illumio

SOLUTION BRIEF

MEETING PCI CHALLENGES WITH ADAPTIVE SECURITY

THE PROBLEM: PCI DSS COMPLIANCE IS DIFFICULT IN DYNAMIC ENVIRONMENTS

The nature of dynamic data centers and cloud infrastructures makes it increasingly difficult to isolate the system components within a Cardholder Data Environment (CDE). Application changes, environmental changes, and organizational changes can all disrupt Payment Card Industry Data Security Standard (PCI DSS) compliance efforts. At the same time, payment systems have grown considerably more complex, allowing for multiple new access points into a cardholder's data. All the while, determined hackers and criminal groups continue to voraciously seek out valuable cardholder information. If a breach or data loss occurs, it can result in termination of a covered organization's ability to accept payment cards, which can considerably impact its bottom line.

Major Credit Card Breaches[1]	
National discount retailer	40 million cards
High-end department store	1.1 million cards
Arts and crafts retailer	2.6 million cards
Picture frame retailer	400,000 cards
Nonprofit organization	868,000 cards
Home improvement retailer	56 million cards

Enterprises can face litigations, fines, and financial settlements for not fully meeting these compliance requirements.[2] At the same time, though, many organizations have faced massive cardholder data breaches, despite being fully compliant at the time of their data loss.[3,4] The difficult realization here for audit committees and security administrators alike is that compliance does not equal security.

Seasoned security practitioners recognize that security is an ongoing process that must be designed and applied across multiple aspects of their business to minimize threat exposure and risk. Simply holding a Report on Compliance (RoC)—which, by its nature, represents a single point in time—does not attest to an organization's current state of compliance due to rapid changes in applications and computing environments that are typical in today's dynamic data centers.

CURRENT CHALLENGES WITH MEETING PCI COMPLIANCE

Businesses also face the following challenges when working to meet PCI DSS compliance:

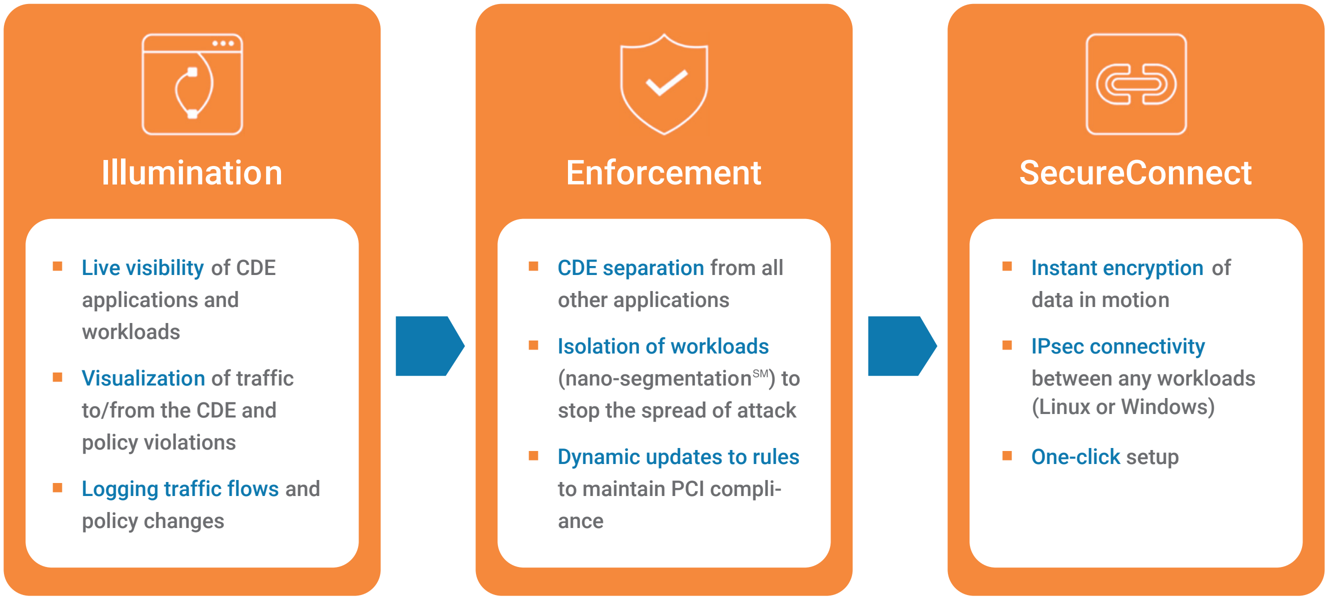
- **Architectural limitations:** Legacy technologies, like firewalls and intrusion detection and prevention systems, along with network security techniques, like configuring virtual local area networks (VLANs) and security zones, are often used to segment the system components within the CDE and connected systems from out-of-scope systems. These legacy technologies rely on writing and enforcing security policies with network constraints (e.g., IP addresses, subnets, VLANs, zones) that can lead to segmentation that is inflexible to changes, configuration errors, or mistakes. Supplemental technologies added to plug holes or gaps in existing network security devices (e.g., next-generation firewalls, web filtering, advanced threat detection, DNS monitoring) further add to cost and complexity.
- **Lack of visibility into the CDE and connected systems:** Most organizations spend the bulk of their security investments to protect their network and data center perimeters, but the inside of their data center—where the CDE resides—is left relatively unprotected. Organizations are also blind to the workloads that constitute their payment application topologies. This lack of visibility into the system components and traffic flowing in and out of the CDE makes it difficult, if not impossible, to fully protect this critical environment.

- **Manual processes to implement changes:** Security policies using traditional security technologies (e.g., firewalls, IDS/IPS) and techniques (e.g., VLANs, security zones) are static in nature. This means organizations are only compliant at that particular point in time; any changes within the CDE potentially puts them out of compliance. In addition, implementing security change controls for systems protecting the CDE involves manual processes that can take weeks to move into production.
- **Inconsistent security policies across environments:** Taking advantage of modern computing infrastructures, like public clouds, creates additional challenges for organizations trying to achieve PCI DSS compliance because public cloud providers do not allow control of their networks. This means organizations seeking the flexibility and cost savings found with cloud offerings are forced to construct divergent security policies from the ones already implemented within their on-premises data center. The lack of uniformity in security architecture and policies constrains businesses when integrating newly acquired businesses (and their data centers) or when migrating applications to public clouds.
- **Multiple workload deployment technologies:** Organizations are facing a tug-of-war amid continuous changes in their computing infrastructure. They are trying to support multiple technologies, from securing legacy bare-metal physical servers, to virtualized machines running on different hypervisors, and now new container-based deployments. Organizations need to streamline security controls evenly across all of these different workload deployment methods.

To address these challenges, organizations often invest in multiple security appliances, technologies, and techniques. However, leveraging different solutions from different providers creates gaps in protection and adds to the complexity, making it difficult to achieve and maintain compliance. Organizations need a solution that brings together all of these infrastructures, environments, and technologies in the most flexible and resilient way to easily achieve and maintain PCI compliance.

APPLYING ADAPTIVE SECURITY TO MAKE PCI EASIER TO IMPLEMENT AND MAINTAIN

The Illumio Adaptive Security Platform® (ASP) lets organizations apply consistent security within the PCI DSS framework and easily maintain compliance with security policies that adapt to changes.



Illumination

- **Live visibility** of CDE applications and workloads
- **Visualization** of traffic to/from the CDE and policy violations
- **Logging traffic flows** and policy changes

Enforcement

- **CDE separation** from all other applications
- **Isolation of workloads** (nano-segmentation^{SM}) to stop the spread of attack
- **Dynamic updates to rules** to maintain PCI compliance

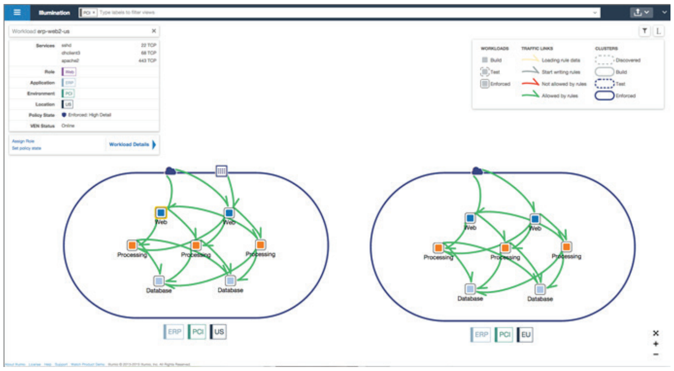
SecureConnect

- **Instant encryption** of data in motion
- **IPsec connectivity** between any workloads (Linux or Windows)
- **One-click setup**

Figure 1: Major capabilities available within Illumio ASP.

Illumio ASP eases the burden of achieving PCI compliance by offering:

- **Live traffic visibility:** Illumio's Illumination capability enables organizations to see live traffic of applications and system components both inside and outside of the CDE, regardless of their location. Real-time traffic connections to and from the CDE are visually graphed, along with any policy violations and anomalous traffic. *See Figure 2.*



Workload erp-web2-us

Services	sshd	22 TCP
	dhclient3	68 TCP
	apache2	443 TCP
Role	Web	
Application	ERP	
Environment	PCI	
Location	US	
Policy State	Enforced: High Detail	
VEN Status	Online	

Figure 2: The Illumination capability is showing permitted traffic connections (green arrows) between the three tiers of applications in the PCI environment. All other connection attempts are blocked by default. In this example, one application is located in the United States, and the other is in the European Union.

- **Visual application topology to support policy creation:** Using an interactive map, administrators can quickly understand the application topology and its potential impact to the CDE, helping them craft well-informed security policies. Administrators can use the Illumination capability to generate simple natural-language policies that capture permitted interactions between application components or use APIs to automate the process.
- **Audit trails and traffic logs:** Consistent with PCI DSS 3.2.1 requirements, Illumio ASP logs all traffic flows and visualizes any policy violations between workloads, enabling administrators to easily analyze the environment. Illumio ASP also provides audit trails and version control for policy changes made by administrators.
- **Granular application segmentation:** Illumio ASP enables segmentation of the CDE, including payment applications and databases, down to the individual workload and port, protocols, and processes within the workloads—an industry first. As an example, two instances of an Apache process running on a single workload could be segmented across two different applications.
- **Whitelist model:** Illumio ASP programs precise inbound and outbound rules on individual workloads using native security controls (i.e., iptables for Linux and Windows Filtering Platform for Windows Server). Enforcement uses whitelisting to only permit approved traffic in or out of the CDE and denies all other connections by default.
- **Threat detection and mitigation:** With Illumio ASP, organizations can apply adaptive security rules at the level of every single workload inside the CDE to stop data breaches in their tracks. For example, Illumio ASP can immediately block an attacker from making an outbound connection to steal skimmed credit card data from a compromised "collection" server. With Illumio protecting all of the workloads inside and outside of the CDE, the attacker's actions are restricted while attempts to spread to other systems are stopped and the data is prevented from being taken out of the CDE.
- **Automation of security:** Security rules are continuously updated to reflect any changes in the workload's state, the application, environment, or location—helping the organization continuously maintain PCI compliance in the face of changes.
- **Policy-based encryption of data in motion:** Illumio ASP safeguards sensitive cardholder data while it is transmitted over open, public networks. The SecureConnect capability provides instant encryption of data in motion between any combination of Linux and Windows workloads. IPsec connections are automatically established between workloads with a single click or specification in a policy rule. Additional IPsec connections are dynamically created for any new workloads (e.g., scale out) and automatically cleaned up once those systems are decommissioned.

ACHIEVING NETWORK SEGMENTATION WITH ILLUMIO

The PCI Security Standards Council strongly recommends segmenting the CDE from the rest of an organization's network. Without this segmentation, the entire network could be considered within the scope of a PCI DSS assessment. How does an organization ensure that even an out-of-scope workload or server that is compromised won't be able to communicate with any system components within the CDE?

By applying segmentation using Illumio ASP within their CDE and surrounding environments, organizations can begin seeing PCI DSS–associated benefits, including:

- **Reducing the scope—and therefore cost—of an assessment:** Isolating CDE down to its critical components. See Figure 3.
- **Decreasing the difficulty of implementing PCI controls:** Security for workloads is centrally managed.
- **Reducing risk to the business:** Shrinking the available attack surface, and tightly controlling access to the CDE.

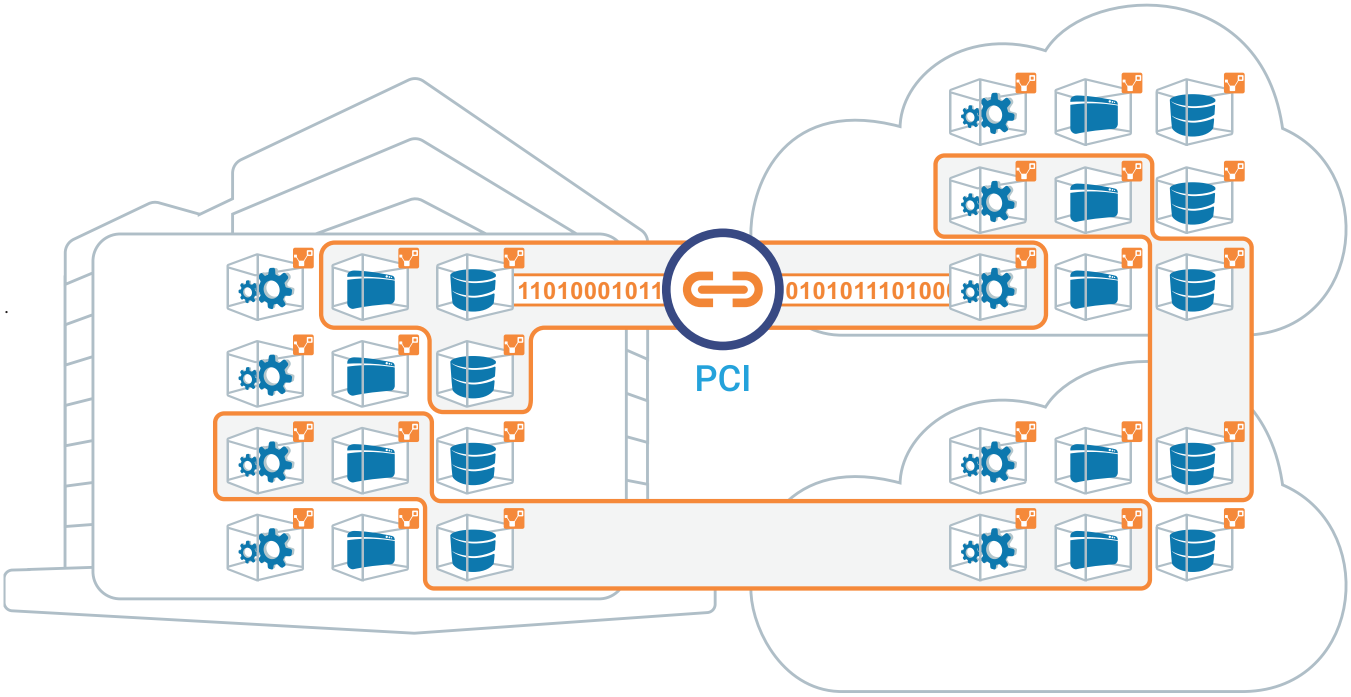


Figure 3: Illumio ASP isolates applications down to the ports, processes, and protocols and separates the PCI environment from environments outside the CDE—across data centers and public clouds.

IMPLEMENTING PCI DSS INTO YOUR DAILY BUSINESS WITH ILLUMIO

The PCI Standards Council encourages organizations to build PCI DSS–recommended best practices into their day-to-day business activities. By incorporating Illumio ASP into daily business activities, it becomes easier for an organization to maintain its PCI DSS compliance.

- **DevOps integration:** Illumio's REST APIs let Illumio ASP integrate with DevOps tools (e.g., Chef, Puppet, Ansible) to help with the automated management and deployment of application workloads, while assuring security is applied consistently and operating effectively.
- **Security decoupled from network:** Illumio enables organizations to express security policies in natural language, eliminating error-prone rules associated with network security constraints (e.g., IP addresses, subnets, VLANs, and zones).
- **Adaptive security:** Illumio ASP continuously adapts security policies to reflect any changes noticed in applications or within the CDE to maintain PCI DSS compliance while reducing complexity and helping cut firewall rules by 90 percent.[5]
- **Application topology view:** Illumination visualizes all application topologies and traffic flows, along with any CDE system components. This helps organizations map existing applications and discover new or unknown applications resulting from an organizational change (e.g., merger, acquisition).
- **Logging:** Illumio ASP logs all traffic connections and tracks all changes made to policy rules along with the responsible party and allows organizations to revert changes to a prior configuration if necessary.

[1] http://www.darkreading.com/operations/customers-arent-the-only-victims-5-stages-of-data-breach-grief/a/d-id/1319216

[2] http://www.pillsburylaw.com/siteFiles/Publications/7F4F43B367B5276B0CFA6D13CFF4044C.pdf

[3] http://www.darkreading.com/risk/compliance/target-pci-auditor-trustwave-sued-by-banks/d/d-id/1127936

[4] http://www.computerworld.com/article/2522625/security0/update--heartland-breach-shows-why-compliance-is-not-enough.html

[5] http://blogs.wsj.com/venturecapital/2015/04/14/illumio-shines-with-100m-for-star-wars-like-approach-to-cybersecurity/

ABOUT ILLUMIO

Illumio, the leader in micro-segmentation, prevents the spread of breaches inside data center and cloud environments. Enterprises such as Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite use Illumio to reduce cyber risk and achieve regulatory compliance. The Illumio Adaptive Security Platform® uniquely protects critical information with real-time application dependency and vulnerability mapping coupled with micro-segmentation that works across any data center, public cloud, or hybrid cloud deployment on bare-metal, virtual machines, and containers. For more information about Illumio, visit www.illumio.com/what-we-do or follow @Illumio.

- Engage with Illumio on Twitter
- Follow Illumio on LinkedIn
- Like Illumio on Facebook
- Subscribe to the Illumio YouTube Channel

CONTACT US

For more information about Illumio ASP and how it can be used to achieve environmental separation, email us at illuminate@illumio.com or call 855-426-3983 to speak to an Illumio representative.

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