EVOLVE IP
THE CLOUD STRATEGY COMPANY™

Cloud Brief

Achieving PCI Compliance with The Evolve IP Compliance Cloud™

PCI DSS CERTIFIED
SERVICE LEVEL 1

This white paper outlines how the security safeguards of *The Compliance Cloud*™ (Evolve IP's virtual private cloud) effectively and efficiently address the PCI requirements in regards to the privacy and security of customer cardholder data.

Overview

Although Evolve IP does not directly manage the storage, transmission and processing of customer cardholder data (CHD), our compliance with PCI DSS 3.1 Service Level 1 ensures our customers have the ability to create their own cardholder data environment (CDE) that can store, transmit or process CHD with The Evolve IP Compliance Cloud™.

Payment Card Industry Data Security Standard – The Basics

The Payment Card Industry Security Standards Council (PCI SSC) was founded in 2006 by the major card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. The Council created the PCI Data Security Standard (PCI DSS) as a worldwide information security standard for protecting credit card data, and agreed to incorporate the PCI DSS as part of the technical requirements for each of their data security compliance programs. In addition to developing the requirements and enforcing annual compliance, each member also recognizes the Qualified Security Assessors (QSA's) and Approved Scanning Vendors (ASV's) that are annually qualified by the Council.

The PCI DSS comprises 12 categories addressing the major areas of Building and Maintaining Secure Networks and Systems; Protecting Cardholder Data; Maintaining a Vulnerability Management Program; Implementing Strong Access Control Measures; Regularly Monitoring and Testing Networks; and Maintaining an Information Security Policy.

PCI DSS standards mirror the practices that security-oriented organizations already employ, following industry practices to properly protect the data and infrastructure of the business. While some of the terms and acronyms used by retailers and payment processing vendors may be unique, the basic processes and technologies required to secure their information and infrastructure don't differ significantly.

Who Must Comply with PCI Regulations?

The number one goal of any PCI DSS solution is ensuring end-to-end security, from the moment a consumer pulls out their payment card until the card-holder data is fully erased from the system. As such, the PCI DSS applies to virtually all entities involved in payment card processing including merchants, processors, acquirers, issuers, and service providers. The PCI DSS also applies to all other covered entities that store, process, or transmit cardholder data and/or sensitive authentication data, or provide services to those covered entities, since they provide services that control or could impact the security of cardholder data.

The first thing merchants need to know are the three critical steps in PCI DSS compliance.

- **Assess:** identify cardholder data, inventory the company's IT assets and business processes for payment card processing, and analyze each for security weaknesses.
- **Remediate:** address perceived vulnerabilities and remove unneeded cardholder data.
- **Report:** compile and submit remediation authentication records (if applicable), and provide compliance reports to each bank and payment card company they do business with.

By amending onsite payment processes and implementing the proper security technologies, organizations can begin to meet the vast majority of PCI DSS requirements, but that still leaves serious gaps outside the business. Has the network been locked down, with effective access protection? Is cardholder data stored properly onsite, and are there effective and secure data backup and recovery systems? To ensure compliance, the process of assessing, remediating and reporting must be continuous practice.

Another key aspect of PCI DSS compliance is the required reporting schedules. Credit card companies validate that retailers and their providers are abiding by the regulations on an annual basis, with the volume of transactions (and risk) determining the depth of that evaluation (as covered under "*Payment Card Industry Data Security Standard - The Basics*"). Along with requiring participating businesses to complete a self-assessment

questionnaire, MasterCard and Visa require on-site visits and network scans performed by authorized PCI compliance scanning vendors.

The information contained in PCI DSS reports includes:

- **Summary of findings**: a general statement and details of the security assessment
- **Business information**: business description, contacts, and provider/processor details
- **Card payment infrastructur**e: network schematics, transaction flow diagram, terminal and POS (point of sale) solutions employed, wireless network details
- **Third-party relationships**: companies with access to cardholder data, such as solution providers, banking institutions and payment card vendors

Implications and Opportunities

PCI DSS can be complicated for the novice solution provider. To help those who build and support secure payment applications, the PCI Security Council created a number of compliance-related resources and programs. That includes the Payment Application Data Security Standard (PA-DSS) and a list of "Validated Payment Applications" to select from, along with Self-Assessment Questionnaires that allow merchants to authenticate their current security procedures.

Compliance goes beyond credit card processing systems. It extends to the network, data storage infrastructure and any method involved in the management or transport of customer data, with responsibility falling on the merchant and those who support it. Solution providers who fail to implement PCI DSS compliant solutions may find themselves liable (at least in part) for any damages their clients and their customers suffer. Noncompliance penalties can range from $1,000 to $100,000 per month for PCI-related violations, while these initial penalties will first be levied by payment brands and from banks. The PCI Council has pointed out that this fine will be passed down to the merchant, leading to higher direct costs, as well as hindered relationships with the bank and often higher transaction fees.

For tools and resources to support your PCI Compliance initiatives, visit:

https://www.pcisecuritystandards.org/

The Solution Provider Role and Accountability

The *PCI DSS Cloud Computing Guidelines Information Supplement*[2] was published in an effort to extend the responsibility for securing credit card information to cloud computing providers. The supplement clearly defines the security responsibilities of the cloud provider and the cloud customer.

The PCI DSS Cloud Computing Guidelines Information Supplement provides clarification on what is required to protect customers' credit card information and support PCI DSS compliance in the cloud. It goes without saying that any business that conducts credit card transactions is obliged to comply with PCI DSS. But as businesses more and more contract hosted data centers – often cloud based storage centers – to warehouse their customers' information, the PCI Security Standards Council needed to explicitly extend compliance to these vendors as well.

According to the PCI SSC, the responsibility of securing credit card information is shared by both the cloud service provider and its clients. However, the ultimate responsibility for PCI DSS compliance lies with the cloud customer who stores cardholder data with a third-party service provider. The supplement helps organizations with the following:

- **Cloud overview:** explains different models of cloud services and how compliance implementation may vary within the different types of models.
- **Cloud provider/cloud customer relationships:** outlines roles and responsibilities across different cloud models. It also provides guidance on determining and documenting responsibilities for cloud providers and their customers.
- **PCI DSS considerations:** provides guidance and examples to help determine responsibilities for specific PCI requirements.
- **PCI DSS compliance challenges:** describes some of the challenges with demonstrating and documenting PCI DSS compliance for cloud providers.

Depending upon the cloud service and deployment model, many security implementations are shared between the cloud service provider and the system owner, and operating under this shared responsibility model can represent a technical and/or an organizational shift. Clear guidelines, like the new PCI DSS standard, helps to provide more clarity for businesses to develop and maintain a robust security control environment in the cloud.

But the cloud can actually help resolve security challenges and meet the demand for a higher level of security. For example, as companies grow and their scope expands, the complexity of managing security increases. PCI DSS has a requirement to centralize log collection and monitoring, which can be challenging when there is a high volume of logs. *The Evolve IP Compliance Cloud* can help with that by providing a way to centrally collect logs and perform that monitoring function.

Customers are responsible for configuring their applications, platforms, websites and portals in a PCI-compliant manner, for restricting and monitoring access to customer cardholder data, and for enforcing policies in their organizations to meet PCI compliance.

Additionally, since businesses span across many regional and international boundaries, it is challenging to understand and apply the various regulations and standards across the company, especially if the data location means that security controls aren't applied as needed. For example, some local laws and regulations have strict limits around data handling and retention. Addressing multiple unique data handling laws can be difficult and time consuming for businesses operating in multiple countries. Evolve IP gives companies a great amount of granular control over where data resides, whether they want to move it to another jurisdiction or prevent it from being moved. Evolve IP's customers also have a great amount of visibility and transparency into which controls are applied to which resources, and how those controls are operating. This granular control greatly reduces their security and regulation risks.

What Makes Evolve IP "Best of Breed" for PCI Compliant Hosting?

Evolve IP is a nationally recognized cloud-based technology provider that designs, hosts, manages and supports enterprise-class integrated hosted technology solutions. These technology solutions can be managed services or hosted environments for customers directly involved in PCI services; therefore, Evolve IP is considered a service provider and needs to have a secure and certified environment that protects these PCI customers. In addition, shared hosting providers (or those providing PCI services for hosted PCI environments) are required to meet additional specific controls for their service environments.

Evolve IP engaged an approved PCI QSA and is now certified as a Level 1 PCI Service Provider in all 12 PCI version 3.1 categories, and has PCI offerings of Managed Firewall, Managed Virtual Data Center (VDC), Customer Managed Virtual Data Center, Co-Location, Hosted Private Branch Exchange (PBX), Backup as a Service, and Hosted Exchange.

As a Level 1 certified PCI Service Provider, the highest level of validation for payment card data security, Evolve IP demonstrates a strong security posture and dedication to information security to their clients.

For covered entities, *The Compliance Cloud*™ delivers the following:

Cloud Model

- Evolve IP uses a private cloud model for PCI customer environments. Each customer has a dedicated virtual switch that routes traffic through their own dedicated firewall; this design model provides complete segregation between customers.
- An independent third-party SOC2 review of the Evolve IP cloud environment was performed by an Independent Service Auditing firm. This review culminated in a favorable report; a summary report of which is available to customers and potential customers.
- An independent certified QSA reviewed the PCI Compliance environment and controls of Evolve IP, and issued a PCI Report on Compliance (ROC) attesting that Evolve IP met all the controls in the 12 PCI version 3.1 categories under their PCI compliance cloud offering. An accompanying Attestation of Compliance (AOC) is available to PCI customers so it can be used for their PCI compliance requirements.

Restricting Access to Customer Data

- Evolve IP limits access to customer firewalls, routers, switches, and other infrastructure equipment to authorized Evolve IP administrators and engineers.
- Customers are responsible for creating their system administrators, individual users, and creating access to resources (fileservers, directories, etc.).
- Physical access to Evolve IP data centers requires two-factor authentication, and is restricted to approved Evolve IP personnel.

Access Controls

- Evolve IP uses logging to monitor customer logins to their servers and environment.
- Evolve IP provides Intrusion Prevention/Intrusion Detection Services (IPS/IDS) at the individual customer firewall edge of their network. All events and logs are continually streamed to a secure 24x7 event monitoring center.
- Evolve IP uses data storage in customer environments that employs a high level of certification for data at rest, and industry-accepted encryption methods for data in transit to and from the covered entities' locations to the Evolve IP locations (includes VPN tunnels and virtual desktop access).

Physical Controls

- Evolve IP requires that all visitors must sign in at the front desk and be escorted in all Evolve IP locations.
- Evolve IP securely removes all customer data from all devices upon termination of services.
- Evolve IP restricts movement within its facilities by use of access badge restrictions.

Risk Controls

- Evolve IP has implemented an annual risk assessment process that requires information owners to identify significant threats to security, availability, and confidentiality and to implement appropriate measures to monitor and manage these risks.
- Evolve IP's information security team monitors the system and assesses the system vulnerabilities; additionally, all IDS alarms are reviewed, escalated and corrective actions are implemented.
- Evolve IP has compliance, data backup, disaster recovery and incident management plans.

Achieving PCI Compliance With The Evolve IP Compliance Cloud

Essential to any compliance program is the establishment of responsibilities and accountabilities addressing both the solution provider and the customer. In accordance with Requirement 12.8.5 and other requirements, Evolve IP provides customers with a responsibility matrix that describes the actions an Evolve IP customer must take in order to maintain its own PCI compliance when cardholder data and other sensitive information is passing through Evolve IP's systems. The PCI DSS responsibility matrix is intended for use by Evolve IP customers and their Qualified Security Assessors (QSAs) for use in audits for PCI compliance.

The following table provides a high-level view of PCI controls and the key technologies or processes provided by Evolve IP:

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	Evolve IP Managed Firewall and Intrusion Detection System (IDS) with Log Management and Notification
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
	Evolve IP Managed ITaaS with Active Directory (AD) roles and Group Policy Objects (GPOs)
Protect Cardholder Data	3. Protect all stored cardholder data
	Encryption in transit and at rest
	4. Encrypt transmission of cardholder data across open, public networks
	Evolve IP Cloud Connect and suite of connectivity solutions

Achieving PCI Compliance With The Evolve IP Compliance Cloud

Goals	PCI DSS Requirements
Maintain a Vulnerability Management Program	5. Employ and update anti-virus software on a continual basis
	Evolve IP Remote Monitoring and Management (RMM) with anti-virus and ITaaS
	6. Develop and maintain secure systems and solutions
	Alert Logic and Qualys Partner with SOC 2 Trust Services Principles
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business necessity
	Evolve IP ITaaS with Active Directory (AD) and Group Policy Objects (GPO)
	8. Assign a unique identification to each person with system and network access
	SOC 2 Trust Services Principles
	9. Restrict Physical Access to Cardholder Data
	All three of Evolve IP's data centers are PCI Compliant
Regularly Monitor and Test Networks	10. Track and monitor all access to networks, applications and cardholder data
	All logging is centralized and correlated through Alert Logic
	11. Regularly Test System Protect and Processes
	Qualys testing conducted monthly and quarterly with third-party penetration and vulnerability testing
Maintain an Information Security Policy	12. Maintain a policy that addresses data security
	SOC 2 Trust Services Principles

In addition to what is described in the responsibility matrix, the customer is responsible for all PCI requirements related to customer-maintained software and systems.

Product Guidance

Evolve IP offers various products to suit a wide range of customer needs. When purchasing cloud services for your compliance project, please specify with your Evolve IP Technology Advisor, that you are seeking the added value and security available exclusively with *The Evolve IP Compliance Cloud*™.

Your Technology Advisor can assist you with a menu of Evolve IP Compliant SKU's for Communications, Desktops, Email, Servers, Storage and Backup to ensure you are selecting *The Compliance Cloud*.

Conclusion

Compliance with the Payment Card Industry Data Security Standard (PCI DSS) is mandatory for all entities involved in payment card processing and finding the right hosting partner is vital to success.

While there are many complex variables relating to PCI, Evolve IP delivers the technology and expertise to help customers confidently meet compliance requirements for hosting their customer cardholder data.

Evolve IP can help customers meet PCI DSS compliance regulations with a solution that provides cloud and local backup and data recovery, proactive data security and reliable data retention and restoration. We offer complete data protection services with support for desktops, laptops, and servers, files and folders, Microsoft Exchange Information Store, Exchange mailbox, SQL, System State and VMware and Hyper-V images. Backups are highly automated and enable fast and easy restores and are performed from a single management console.

Designed to deliver data-centric security architecture, military-grade encryption, and robust auditing features, *The Compliance Cloud*™ provides security decision-makers and administrators with a virtual private cloud that meets, and in many instances exceeds PCI DSS requirements.

Learn More

For more information on *The Evolve IP Compliance Cloud* including additional security and compliance offerings, visit: http://www.evolveip.net/compliance.

References

[1] *PCI DSS Cloud Computing Guidelines*
https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

[2] PCI DSS Cloud Computing Guidelines Information Supplement
https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

About Evolve IP

Evolve IP is The Cloud Strategy Company™. Designed from the beginning to provide organizations with the ability to deploy both cloud computing and cloud communications onto a single platform, today, nearly 200,000 users rely on Evolve IP for services like disaster recovery, contact centers, unified communications, virtual desktop services, IaaS and more. With deployments across the globe, Evolve IP provides cloud services in virtually every industry with specializations in the healthcare, finance, veterinary, retail, legal, and insurance verticals.