PCI QSA Company

Illumio, Inc.
LIGHTING A PATH TO PCI COMPLIANCE

v1 December | 2015

truvantis

PR57F002

Truvantis, Inc.
548 Market Street
San Francisco, CA 94104
415.422.9844
truvantis.com

Illumio, Inc.
160 San Gabriel Drive
Sunnyvale, CA 94086
669.800.5000
illumio.com

TABLE OF CONTENTS

PURPOSE

Truvantis is an established and trusted Payment Card Industry Qualified Security Assessor (PCI QSA), providing audit and governance solutions that allow organizations to identify risk areas and implement remediation that is practical for their business type and size. The specific role of the QSA is to validate information about an environment and report compliance with the standards detailed in the Payment Card Industry Data Security Standard (PCI DSS).

As a regular part of this process, Truvantis evaluates the efficacy of professional solutions implemented in customer environments to achieve specific technical and policy-driven governance objectives. Because of its fit in addressing an identified need, this review is meant to provide the reader with an opinion on which aspects of the PCI DSS standard may be addressed by the Illumio Adaptive Security Platform (ASP) solution, and to what extent.

EXECUTIVE SUMMARY

The Illumio ASP is a flexible solution for the Enterprise environment to support its PCI requirements and is breaking new ground on giving IT Managers up to date awareness of their risk posture, through intelligent automation and adaptation. With its illumination technology, Illumio can help enterprise and auditors better understand the scope of their PCI systems to streamline audit and compliance activities.

By coupling environmental separation to strictly control access to PCI systems with SecureConnect technology that encrypts Cardholder data in-motion, the Illumio ASP can help enterprises meet or validate compliance with 7 out of 12 top level requirements.

Truvantis was furnished with a demonstration lab environment courtesy of Illumio in order to independently evaluate product features against PCI requirements. This document includes detailed analysis, a capability mapping to PCI DSS 3.1 requirements and conclusions based on our evaluation.

EVOLVING PCI LANDSCAPE

Traditional PCI compliance happens much like any other audited standard, and many companies offer much the same solution in terms of methodologies. Specialists engage in a process to capture a 'snapshot in time' for the targeted environment and compare against a standard. These are the only lines that have been measureable, but it leaves an obvious problem. Traditional audit cycles take time. Depending on the size of a scoped environment, testing, recording, and evaluating results of PCI audits may take days, weeks or even months. This is not an effective way to monitor and manage an environment's security or compliance with governance targets.

Depending on the size of a scoped environment, testing, recording, and evaluating results of PCI audits may take days, weeks or even months.

Looking at the regular release of critical vulnerabilities identified by vendors and security researchers, we know that every day that passes with an unresolved issue could leave an organization at significant operational and financial risk.

Enterprise complexity grows all the time. Production environments now rarely comprise a few relatively static systems humming along handling business. Advancements in collaboration tools, supply chain management and fulfillment, divergent security specializations, infrastructure as a service, complexity in necessary role based access controls, dynamic content, and endless other examples, have made keeping up with the live environment more and more challenging. Moreover, staff are required to keep on top of the changing operational heartbeat and to know the actual risk posture of their organization has grown significantly; their tasks have become increasingly daunting, time-consuming and expensive. The PCI standard specifies that an enterprise must maintain compliance through control of their inventory, locations and assets. In these complex environments that demands operationalization and automation of security controls and reporting.

It isn't just ordinary updates to the enterprise that occur. Technology solutions to identified needs are being released all the time. At the end of the audit cycle, the information could be so dated that the information may be significantly understated for real risk. Significant changes may have occurred that could go unidentified until the next audit cycle, a year later. Now that a significant portion of the financial liability of card fraud has formally transferred onto the merchant, they would do well to attain and retain a real time awareness and confidence in their operational risk posture.

Maintaining a real time awareness and confidence in operational risk posture becomes increasingly more essential and valuable to e-Commerce sites since they risk both prosecution and civil liability if they are breached. The payments industry is discussing this widely now.

EVOLVING TECHNOLOGIES

One such innovation that has left many industry standards behind is the move towards microsegmentation. Traditional models revolve around perimeters, tiered architectures and trust zones. Recent experience from breaches has shown us that such a 'line in the sand' approach is ineffective. Once a threat breaches a trust zone, the risk of onward compromise becomes high. Microsegmentation represents an effort to minimize the size of those trust zones, even as far as a single end-point being its own security zone with inbound and outbound traffic being controlled. This greatly enhances the security properties of a network as it reduces the ability of a breach to pivot or propagate thought that network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements…

PCI DSS v 3.1 Requirement 1

The disadvantage with microsegmentation is the management overhead. With all traffic being effectively whitelisted within the network it would be unreasonable to expect a tradition firewall ruleset to be maintained that could represent only what is permitted between every endpoint – let alone handle all the traffic. Microsegmentation is therefore generally implemented in the hypervisor or using host based controls. PCI DSS often presents requirements in terms of legacy technologies names – Firewall, IPS, WAF. But new technologies are often overlooked for many reasons, including a fear that while technically equivalent (or superior), they may not be accepted by an auditor who may not be familiar enough with them. However, the PCI Security Standards Council, and in places the PCI DSS standard itself, states that new technologies are permitted if they meet the letter and intent of the requirement. For example, the preamble to the first requirement clearly states *"Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1."*

Illumio, Inc. addresses this modern dynamic environment with their Adaptive Security Platform (ASP), which when deployed with proper coverage in a production environment, can monitor and display real time events and be set to enforce security policy using microsegmentation all the way to the endpoint systems. This either supports or meets and exceeds many PCI-DSS requirements even though the solution does not carry the traditional product class label familiar to experienced security practitioners.

MAPPING PCI REQUIREMENTS AND ILLUMIO ASP

PCI DSS Overview

The PCI standard is grouped into 6 Control topics across 12 requirements.

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. "System components" include network devices, servers, computing devices, and applications.

For most merchants and service providers, the scope of applicability for PCI DSS is vast, complex and … constantly changing.

What business processes use credit card data and where is this data stored? Who has access to such data? Can you identify the ports used when transmitting cardholder data? What are the protocols involved? Are you certain of the technology assets and data flows involved? A change currently affecting many merchants is the shift from "swipe and sign" to chip enabled credit cards as the standard payment forms. For most merchants and service providers, the scope of applicability for PCI DSS is vast, complex and due to evolving standards and dynamic environments, constantly changing.

Illumio ASP Overview

The Illumio ASP works by installing a lightweight agent called a "Virtual Enforcement Node" (VEN) on each computing instance in the environment. This collects data about the IP addresses that are communicating with each other and the ports and protocols involved in those communications and sends it to a central controller called the Policy Compute Engine (PCE). The PCE then provides a visual representation of both the direction of communication and the devices involved. When configured in "Enforcement Mode," the PCE computes policies applicable for each device and sends them to the VENs to instrument native stateful firewalls (iptables or Windows Filtering Platform) already present on those operating systems. In this way, the Illumio ASP can be used to ensure that only expected sources and destinations communicate over only expected ports and protocols across the entire environment.

Some management features of the ASP include easy drag and drop of workload profiles onto assets with automatic firewall rule generation to support the desired dataflow, easy correlation by operators of expected versus actual traffic patterns, and the solution is flexible for use in any extended enterprise, including cloud or virtual environments.

Mapping of Illumio ASP Solution by PCI-DSS Requirements

In our opinion, Illumio ASP supports PCI DSS in several ways:

- Selected features that can be used to **meet** PCI DSS requirements
  - Restricting connections like a firewall
  - Encrypting traffic over public networks
- Selected features that **support** efforts to meet PCI DSS requirements
  - Tagging server roles so that configuration standards can be applied
  - Mapping connections to support the development of a cardholder dataflow diagram
- Selected features that support efforts to **validate** compliance
  - Listing connections so that their authorization and business purpose can be verified
  - Providing visual confirmation of segmentation effectiveness

For a detailed analysis of how each requirement of the PCI DSS may be supported, please refer to Addendum A, within this document.

When an entity's Cardholder Data Environment is fully protected by the Illumio ASP solution, the solution may be used to meet the following requirements outright – or it may support compliance or validation.

		Meet	Support	Validate
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data	1.2, 1.2.1, 1.3, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7	1.1.2, 1.1.3, 1.1.7, 1.3.1	
	2. Do not use vendor-supplied defaults for system passwords and other security parameters		2.2.4, 2.4, 2.6	2.2.1, 2.2.2, 2.2.3
Protect Cardholder Data	3. Protect stored cardholder data			
	4. Encrypt transmission of cardholder data across open, public networks	4.1		
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs			
	6. Develop and maintain secure systems and applications	6.4.1, 6.5.4		6.3
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know			
	8. Identify and authenticate access to system components	8.2.1	8.1.5	
	9. Restrict physical access to cardholder data			
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data		10.2.4	
	11. Regularly test security systems and processes		11.4	
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel			

ADDITIONAL ANALYSIS INFORMATION AND LIMITATIONS

Truvantis was furnished with a demonstration lab environment courtesy of Illumio. This gave us a live environment to evaluate. It provided a means to review many of the described solution features, in operation. Exactly how one can meet PCI requirements using Illumio ASP to secure the infrastructure will of course depend on unique customer specific details. However, the analysis provided within this document is a capability mapping and the conclusions are based on that information. Based on the product review, it seems very viable for Illumio ASP to support PCI compliance.

There are some features of Illumio ASP that could easily substitute for more traditional methods such as the requirement for a firewall. Since Illumio ASP contains a Policy Compute Engine (PCE) which is capable of creating 'iptables' configurations for Linux systems, and Windows Filtering Platform (WFP) filters for Microsoft Windows installations, the Illumio ASP can be used as a substitute for both firewall and routers when used in "Enforcement" mode.

CONCLUSION

as reviewed from the standpoint of a QSA … the product features do carry significant merit with regard to meeting many PCI requirements.

The Illumio ASP is a flexible solution for the Enterprise environment to support its PCI requirements and is breaking new ground on giving IT Managers up to date awareness of their risk posture, through intelligent automation and adaptation. Like any solution, it is not all encompassing to the entire standard, but may prove substantially useful to administrators of a dynamic or complex environment. The nature of the solution is to constantly update itself and in this way it brings confidence to the administrators that they have current operational awareness. Because every infrastructure is unique, the best way to assess how Illumio could fit into a particular organization would be to contact the vendor and request a trial instantiation within an organization's live environment and then review your planned approach with your QSA. But as reviewed from the standpoint of a QSA company ourselves, the product features do carry significant merit with regard to meeting many PCI requirements.

ADDENDUM A - ILLUMIO ASP PCI SUPPORT MATRIX

Note: Some data within this chart is abbreviated from the PCI DSS for readability. See specification for full details.

No.	Requirement	Guidance	Analysis
1.1.2	Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.	Network diagrams describe how networks are configured, and identify the location of all network devices. Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.	The Illumio management interface displays real time connectivity and data flow across VEN nodes. This information may be used to create an initial draft of the CDE network or to validate existing documentation.
1.1.3	Current diagram that shows all cardholder data flows across systems and networks	Cardholder data-flow diagrams identify the location of all cardholder data that is stored, processed, or transmitted within the network. Network and cardholder data-flow diagrams help an organization to understand and keep track of the scope of their environment, by showing how cardholder data flows across networks and between individual systems and devices.	The Illumio management interface displays real time connectivity and data flow across VEN nodes. This information may be used to create an initial draft of the CDE network or to validate existing documentation.
1.1.7	Requirement to review firewall and router rule sets at least every six months	This review gives the organization an opportunity at least every six months to clean up any unneeded, outdated, or incorrect rules, and ensure that all rule sets allow only authorized services and ports that match the documented business justifications. Organizations with a high volume of changes to firewall and router rule sets may wish to consider performing reviews more frequently, to ensure that the rule sets continue to meet the needs of the business.	The Illumio management interface displays the current active firewall rules installed across VEN nodes. This information may be used to create an initial draft of the CDE network or to validate existing documentation.

No.	Requirement	Guidance	Analysis
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.	It is essential to install network protection between the internal, trusted network and any untrusted network that is external and/or out of the entity's ability to control or manage. Failure to implement this measure correctly results in the entity being vulnerable to unauthorized access by malicious individuals or software. For firewall functionality to be effective, it must be properly configured to control and/or limit traffic into and out of the entity's network.	This is the core function of Illumio in Enforcement mode. Host firewalls are discretely configured by the analysis engine and applied to each system with the VEN agent installed. Real time connection information provided by Illumio may be compared against network documentation to verify connections to the CDE are appropriately restricted. Examination of the VEN firewall rules are the configured and installed rules, cited by this requirement.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	This requirement is intended to prevent malicious individuals from accessing the entity's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within your network out to an untrusted server). Implementing a rule that denies all inbound and outbound traffic that is not specifically needed helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic in or out.	VEN firewall rules are built by the analysis engine for both ingress and egress from each node on a per interface basis.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	A firewall's intent is to manage and control all connections between public systems and internal systems, especially those that store, process or transmit cardholder data. If direct access is allowed between public systems and the CDE, the protections offered by the firewall are bypassed, and system components storing cardholder data may be exposed to compromise.	The Illumio ASP will show all dataflow enforcement and compared to the existing Dataflow diagram validates compliance, when architected in accordance with 1.3.

No.	Requirement	Guidance	Analysis
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	The DMZ is that part of the network that manages connections between the Internet (or other untrusted networks), and services that an organization needs to have available to the public (like a web server). This functionality is intended to prevent malicious individuals from accessing the organization's internal network from the Internet, or from using services, protocols, or ports in an unauthorized manner.	The Illumio ASP can assist with creating a DMZ and will show all dataflow enforcement, which, compared to the existing Dataflow diagram, validates compliance. Because the host-based firewall enforces explicitly on authorized traffic, unintended services, protocols and ports will be disallowed.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	This functionality is intended to prevent malicious individuals from accessing the organization's internal network from the Internet, or from using services, protocols, or ports in an unauthorized manner.	The Illumio ASP will show all dataflow enforcement and, when compared to the existing Dataflow diagram validates compliance, when architected in accordance with 1.3.
1.3.3	Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	Examination of all inbound and outbound connections allows for inspection and restriction of traffic based on the source and/or destination address, as well as inspection and blocking of unwanted content, thus preventing unfiltered access between untrusted and trusted environments. This helps prevent, for example, malicious individuals from sending data they've obtained from within your network out to an external untrusted server in an untrusted network.	The Illumio ASP will prevent direct connections between untrusted networks and the CDE, and show any attempts at such communications.

No.	Requirement	Guidance	Analysis
1.3.4	Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	Normally a packet contains the IP address of the computer that originally sent it so other computers in the network know where the packet came from. Malicious individuals will often try to spoof (or imitate) the sending IP address so that the target system believes the packet is from a trusted source. Filtering packets coming into the network helps to, among other things, ensure packets are not "spoofed" to look like they are coming from an organization's own internal network.	VEN node enforces firewall rules on a per interface basis will disallow unexpected source traffic from vectors not actively configured during the build and test phases of deployment.
1.3.5	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	All traffic outbound from the cardholder data environment should be evaluated to ensure that it follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications (for example by restricting source/destination addresses/ports, and/or blocking of content).	The VEN implicitly enforces the rules it has established on any traffic destined for or traversing nodes with the Illumio ASP VEN software installed.
1.3.6	Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	A firewall that performs stateful packet inspection maintains the "state" (or the status) for each connection through the firewall. By maintaining the "state," the firewall knows whether an apparent response to a previous connection is actually a valid, authorized response (since it retains each connection's status) or is malicious traffic trying to trick the firewall into allowing the connection.	It is the inherit nature of IPtables and Windows Filtering Platform (WFP) to create stateful connections on match. Illumio leverages these technologies for enforcement and therefor this will always be compliant where Illumio is deployed at any and boundary nodes.

No.	Requirement	Guidance	Analysis
1.3.7	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	If cardholder data is located within the DMZ, it is easier for an external attacker to access this information, since there are fewer layers to penetrate. Securing system components that store cardholder data in an internal network zone that is segregated from the DMZ and other untrusted networks by a firewall can prevent unauthorized network traffic from reaching the system component. Note: This requirement is not intended to apply to temporary storage of cardholder data in volatile memory.	Illumio can be used to view real time connections and filtering to show that no direct network connections exist between untrusted networks and the CDR.
2.2.1	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)	If server functions that need different security levels are located on the same server, the security level of the functions with higher security needs would be reduced due to the presence of the lower-security functions. Additionally, the server functions with a lower security level may introduce security weaknesses to other functions on the same server. By considering the security needs of different server functions as part of the system configuration standards and related processes, organizations can ensure that functions requiring different security levels don't co-exist on the same server.	PCI requirements dictate that CDE services be protected from direct untrusted access. By having VENs deployed to the core components of the CDE (front end, DB, etc.) Illumio brings visibility of actual connections. By comparing to the CDE architecture data flow, it is simple to verify.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	As stated in Requirement 1.1.6, there are many protocols that a business may need (or have enabled by default) that are commonly used by malicious individuals to compromise a network. Including this requirement as part of an organization's configuration standards and related processes ensures that only the necessary services and protocols are enabled.	Illumio ASP assures that only allowed and expected protocols are in use through the whitelisting features.

No.	Requirement	Guidance	Analysis
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc. Note: SSL	Enabling security features before new servers are deployed will prevent servers being installed into the environment with insecure configurations. Ensuring that all insecure services, protocols, and daemons are adequately secured with appropriate security features makes it more difficult for malicious individuals to take advantage of commonly used points of compromise within a network. Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.).	Here Illumio will show any ports or protocols which are considered insecure and enable the Administrators to implement alternative solutions. Illumio can also provide real time evidence that no ports or protocols exist across any node employing the VEN software.
2.2.4	Configure system security parameters to prevent misuse.	System configuration standards and related processes should specifically address security settings and parameters that have known security implications for each type of system in use. In order for systems to be configured securely, personnel responsible for configuration and/or administering systems must be knowledgeable in the specific security parameters and settings that apply to the system.	Illumio's VEN whitelist strategy are in line with Principle of least privilege and disable unnecessary services concepts. While it does not change the authorization configuration nor the services operation, it does effectively reduce these attack surfaces somewhat. In this way, Illumio may be used as a compensating control to reduce risk, if these requirements cannot otherwise be met, in the CDE.

No.	Requirement	Guidance	Analysis
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	Maintaining a current list of all system components will enable an organization to accurately and efficiently define the scope of their environment for implementing PCI DSS controls. Without an inventory, some system components could be forgotten, and be inadvertently excluded from the organization's configuration standards.	Illumio's dynamic learning function for the VEN ruleset build will show all network activity required to complete all business functions. This situation will result in the opportunity to update PCI documentation to include all system components.
2.6	Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in the standard's "Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers."	This is intended for hosting providers that provide shared hosting environments for multiple clients on the same server. When all data is on the same server and under control of a single environment, often the settings on these shared servers are not manageable by individual clients. This allows clients to add insecure functions and scripts that impact the security of all other client environments; and thereby make it easy for a malicious individual to compromise one client's data and thereby gain access to all other clients' data. See Appendix A for details of requirements.	In a standard shared environment, resources on any shared platform would typically retain their own network assignment. This would engage the host's VEN and corresponding Host and network firewall rules.
4.1	Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks	Sensitive information must be encrypted during transmission over public networks, because it is easy and common for a malicious individual to intercept and/or divert data while in transit.	Illumio may be configured to build its own point to point VPNs between VEN nodes.

No.	Requirement	Guidance	Analysis
6.3	Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: -In accordance with PCI DSS (for example, secure authentication and logging) -Based on industry standards and/or best practices. -Incorporating information security throughout the software-development life cycle	Without the inclusion of security during the requirements definition, design, analysis, and testing phases of software development, security vulnerabilities can be inadvertently or maliciously introduced into the production environment.	Illumio would show and thus validate when secure authentication connection requests and logging connections occur, as expected in the CDE networks.
6.4.1	Separate development/test environments from production environments, and enforce the separation with access controls.	Due to the constantly changing state of development and test environments, they tend to be less secure than the production environment. Without adequate separation between environments, it may be possible for the production environment, and cardholder data, to be compromised due to less-stringent security configurations and possible vulnerabilities in a test or development environment.	Deploying VENs across all of the CDE nodes will create an innate blocking enforcement between any unauthorized networks or hosts, including Production/staging/test and dev.
6.5.4	Insecure communications	Applications that fail to adequately encrypt network traffic using strong cryptography are at increased risk of being compromised and exposing cardholder data. If an attacker is able to exploit weak cryptographic processes, they may be able to gain control of an application or even gain clear-text access to encrypted data.	VENs can be configured to augment less secure communications by building its own secure point to point tunnels.

No.	Requirement	Guidance	Analysis
8.1.5	Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: -Enabled only during the time period needed and disabled when not in use. -Monitored when in use.	Allowing vendors to have 24/7 access into your network in case they need to support your systems increases the chances of unauthorized access, either from a user in the vendor's environment or from a malicious individual who finds and uses this always-available external entry point into your network. Enabling access only for the time periods needed, and disabling it as soon as it is no longer needed, helps prevent misuse of these connections. Monitoring of vendor access provides assurance that vendors are accessing only the systems necessary and only during approved time frames.	Vendors typically interact from well known (i.e. static) source IP addresses. This is easily configurable as an inclusion to VEN rulesets managing remote access across the vendor.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	Many network devices and applications transmit unencrypted, readable passwords across the network and/or store passwords without encryption. A malicious individual can easily intercept unencrypted passwords during transmission using a "sniffer," or directly access unencrypted passwords in files where they are stored, and use this data to gain unauthorized access.	The one-click IPsec configurable feature within the ASP can ensure any communications, including credential transmission is conducted with strong encryption.
10.2.4	Invalid logical access attempts	Malicious individuals will often perform multiple access attempts on targeted systems. Multiple invalid login attempts may be an indication of an unauthorized user's attempts to "brute force" or guess a password.	The whitelist methodology Illumio employs will close the attack surface for any unauthorized authentication attempt by brute force or other means from unexpected sources.

No.	Requirement	Guidance	Analysis
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	Intrusion detection and/or intrusion prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known "signatures" and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and send alerts and/or stop the attempt as it happens. Without a proactive approach to unauthorized activity detection, attacks on (or misuse of) computer resources could go unnoticed in real time. Security alerts generated by these techniques should be monitored so that the attempted intrusions can be stopped.	Illumio provides real time status and visually alerts users of its management interface and provides logging events. With that monitoring and blocking (prevention), Illumio can be a strong component in enforcing any unexpected communications pattern.