illumio

SOLUTION BRIEF

# PCI Segmentation TCO: Hardware Firewalls vs. Illumio Core

## Challenges in PCI Scoping and Segmentation

PCI DSS compliance does not require segmentation. However, segmentation of east-west traffic can be an effective tool for reducing the scope of PCI audits. The Payment Card Industry Security Standards Council (PCI SSC) published the "Guidance for PCI DSS Scoping and Network Segmentation" information supplement to help PCI-covered entities enhance the accuracy and efficacy of their PCI segmentation architecture (Figure 1). In reality, many PCI-covered entities struggle to execute these recommendations because:

- The payment ecosystems and data center environments that support these processes are more complex, heterogeneous, distributed, and dynamic. Entities are unable to keep track of the legitimate connections to PCI-connected systems and security-impacting systems, leading them to keep more ports and connections open than they need to.
- Attack tactics and techniques of malicious actors continue to evolve, but prevention and perimeter security solutions are unable to keep up with these advanced and targeted attacks.

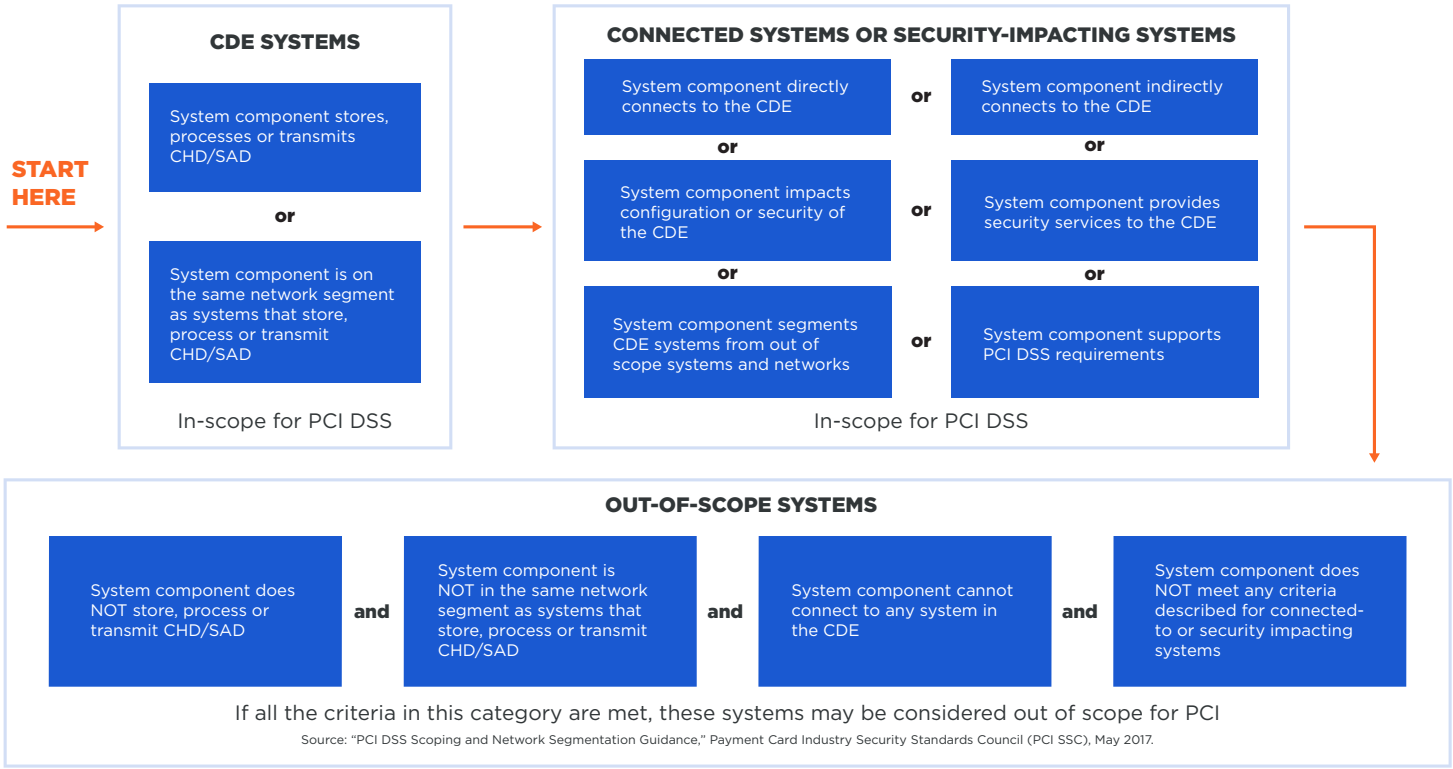



Figure 1: PCI DSS Scoping & Segmentation Guide

## Using Data Center Firewalls to Segment East-West Traffic a Bad Idea

Customers have tried using VLANs and firewalls to segment their complex east-west PCI traffic. These entities report the following hurdles:

- Visibility and Accuracy. How do you validate that your data flow and network flow diagrams are accurate? How do you maintain an accurate inventory of the Cardholder Data Environment (CDE), and PCI-connected system and security-impacting system components? How do you document and defend to your QSA that your PCI scope is accurate?

- Efficacy of Segmentation Architecture. How do you prove to your QSA that your segmentation architecture is effective and accurate? How do you effectively scope and segment your PCI environment so that you avoid major segmentation errors? How do you ensure that your segmentation solution will scale with the environment and support the deployment of new technologies?
- Firewall Management Complexity. How do you keep track of the applicable firewall rules so that you do not fail your annual or bi-annual PCI segmentation pen test? How do you reduce the time to create or change the applicable firewall rules in response to changes in the PCI environment? How do you keep the firewall rules up to date in highly dynamic, abstracted, and multi-cloud environments?
- Total Cost of Ownership. How do you avoid the overheads associated with deploying more data center firewalls and VLANs?

## PCI Segmentation: Comparing the TCO of Hardware Firewalls vs. Illumio Core

### Customer Challenge

PCI DSS requires covered entities to maintain 100% compliance continuously. A global acquiring bank's ("Acquiring Bank") fraud management team flagged a global online entertainment and media retailer ("Retailer") as a common fraud target. As a result, Retailer found itself subject to more aggressive PCI audits. Retailer's QSA found that their network was too flat and issued a failed ROC (Report on Compliance). The QSA reported the following audit findings:

- Reported inventory of applications and systems that comprise the CDE, PCI-connected systems and security-impacting systems was not accurate.
- Out-of-scope system components were not effectively segmented from the PCI environment. Pen testers were able to compromise a PCI-connected system component and use this to access and breach Retailer's CDE.

Retailer was required to notify Acquiring Bank about the failed ROC and also come up with a solution and timeline for recovery. Acquiring Bank gave Retailer a very short window (3 months) to address these issues. Acquiring Bank also informed Retailer that if it fails to remediate these issues, it will denylist Retailer and refuse to process future payment transactions.

### Retailer's Data Center Environment and Security Program

The following attributes describe Retailer's payment infrastructure and data center environment (Figure 2):

- 3 regional data centers (one for HA/DR)
- 16,000 workloads (including 2000 physical servers)
- Workloads running on a mix of Windows, Linux, VMware servers, and AIX operating systems
- 30 hardware firewalls (a combination of Fortinet FG and Palo Alto Networks PA-5280)
- Approximately 12 PCI applications (based on out-of-date data flow maps and network topology documents)
- Unknown number of PCI-connected servers and PCI security-impacting servers
- Out-of-date physical and logical PCI network diagrams
- Out-of-date data flow maps
- An MS Excel file holding data about its VLANs, subnets, switches, firewalls, and IP addresses (from another IT project)
- An MS Excel file that maintains a list of its third-party PCI ecosystem, including connections to Acquiring Bank, an online content management platform, and online member loyalty program
- An out-of-date CMDB

Retailer had acquired two online properties in the last five years and it never got around to standardizing its security and PCI compliance practices.

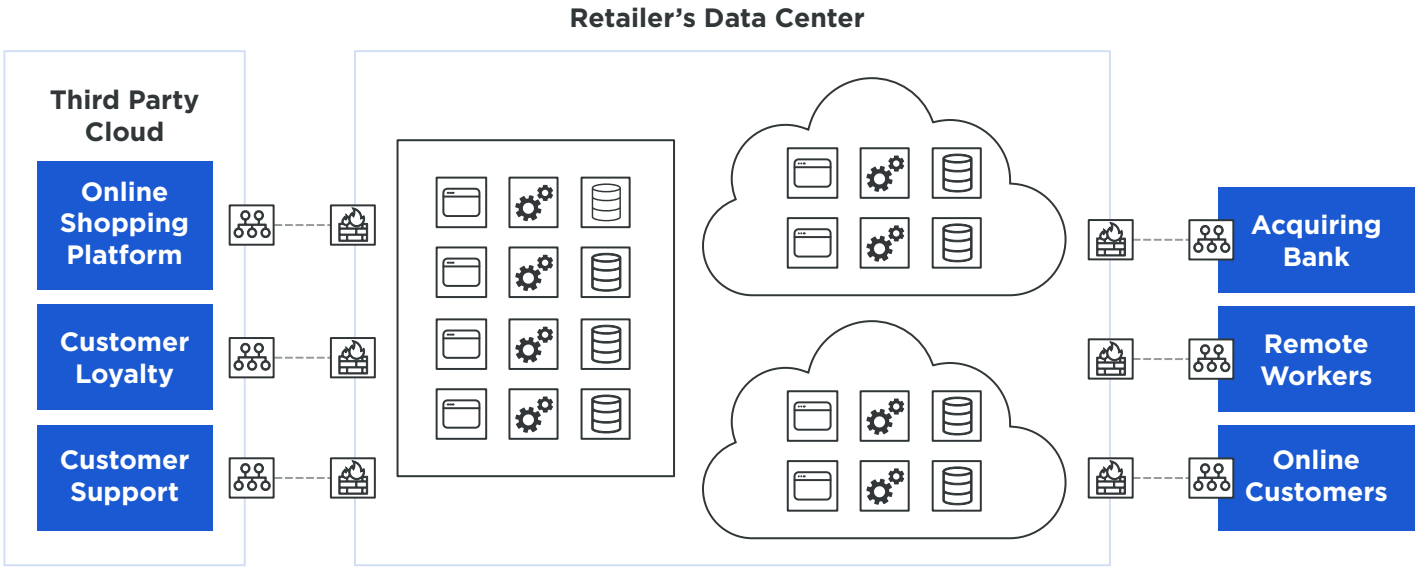



Figure 2: Retailer's Payment Infrastructure

## Retailer's Failed ROC Recovery Goals

Retailer had the following goals as part of its Failed ROC Recovery Plan:

- Verify the number of applications and components that make up its cardholder data environment (CDE).
- Maintain an accurate inventory of its PCI program scope.
- Identify and inventory its PCI-connected and security-impacting systems.
- Segment the PCI environment from the out-of-scope applications and workloads.
- Standardize its security processes and PCI program.

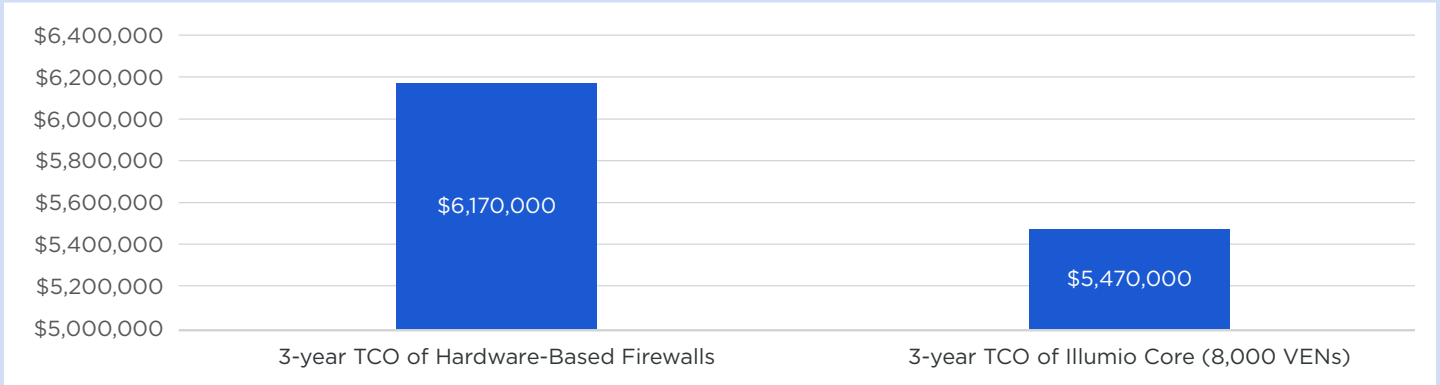
## Failed ROC Recovery Activities

### 1. Initial Assessment

Retailer started with the assumption that all of its 16,000 workloads were in-scope for PCI. It reviewed the database that contained data about the VLANs, subnets, security zones, firewalls, and IP addresses and crossreferenced this data with its existing data maps, network topology diagrams, and CMDB to initially re-scope its PCI environment. The initial assessment concluded that deploying an additional 100 hardware firewalls across its three data centers would reduce the total number of in-scope PCI systems by 50% to 8,000 workloads.

**Initial TCO Calculation:** Retailer's security and IT infrastructure team used information from the initial assessment to calculate and compare the TCO from using Fortinet Fortigate (FG) vs. Illumio Core (Figure 3).

INITIAL TCO CALCULATION




| | Hardware-Based Firewall | Illumio Core |
|---|---|---|
| In-scope workloads (initial assessment) | 8,000 | 8,000 |
| Number of physical servers | 1,000 | 1,000 |
| Workloads per VM | 8 | 8 |
| Number of HW Firewalls | 100 | NA |
| Number of VENS required | NA | 8,000 |
| Number of in-scope PCI Systems | 12 | 12 |
| | **Savings with Illumio Core** | **$700k** |
| | **% Savings with Illumio Core** | **13%** |

Figure 3: Hardward-Based Firewall Solution vs. Illumio Core (Initial Scope)
Source: Illumio Internal TCO Analysis, August 2019

## TCO Analysis Assumptions

It is common knowledge that hardware firewalls are much more complex, will require re-architecting of the existing network, and are more time-consuming and costly to deploy. To simplify the TCO analysis for this document:

1. The following considerations were excluded in the TCO calculator:
   - Cost to deploy hardware firewalls (FTE and other resources)
   - Cost to configure hardware firewalls (FTE and other resources)
   - Cost to re-architect the network
2. The following factors and assumptions were included in the analysis:
   - Assume a pair of firewalls per rack
   - Cost of firewall per rack included hardware, software, support and maintenance
   - Cost of implementing security change per application change (FTE)
   - Cost of initial Illumio Core implementation
   - Cost of installing and operating the PCE

## 2. Phased Implementation and Deployment of Illumio Core

Retailer's initial analysis lead them to select Illumio Core. Retailer initially purchased 2,000 VENs and deployed these among its top five payment applications. Illumio Core collected telemetry information for a month which enabled Retailer to address the following priorities:

- Validate and update its inventory of CDE components.
- Identify and inventory their PCI-connected systems and security-impacting systems.
- Validate and update the inventory of out-of-scope systems.
- Identify and monitor the legitimate connections and flows within the CDE.
- Identify and monitor the legitimate connections and flows between the CDE and PCI-connected and security-impacting systems.
- Inventory existing firewall rules.
- Identify firewall rules that are out-of-date, misconfigured, and non-existent.
- Validate and update the PCI network and data flow diagrams.

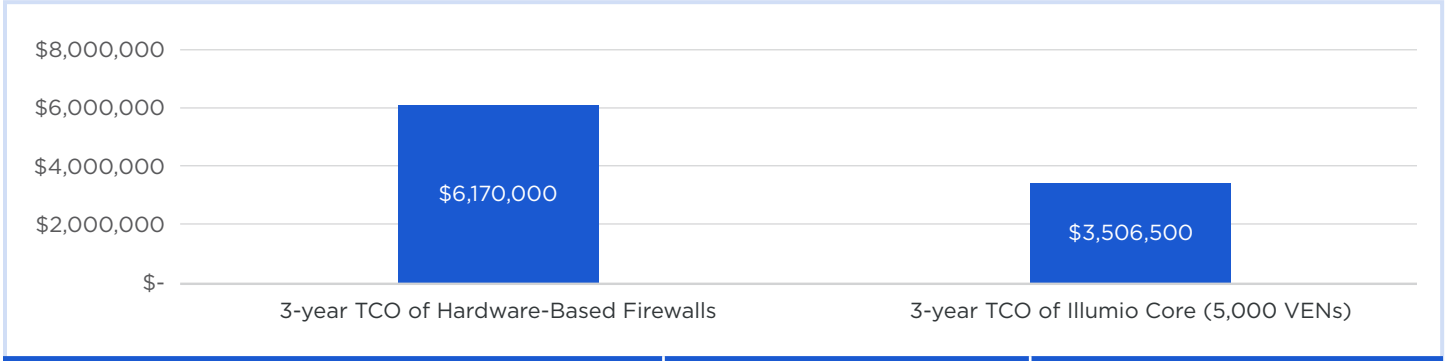
### The Value of the Application Dependency Map

Illumio Core collected telemetry information about the workload connections and flows for 30 days. Illumio Core used this historical traffic information to create Retailer's real-time application dependency map. The visibility offered by the application dependency map lead to the following findings:

- Instead of 12, Retailer had 10 applications that were considered as CDE system components.
- Instead of 8,000 workloads, the total number of workloads that were considered in-scope for PCI was 5,000.
- Instead of the original 8,000 VENS, Retailer only needed to purchase and deploy 5,000 VENs to secure its PCI environment.
- Undisclosed number of misconfigured and out-of-date firewall rules.

Estimated cost for securing 5,000 workloads with Illumio Core including annual support was $3.506 million (Figure 4), which resulted in an additional $1.96 million in savings for Retailer.

FINAL 3-YEAR COST COMPARISON (POST-ILLUMINATION)




| | Hardware-Based Firewall | Illumio Core (5,000 VENS) |
|---|---|---|
| In-scope workloads (initial) | 8,000 | 8,000 |
| In-scope workloads (post-Illumination) | NA | 5,000 |
| Reduction in in-scope workloads | NA | 3,000 |
| Number of physical servers (in-scope for PCI) | 1,000 | 625 |
| Workloads per VM | 8 | 8 |
| Number of HW Firewalls | 100 | NA |
| Number of VENS purchased | NA | 5,000 |
| Number of in-scope PCI Systems | 12 | 10 |
| | **Savings with Illumio Core** | **$2,664,000** |
| | **% Savings** | **76%** |

Figure 4: Hardward-Based Firewall Solution vs. Illumio Core (with application dependency map, Illumination)
Source: Illumio TCO Internal Analysis, August 2019

In addition, the application dependency map also pointed to critical gaps in its security controls. For example, the map revealed that Retailer needed to tightly control connections with its authorized third-party cloud-based partners, specifically the customer loyalty program and support portals. The assessment showed that malicious hackers could potentially use a compromised partner's systems as attack pathways to breach Retailer's CDE.

## Final 3-Year TCO Calculation: Hardware-Based Firewalls vs. Illumio Core

The visibility provided by the application dependency map enabled Retailer to update their TCO calculations, and confidently reduce the total number of in-scope PCI workloads from 8,000 to 5,000 resulting in additional savings.

| | **Inaccurate Scope with Hardware-Based Firewalls** | **Right-Scope Secure with Illumio Core** |
|---|---|---|
| **Description** | **Initial count of in-scope PCI workloads, before Illumination** | **Final count of in-scope PCI workloads, after Illumio application dependency map** |
| Number of in-scope PCI workloads | 8,000 | 5,000 |
| Number of hardware firewalls purchased | 100 | NA |
| 3-year TCO | $6.17 million | $3.506 million |
| Savings in total number of VENs purchased | | 3,000 |
| TCO Savings with Illumio | | $2.664 million |
| % TCO Savings with Illumio | | 76% |
| **Key Benefits** | **Inaccurate Scope with Hardware-Based Firewalls** | **Right-Scope** |
| Visibility & Real-time Application Dependency Map | NO | YES |
| Rearchitect networking architecture | YES | NO |
| Complex firewall rules management | YES | NO |

*Note: Hardware-based firewall TCO is dependent on the vendor. Retailer evaluated the least expensive next-gen firewall in its class (Fortinet FG) as an option, which had a reported MSRP of $50K.

## Summary of Benefits

In addition to the TCO savings, Illumio Core offered the following benefits to Retailer:

- Reduce PCI audit burden by improving the accuracy of its PCI scope and the efficacy of its segmentation architecture.
- Avoid PCI segmentation errors by keeping up with changes in the environment and maintaining an accurate inventory of its in-scope PCI systems.
- Mitigate risks from lateral movement attacks arising from outdated and misconfigured firewall rules.
- Eliminate outdated and misconfigured firewall rules.
- Avoid the management and administrative overheads and adverse service impact associated with deploying a significant volume of firewalls inside its data centers.
- Recalculate and enforce the applicable firewall rules in response to changes in the workload environment, without any downtime and without accidentally breaking production applications.

### Learn more:

- Visit illumio.com/solutions/pci-compliance.
- Read the white paper, Supporting PCI DSS Requirements: An Illumio/Protiviti Research Project.

Illumio enables organizations to realize a future without high-profile breaches by preventing the lateral movement of attackers across any organization. Founded on the principle of least privilege in 2013, Illumio provides visibility and segmentation for endpoints, data centers or clouds. The world's leading organizations, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com/what-we-do.

Gartner peerinsights™

See what customers have to say about Illumio.