASE STUDY

COMPROMISE ASSESSMENT

PAYMENT CARD INDUSTRY

CARBON BLACK

FORESITE
VISIONARY SECURITY & COMPLIANCE SERVICES

Business Challenges

- Past incidents left them concerned that there could be residual malware
- Lack of 24/7 monitoring to be alerted
- Internal staff not formally trained

Opportunities

- Determine current state and provide actionable intelligence for next steps
- Provide a road map to optimal state in manageable stages

Foresite Solutions

- Compromise Assessment

BACKGROUND

A retail chain was aware that they had experienced a few minor cybersecurity incidents and wanted to be sure that they had fully remediated. The CISO was new to the organization as well, so having an firm report on current state would be helpful to him as he reviewed pending projects to decide where to invest first.

OUR **OBJECTIVES**

☐ Confirm remediation from past cyber incidents

☐ Look for signs of compromise to address before they become a reportable breach

☐ Provide recommendations for improvements based on our findings

☐ Leverage Carbon Black tool used in assessment as Proof of Concept for endpoint security

OUR **SOLUTION**

☐ Compromise Assessment to proactively gather logs over a period of time from key devices - firewalls, IDS/IPS, servers, and endpoints