VipeCloud Security, Privacy, and Architecture

Last Updated: June 5, 2016

VipeCloud's Corporate Trust Commitment

VipeCloud is committed to gaining and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including data submitted by customers to our services ("Customer Data").

Services Covered

This documentation describes the architecture of, the security and privacy-related audits and certifications received for, and the administrative, technical, and physical controls applicable to the services branded as VipeCloud (the "VipeCloud Services").

Third-Party Architecture

The infrastructure used by VipeCloud to host Customer Data submitted to the VipeCloud Services is provided by a third party provider, Amazon Web Services, Inc. ("AWS"). Currently, the infrastructure hosted by AWS in provisioning of the VipeCloud Services is located in the United States.

Information about security and privacy-related audits and certifications received by AWS, including information on ISO 27001 certification and Service Organization Control (SOC) reports, is available from the AWS Security Web site and the AWS Compliance Web site.

Some of the email related functionality is provided by SendGrid, Inc. ("SendGrid") and Nylas, Inc. ("Nylas"). Information about security and privacy for SendGrid and Nylas can be found on SendGrid's Security Web site and Nylas' Web site.

Additionally, a portion of customer support for the VipeCloud Services is provided using third-party technology, which may contemplate data, including screenshots of customers' instances of the VipeCloud Services, being hosted on the third-party's infrastructure.

Security Controls

The VipeCloud Services include a variety of security controls. These controls include:

- Unique user identifiers (user IDs) to ensure that activities can be attributed to the responsible individual;
- Password length controls;
- Password complexity requirements for Web and mobile access to the VipeCloud Services.

Security Procedures, Policies and Logging

The VipeCloud Services are operated in accordance with the following procedures to enhance security:

- User passwords are stored using a salted hash format and are never transmitted unencrypted;
- User access log entries will be maintained, containing date, time, URL and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by a customer or its ISP;
- Passwords are not logged under any circumstances.

User Authentication

Access to the VipeCloud Services, directly or via the VipeCloud API, requires a valid user ID and password combination, or an API key/secret, both of which are encrypted via TLS while in transmission. Following a successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

Physical Security

Production data centers used to provide the VipeCloud Services have systems that control physical access to the data center. These systems permit only authorized personnel to access secure areas. The facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around-the-clock guards, physical access screening and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure. Further information about physical security provided by AWS is available from the AWS Security Web site, including AWS's overview of security processes.

Reliability and Backup

All networking components, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the VipeCloud Services is stored on a primary database server that is clustered with a backup database server for higher availability. All Customer Data submitted to the VipeCloud Services is backed up daily.

Viruses

The VipeCloud Services do not scan for viruses that could be included in attachments or other data uploaded into the VipeCloud Services by customers.

Data Encryption

The VipeCloud Services use industry-accepted encryption products to protect Customer Data and communications at rest and during transmissions between a customer's network and the VipeCloud Services, including 256-bit TLS Certificates and 256-bit AES encryption at a minimum.

Return of Customer Data

During the contract term, customers may export a copy of any Customer Data made available for export through the VipeCloud Services. Within 30 days post contract termination, customers may request return of their respective Customer Data, to the extent such Customer Data can be copied and exported from the VipeCloud Services and the ability to export such data is generally made available to customers, by contacting support@vipecloud.com.

Deletion of Customer Data

After contract termination, to request deletion of Customer Data submitted to the VipeCloud Services, contact us at support@vipecloud.com. After such deletion is initiated by VipeCloud, Customer Data will remain in inactive status on back-up media for 90 days, after which it will be overwritten or deleted. This process is subject to applicable legal requirements.

Without limiting the ability for customers to request return of their Customer Data submitted to the VipeCloud Services, VipeCloud reserves the right to reduce the number of days it retains such data after contract termination. VipeCloud will update this VipeCloud Security, Privacy, and Architecture Documentation in the event of such a change.

Sensitive Personal Data

Important: The following types of sensitive personal data may not be submitted to the VipeCloud Services: government issued identification numbers; financial information (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers); personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life; information related to an individual’s physical or mental health; and information related to the provision or payment of health care.

For clarity, the foregoing restrictions do not apply to financial information provided to VipeCloud for the purposes of checking the financial qualifications of, and collecting payments from, its customers, the processing of which is governed by the Web Site Privacy Statement for the VipeCloud Services.

Tracking and Analytics

VipeCloud may track and analyze use of the VipeCloud Services for the purposes of security and helping VipeCloud improve both the VipeCloud Services and the user experience in using the VipeCloud Services. VipeCloud may also use this information and users’ e-mail addresses to contact customers or their users to provide information about the VipeCloud Services. Without limiting the foregoing, VipeCloud may share data about VipeCloud customers' or their users' use of the VipeCloud Services (“Usage Statistics”) to VipeCloud’s service providers for the purpose of helping VipeCloud in such tracking or analysis, including improving its users’ experience with the VipeCloud Services, or as required by law.