



Apigee Enterprise Cloud PCI

Add transactions to your APIs, while protecting your buyers and your reputation.

Most APIs begin life serving content.

Most APIs start out simply exposing content—information about your organization, products and services. These content APIs usually open up your brand and corporate data to developers, enabling new applications that take your data beyond the Web and onto the multitude of tablets and devices.

What content APIs usually do not provide is the ability to transact directly with your customer—to sell your goods and services and to monetize the new channels being opened by your developers.

Successful APIs quickly cross the compliance threshold.

As more developers build applications against your APIs, you may find that your API strategy evolves to include transactions. What was formerly a content interface now might include sensitive customer data—including credit card information—which exposes additional risk and is may put you in the crosshairs of industry regulation.

PCI DSS: Protecting customers in commerce transactions.

The Payment Card Industry Data Security Standard (PCI DSS) addresses the secure handling of cardholder information, such as credit card numbers, CVV, and personal information.

The goal of the standard is to minimize the risk of exposing cardholder data to compromise. It addresses the risks to data while crossing the network, and while it is stored in a database.

For those organizations seeking the benefits of deploying their APIs in the cloud, regulatory compliance presents a new set of challenges. When your transactions flow through cloud-based solutions, they are out of your control, and, hence they are beyond the control of your security and auditing teams—putting your overall PCI compliance at risk.

PCI DSS takes into account the physical location and procedures around IT infrastructure—a concept that at odds with a cloud topology. Unfortunately, PCI compliance cannot be obtained just by acquiring technology. Rather, achieving compliance involves technology in combination with operational procedures and

audits.

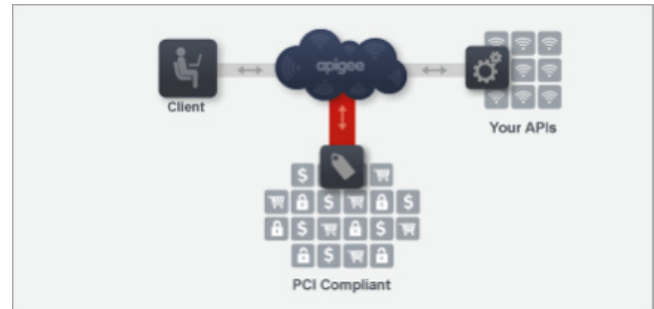


Fig 1. API management in the cloud: now PCI Compliant

Transact with your APIs in the cloud—and keep PCI compliance.

Apigee addresses the challenging requirements of cloud topology by delivering a fully PCI-compliant cloud API management solution, making it straightforward to pass PCI audits, while deriving all of the benefits of a cloud-based solution. Benefits include:

Deploy quickly - Deploy compliant cloud API management in as little as 1-2 weeks as a fully managed service that requires minimal overhead and effort.

Secure cardholder data – Ensure that no PCI-regulated data remains at rest in the cloud, and that it is appropriately masked, or encrypted at the message or transport level as it travels across the network.

Reach a global audience – Support global commerce initiatives for your APIs with multi-region international deployment.

Industrial-grade API management – Apigee Enterprise Cloud PCI gives you all of the enterprise-class visibility, control and scale of Apigee Enterprise over your APIs in a PCI-Compliant deployment option.

How it Works

Apigee Cloud PCI is a cloud API management solution deployed and managed in audited, PCI-compliant hosting facilities.

Apigee Enterprise Cloud PCI

API requests flow from consumer applications through the Apigee solution, and on to your APIs. Policies are applied to incoming request and outgoing responses according to business and operational rules, enabling sensitive data to be encrypted and masked for protection. Apigee logging policies can ensure that sensitive data is not logged in the cloud.

Additional offloaded functions include authentication and authorization (including OAuth), traffic management (rate limiting and distributed quotas), analytics, audit and other processing intensive operations.

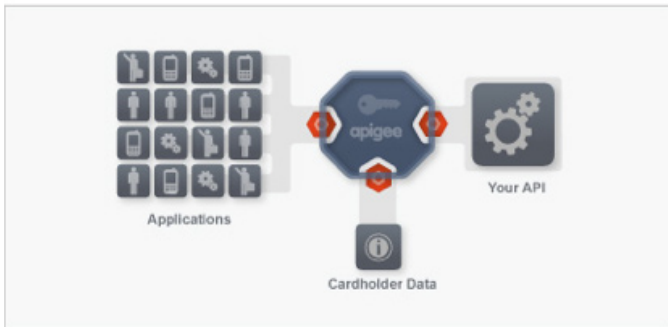


Fig 2. Security for cardholder data as it traverses the network to your APIs

A global solution

Apigee Enterprise Cloud PCI works with the Apigee API Delivery Network to provide PCI compliance for APIs that transact internationally. Combining intelligence at the edge with PCI compliance, Apigee API DN enables organizations to take multichannel commerce initiatives global.

Apigee on-premise PCI Compliance

Apigee also helps to ensure that the technology and procedures around your in-house API management comply with PCI.

Apigee Enterprise is also available as an on-premise solution that provides policy enforcement and auditing for your APIs that assist in PCI compliance.

Apigee controls access to your APIs using a variety of security mechanisms, and provides auditing over administrative access to the security configuration.

Apigee policies can ensure that no PCI-regulated data is stored,

by automatically masking data that matches patterns associated with cardholder data.

And if your applications call out to other systems, Apigee helps to ensure that they don't send more PCI data that is unnecessary, and can intelligently mask or encrypt such data as necessary.

Features

Apigee Enterprise Cloud PCI features deployment in audited PCI-compliant datacenters that address technical and operation requirements of PCI, including:

- Managed Firewall
- Web Application Firewall (WAF)
- Antivirus and Anti-malware
- Intrusion Detection
- Vulnerability Assessment & Notification
- Event Management
- Continuous Audit
- Change Control
- Patch Management
- Server Configuration and Management

Apigee Enterprise Cloud PCI is a deployment option of Apigee Enterprise.

Common Questions

What is the impact on my APIs and Client applications?

Apigee Enterprise Cloud PCI places no special requirements on your clients or APIs. Your clients can continue interacting with your APIs as they do today, except that traffic now flows through the Apigee Enterprise Cloud PCI solution.

Does this solution provide global coverage?

Yes, Apigee Enterprise Cloud PCI provides compliance for global eCommerce solutions with the Apigee API Delivery Network. The Apigee API DN delivers intelligence at the edge to enhance the speed and quality of international application delivery.

How does this fit into my current auditing procedures?

Apigee provides access to a Qualified Security Assessor (QSA) who can coordinate with your organization's QSA to document compliance.

For more information or sales inquiries, contact sales@apigee.com.

About Apigee

Apigee is the leading provider of API products and technology for enterprises and developers. Over 200 enterprises like Comcast, GameSpy, TransUnion Interactive, Guardian Life and Constant Contact and thousands of developers use Apigee's technology. Enterprises use Apigee for visibility, control and scale of their API strategies. Developers use Apigee to learn, explore and develop API-based applications. Learn more at www.apigee.com.

