1 Executive Summary

1.1 Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is a global set of security standards defined by the Payment Card Data Security Council to protect payment card data against evolving cybersecurity threats. Any organization that stores, processes, or transmits payment cards online, from small start-ups to large global enterprises, must adhere to each requirement outlined in PCI DSS to remain compliant and avoid penalties. Released in March of 2022, version 4.0 of PCI DSS introduces several new security requirements, including the need for organizations to actively manage and protect against JavaScript threats on the client side. IT managers, security teams, and internal auditors can benefit from the use of Akamai Client-Side Protection & Compliance to accelerate compliance with version 4.0 of the Payment Card Industry Data Security Standard (PCI DSS) by providing the auditor with comprehensive real-time and historical visibility of JavaScript execution behaviors, assisting security teams in detecting and mitigating client-side data breaches, as well as addressing two critical JavaScript security requirements with one solution.

Meeting all the requirements outlined in PCI-DSS v4.0 and achieving certification puts a significant burden on organizations.

1.2 Background

Akamai provides a platform for cloud computing, security, and content delivery. In 2023, Akamai contacted GRSee Consulting Ltd. requesting an assessment and documentation of the security status of a core web application security product, Akamai Client-Side Protection & Compliance, as it compares to PCI -DSS v4.0. The GRSee Consulting QSA has examined Akamai Client-Side Protection & Compliance (CPC), mapping to PCI DSS v4.0 for assessment.