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. IT managers and internal auditors can benefit from the use of Akamai Guardicore Segmentation to accelerate compliance with version 4.0 of the Payment Card Industry Data Security Standard (PCI DSS) by providing the auditor with a comprehensive, real-time and historical map showing IT environments in scope along with segmentation that isolates the cardholder data environment (CDE) from the rest of the network and unrelated systems, disallowing out-of-scope systems from interacting with the assets in the CDE.

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

1.1.1 Diverse and dynamic environments

The difficulty: Applications and network environments that are included in the PCI scope are usually quite complex, spanning multiple machines and in many cases across different infrastructure types, technologies, and even physical locations. Therefore, the visibility of their network is very important.

In some cases, the applications include tiers that are auto-scaling to support load spikes and are constantly changing to provide more services and innovation to the customers.

This introduces several major challenges from the PCI-DSS perspective:

1. Scoping: understanding, at any given time, where the workloads are located within the CDE, and which workloads are out-of-scope, giving one an up-to-date picture of the network.
2. Placing controls within the diverse and dynamic environment: PCI DSS requires controls across the CDE. Even placing a FW (as mandated by the first requirement) can be a difficult problem as placing firewalls between two containers, or two VMs, on the same Hypervisor, may require an entirely different set of technologies and APIs.

How can Akamai Guardicore Segmentation help: Corresponds to the One of the key features of Akamai Guardicore Segmentation is the Reveal map, as visibility is crucial at may stages of the compliance process, starting from scoping the CDE and understanding its dynamic boundaries. The Reveal map is helpful in the process of meeting and expediting many of the requirements. Additionally the flexible policy engine, Insight and the Hunt service aids in protecting the CDE and staying in a compliant state.