illumio

WHITE PAPER

Three Steps to Effectively Segment Your PCI Environment

Overview

Protecting cardholder data in today's dynamic data environments has never been more difficult. PCI starts with the assumption that everything in the environment is in scope, which can be a cost-prohibitive exercise because data centers and payment infrastructures are becoming increasingly more complex.

PCI boundaries are more dynamic. The PCI Standards Council recommends that you start by identifying the CDE, the PCI connected-to, and the PCI security-impacting system components. These make up your PCI compliance program and audit scope. You can then use segmentation to isolate the PCI environment from your out-of-scope systems.

Executing the PCI council's recommendations on scoping and segmentation is not always easy for many organizations. An overly broad scope can run up the price of your audit and turn up the heat from your auditor. A mistake in scoping is even worse, inviting auditors to root through your systems, revalidate your entire architecture, and require expensive adjustments to address the problem. A narrow and accurate PCI scope is the best way to ensure a fast, painless, and inexpensive audit.

But getting scoping right requires that you understand where your cardholder data is stored and processed and are able to enforce that boundary to keep it contained. You also need to be able to keep track of PCI connected-to devices and applications that are in the same subnets or zones as non-PCI connected applications and devices. Most organizations address this challenge today through a combination of manual network analysis and network segmentation tools. Unfortunately, this approach is often expensive, slow, and prone to mistakes. Worst of all, it struggles in modern, virtualized cloud environments, forcing organizations to stick to outdated, static data center architectures for their PCI environment.

Host-based security segmentation does not rely on IP addresses and breaks the networking logjam. It allows PCI scoping and segmentation to be fast, painless, and more affordable. You don't have to maintain dedicated full-time employees to manage internal firewall change management. You don't have to buy and deploy additional networking equipment or re-architect your networking architecture. Security segmentation combines host-based intelligence and enforcement with centralized policy coordination, so you can quickly find and secure the cardholder data within your environment.

Security segmentation can help with your PCI scoping and segmentation in three steps:

1. Identify your PCI environment from out-of-scope system components.
2. Define policies and program firewalls rules that segment your PCI environment from out-of-scope systems.
3. Monitor and adapt firewall rules to maintain your PCI segmentation posture and demonstrate compliance to your auditors.

This white paper explains these steps and guides you through them, identifying the most valuable capabilities you need for each step.

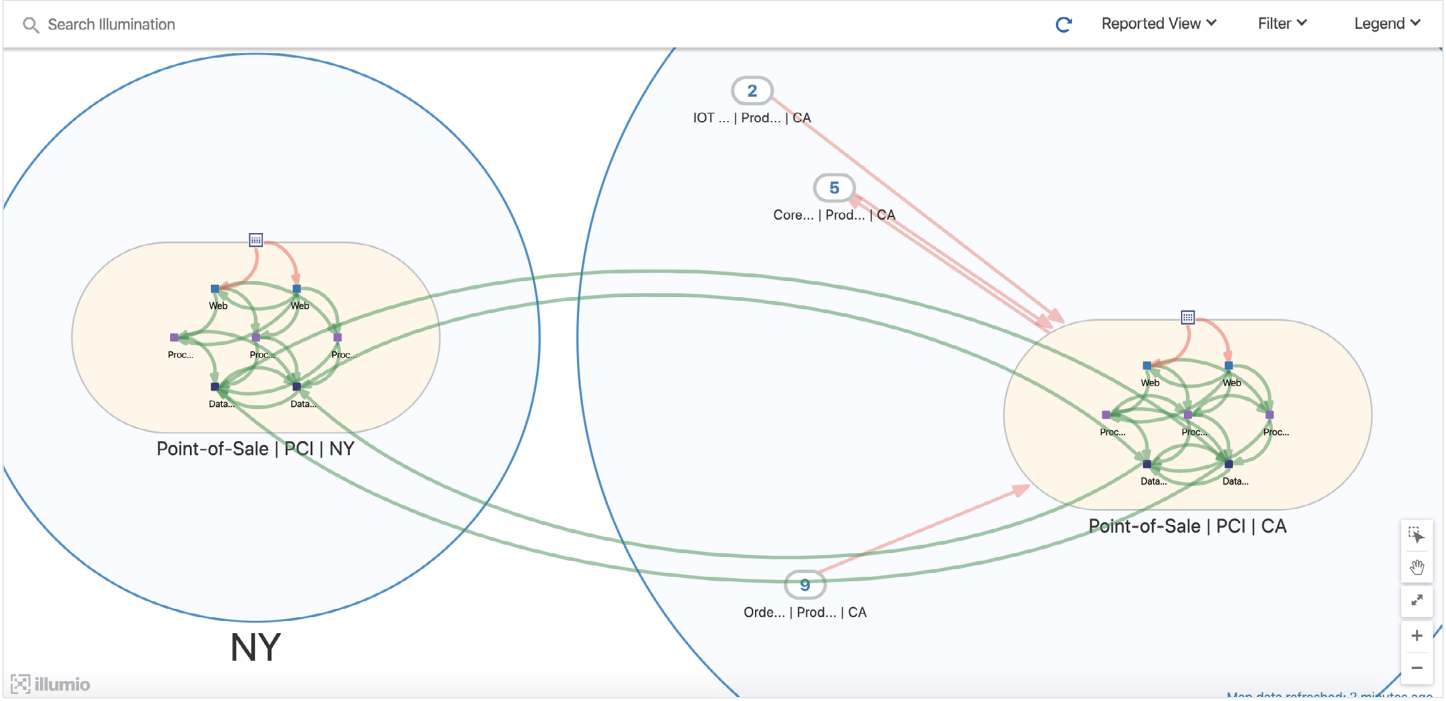
Step 1: Identify and Validate Your PCI Scope

The first step of any scoping exercise is to build a data flow diagram, which maps how cardholder data is stored, processed, and communicated and what applications and devices outside the CDE are authorized to communicate with the CDE. If non-PCI applications and devices are in the same subnets as a CDE component, you want to be able to view and validate that there are no traffic flows between these and the PCI-connected devices. Many organizations build this by starting with a network diagram, but network diagrams only reveal how your network devices communicate; they don't reveal how your applications function and share data in real time. To build the data flow diagram that PCI auditors generally seek requires extensive manual work to identify application-specific information about the cardholder data. This can be expensive and slow and requires constant manual investment to keep it up-to-date as your environment changes.

But building this diagram can be accelerated from days to hours if you have access to a real-time application dependency map —that is, a map that outlines all the ways that your applications communicate and the nature of those communications. PCI also requires that you maintain an accurate inventory of your PCI components at the beginning and end of the audit period, including what components and connections changed and were added or removed between audit periods, and the business rationale behind these changes. Your security segmentation solution should maintain this data over time. By using an application dependency map, you can build a faster, narrower, and more accurate scope for your cardholder data environment.

Benefits of Application Dependency Mapping Versus Network Diagramming

	Real-Time Application Dependency Map	Network Diagram
Accuracy	An ADM can automatically identify every system with which your PCI applications communicate. This automatic identification process is reliable, repeatable, and up-to-date, greatly reducing the risk of costly human error.	A network diagram shows you the devices connected to your systems, but not what they do. You must manually map this to your PCI functions to identify the scope of your CDE. A manual mapping exercise like this is prone to errors, making it likely that your team will miss systems and connections that should be covered and expose you to liability.
Precision	ADM's automated analysis lets you narrowly scope your PCI compliance and makes sure you don't miss systems, saving you resources and time and avoiding mistakes.	Because of the risk of inaccuracy inherent in the manual steps required when using network diagrams, you will likely err on the side of over-inclusion, scoping systems into your PCI systems where their membership is uncertain. This means you must apply PCI controls to more systems, increasing your cost and burden.
Speed	ADM's automated, real-time process speeds up PCI scoping by reducing the manual work your team must do. It speeds up the first audit and speeds up subsequent audits (when only environmental change must be tracked) even more.	Although a network diagram can serve as a useful jumping off point for a scoping exercise, it takes extensive manual effort to transform a network diagram into a data flow map and PCI scope. This effort takes time and resources and can slow down PCI compliance to a crawl.



Real-time connections across and within the PCI environment across the NY and CA data centers. Green lines indicate that traffic was detected and these connections are covered by firewall rules. Red lines indicate that traffic was detected between the PCI environment and Core Services, IoT devices, and Ordering applications, but these connections are not governed by firewall rules. Double-clicking into Core Services will reveal that these workloads are not only connected to the PCI applications but also to HR and Ordering applications. Core Services fits the definition of a PCI-connected system and is considered in scope for the PCI audit.

Step 2: Segment Your PCI Environment with Security Segmentation

Once you have identified your PCI scope, you need to enforce the boundaries that you have mapped because, according to the PCI council, out-of-scope systems must "not have access to any system in the CDE."

When most people think of enforcing their scope, they think of traditional, network-based segmentation solutions, such as ACLs. For many modern data centers and payment architectures, however, network segmentation is not sufficient. For instance, if you have cardholder data in a could environment and the public cloud application has legitimate connections to your on-premise database, you will want to ensure policies across both cloud and on-prem environments are aligned. You also want to be able to encrypt traffic across your public cloud and on-prem data center. Similarly, if you use a dynamic environment that relies on virtualization and/or containers, network segmentation is too static and manual to address your needs.

Thankfully, the PCI council has made it clear that there are a range of technologies beyond traditional VLANs and data center firewalls that can be used for PCI segmentation. Recent guidance lists several of these, from restricted user access to physical air-gapping and host-based firewalls.

Many IT organizations are moving from network segmentation to these new technologies. Security segmentation combines the benefits of these new approaches.

Key Characteristics of Security Segmentation

Flexible Granularity. Network segmentation can only enforce broad separations (for example, separating development from production). Host-based security segmentation can enforce both broad separations and extremely precise segmentation.

Hybrid Environments. Many PCI environments today stretch across multiple data centers, cloud deployments, operating systems, and hypervisors. Network segmentation works only within traditional, static data centers. Security segmentation works across static and dynamic environments, in the cloud, and on bare-metal servers and containers.

Adaptive Enforcement. The scope of modern PCI environments shifts as the systems on which they run shift. Security segmentation is able to monitor and detect for changes to the environment and in application-to-application connections, and updates the applicable firewall rules so that you are able to continuously maintain your PCI segmentation posture. You do not need to manually update your scope and firewall rules.

Application Awareness. Network segmentation does not understand the details of your applications and your communications, making it hard to secure your PCI environment. Security segmentation understands your applications, ensuring that your segmentation protects the most valuable data in your PCI environment.

	Network Segmentation	Security Segmentation
Flexible Granularity	✗	✓
Hybrid Environments	✗	✓
Adaptive Enforcement	✗	✓
Application Awareness	✗	✓

Step 3: Demonstrate Continuous Compliance of PCI Segmentation Posture to Auditors

PCI requires 100% compliance to controls at all times. You must be able to detect for changes to the environment and connections, and update the applicable firewall rules in order to maintain your PCI segmentation posture. If you are unable to patch a vulnerability, you must demonstrate that you have an effective compensating control to isolate traffic in potentially vulnerable systems.

PCI also requires periodic scope reviews, and any auditors you engage with will need to review your scope themselves. When designating your scope and considering solutions to enforce that scope, remember that achieving compliance means being able to prove compliance. You also need to prove that you have an accurate inventory of in-scope PCI systems, enforce the applicable firewall rules, detect and document changes to the applications and the PCI-connected systems, and document that the applicable firewall rules were adjusted to maintain the target PCI segmentation objectives.

Here are four characteristics to look for in any scoping and segmentation tool to ensure you are maintaining your security posture and can prove continuous compliance.

Human-Readable Policies

Scoping and segmenting any modern PCI environmnent can easily require thousands of firewall rules, and handing a list of twenty thousand firewall rules over to your auditor isn’t going to make him or her—or you—happy. Rather than relying on PCI segmentation reports that rely on IP address-based firewall rules, look for solutions that use environmental metadata to create richer and more understandable rules. These make it easier for you to explain your scope to an auditor and easier for auditors to validate it as well.

A Picture is Worth a Thousand Words

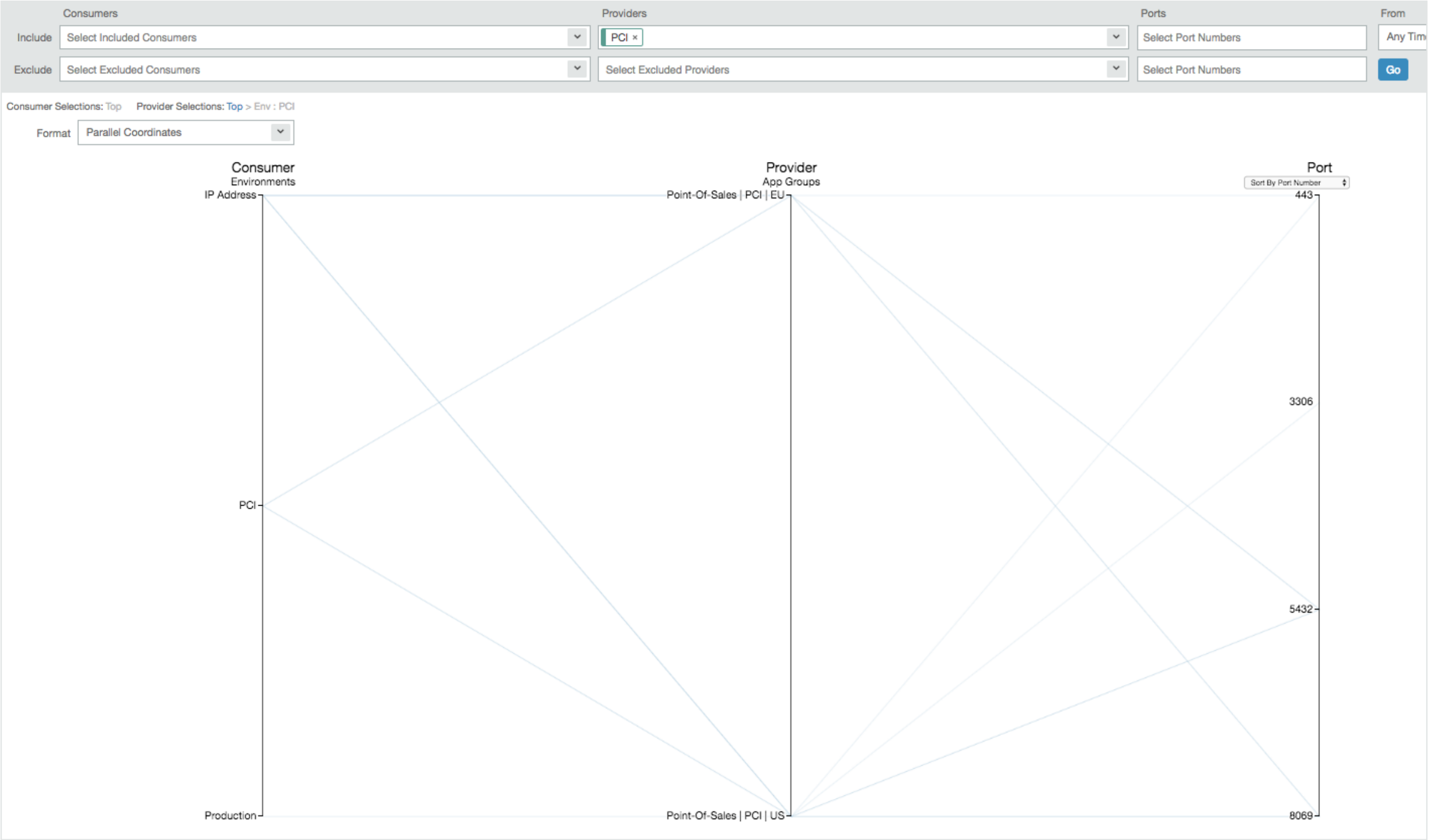
There's a reason that most PCI audits start with a data flow diagram. Auditors are used to working with spreadsheets, but a visual interface that enables them to actually map your PCI environment, understand the primary connections with applications and devices, and then identify key characteristics about those connections is much more effective and efficient.

Answer Key Questions Before They're Asked

There are certain questions that auditors ask again and again. Do you have any evidence of your development environment communicating with your production environment? Show me a list of all the connections into and out of your CDE and PCI-connected systems. Use a solution that lets you identify and answer these questions at the beginning of the audit, simplifying back-and-forth, and get through the audit as quickly as possible.

Query Platform to Chase Down and Fix Errors

Inevitably, your audit will turn up something you didn't expect. Given the complexity of modern environments and the range of requirements that PCI imposes, at least one curveball is guaranteed. Look for a security solution that prepares you for this with an effective query-and-correct interface so you can pinpoint and address mistakes when they do arise.



Providers Include: PCI ×

Consumer Selections: Top Provider Selections: Top > Env : PCI

Format: Parallel Coordinates

Query and visualization of all communications to PCI environments.

Conclusion

Accurate scoping and effective segmentation is the foundation of any successful PCI DSS program. It helps you effectively reduce your PCI scope, lower your compliance maintenance and audit costs, and pass your PCI audits. It is important to get started on the right foot. Host-based security segmentation lets you understand your PCI scope quickly, accurately, and precisely with application dependency mapping. It can enforce your PCI scope across environments and platforms to draw the narrowest possible circumference around your CDE, PCI-connected systems, and security-impacting systems. And it offers powerful tools to demonstrate compliance, from human-readable policies to visual mapping capabilities, and a powerful query platform to find and fix errors.

If you follow the steps laid out in this white paper, you won't just get through your PCI segmentation exercise quickly and painlessly—the entire audit will run more smoothly, quickly, and inexpensively. Best of all, it will leave you with a PCI environment that is secure, flexible, and ready to run your business.

About Illumio

Illumio enables organizations to realize a future without high-profile breaches by providing visibility, segmentation, and control of all network communications across any data center or cloud. Founded in 2013, the world's largest enterprises, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085. Tel (669) 800-5000 www.illumio.com.