PipelineDeals

Security Best Practices

2019

Table of Contents

Overview

At PipelineDeals, the security of our application and our customers' data is the top priority.

We use industry best practices to establish and maintain a secure online experience. And we always remember that your data is *your* data. We never touch your data without your explicit permission, and we make it easy to export it whenever you want.

Standards and Certifications

Type 1 Soc 2

Cyber security and compliance firm A-Lign Inc certified PipelineDeals as SOC 2 compliant in September 2017. This means they examined our Sales CRM Services System and certified the suitability of the design of controls to meet the criteria for the Security, Availability, and Confidentiality principles set forth in TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids) (applicable trust services criteria).

GDPR

At PipelineDeals, we value our customers' success, and understand the importance of knowing that personal data is being protected.

PipelineDeals hired both US-based and EU-based legal counsel to work closely with us to ensure complete GDPR compliance. We worked with our legal counsel and internal teams to create a GDPR compliance policy that addresses each relevant requirement that PipelineDeals must comply with. To this effect, PipelineDeals addressed the GDPR requirements that are applicable to data processors.

We amended our policies and implemented procedures to make them GDPR compliant. These changes include, but are not limited to, policies relating to data processing, information security, transition, third party processors, data protection and breach notification. We also made changes to our Terms of Use, Privacy Policy, and introduced a Data Processing Agreement. We require all PipelineDeals' employees to complete additional data privacy and security training that is GDPR focused. PipelineDeals will keep customers informed of any and all changes as they progress.

Data Center Security

PipelineDeals is fully cloud hosted by Amazon Web Services. PipelineDeals can provide Amazon's public SOC 3 report for an overview of their SOC II compliance upon request.

Operations Security

Production System Access

Amazon VPC

> Once the data arrives from the user's browser to our Amazon Web Services infrastructure, it hits our AWS VPC. There are no VPN's connected to the VPC. We only allow SSL access to any machines within the VPC.

Bastion Host

> Access to any production machine is only allowed through a bastion host. Users must SSH into the hardened bastion, and from there are relayed to the other machines. All access to the bastion is logged and audited.

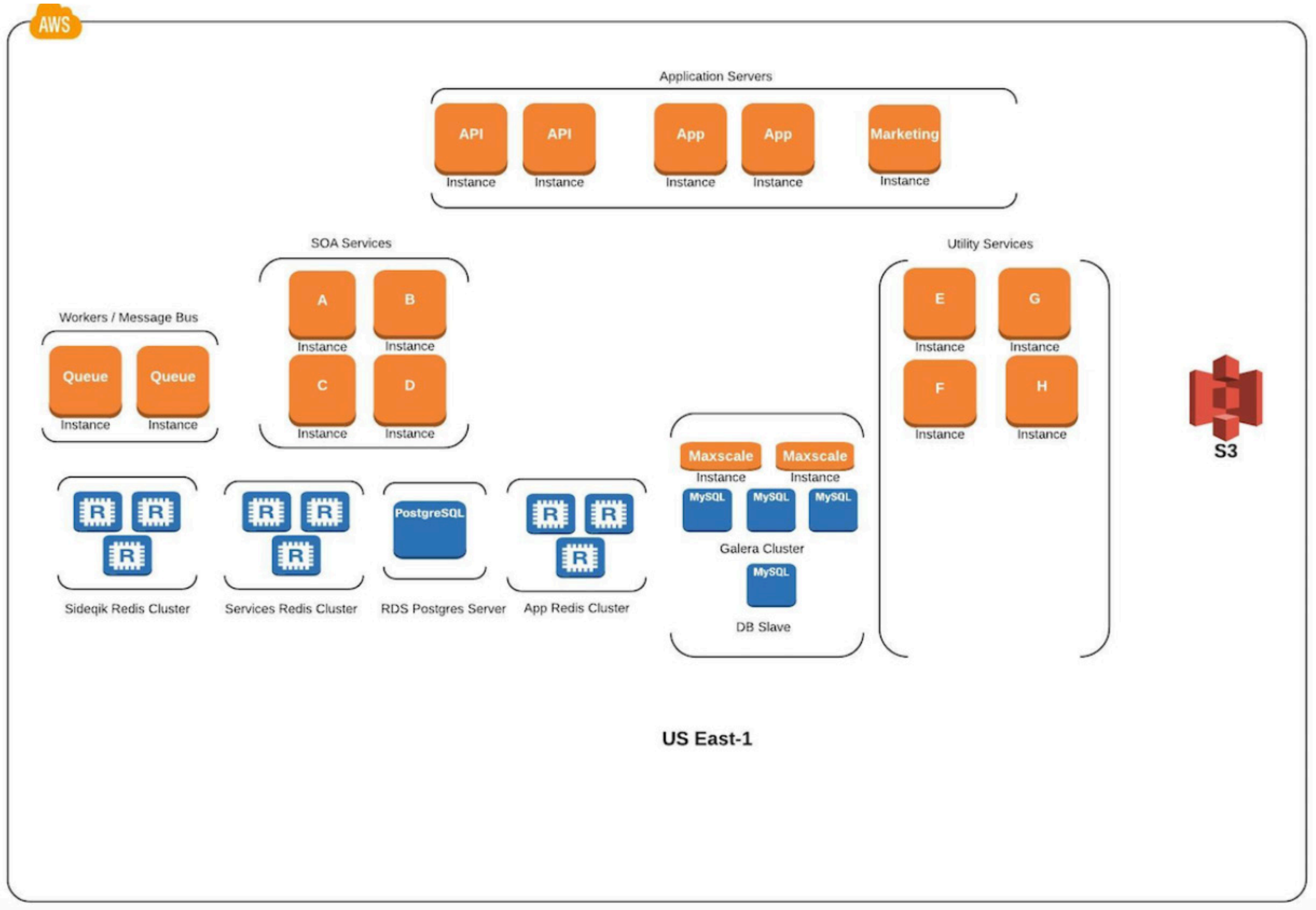
Application Architecture and Security

Application Architecture

PipelineDeals' SaaS application is a Ruby on Rails and Javascript web application hosted on Amazon Web Services. It uses a multi-tier architecture that includes Service Oriented Architecture for supporting web services.

The databases are **multi-tenant** Galera clusters built for high availability and redundancy. All customer data is stored in a single multi-tenant MySQL database.

See diagram on next page.



Application Security

User Authentication — Web

User credentials are stored in a MySQL database using a one way SHA512 hashing algorithm and random salted password.

PipelineDeals is flexible with the password criteria built into the app, recognizing that various clients want different levels of strictness based on their business, so we have a 8 character minimum with a mix of numerical and special character requirements. We recommend to our customers to create their own much stricter policies for the users they create within the application.

User Authentication — API

API authentication is handled through an API key granted within the admin section of a customer's account. API access (and thus the key) is all encrypted via standard HTTPS over SSL.

Payment and Billing Data

PipelineDeals does not store any billing or credit card information on our systems. It is protected via HTTPS and is sent and retrieved via our billing partner, Zuora.

Zuora supports customers in successfully meeting the requirements of many certifications and regulatory demands of their industry or governing agency. The support includes the compliance in the following:

- SOC 1 Type 2 and SOC 2 Type 2 examinations
- PCI DSS Level 1
- ISO 27001
- Data Privacy Management Platform (TRUSTe)
- EU-U.S Privacy Shield and Swiss-U.S. Privacy Shield
- HIPAA

User Uploaded Data Files

Any data files that are uploaded by users of the application are stored in encrypted AWS S3 buckets and uses server side encryption with Amazon Key Management Service.

Customer Data

At Rest

> Our application customer data at rest is all encrypted using standard AWS RDS encryption and AWS EBS Encryption and utilizes Amazon Key Management Service for encryption key management.

In Transit - SSL

> All data that is transported between our users' devices and our application are encrypted via HTTPS over SSL. When you log into PipelineDeals, you are connected via a 256 bit extended-validation SSL security certificate provided by Cloudflare via Comodo Cybersecurity. This type of secure connection is comparable to the online security provided by many major banks and financial institutions. The encryption key is RSA 2048 bits with an encryption algorithm using SHA256 with RSA.

Availability

PipelineDeals builds an engineering culture based on operational excellence. We take pride in our uptime capability through the redundant infrastructure and deployment process we have built. **Our 12-month availability rate is 99.99%.**

System & Network Security

Access Audit

By using a bastion host (jump host) into all production machines, we capture all access into all machines within our production environment and routinely view for anomalies.

Cloudflare Web Application Firewall

PipelineDeals uses several technologies provided by the Cloudflare, a leading internet performance and security company to provide even deeper levels of protection and speed to our customers.

DDoS Prevention

Cloudflare provides PipelineDeals with unmetered Distributed Denial of Service attack mitigation to maintain performance and availability. Cloudflare can prevent DDoS attacks because an extremely large portion of all internet traffic is routed through them. Cloudflare's network capacity is 15x bigger than the largest DDoS attack ever recorded. With 20 Tbps of capacity, it can detect any modern distributed attack before it can affect our servers.

Web Application Firewall

We use Cloudflare's enterprise-class web application firewall (WAF) which protects our applications from common vulnerabilities like SQL injection attacks, cross-site scripting, and cross-site forgery requests with no changes to your existing infrastructure.

Malicious Bot Blockage

Cloudflare prevents bots from excessive usage and abuse across our websites, applications, and API endpoints.

Rate Limiting

Cloudflare Rate Limiting protects against denial-of-service attacks, brute-force login attempts, and other types of abusive behavior targeting the application layer.

Patch Management

PipelineDeals is committed to ensuring that all of our systems have the latest security patches and updates. Therefore, we leverage Amazon Inspector to scan all of our servers in the cloud for vulnerabilities.

Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

We have created an automated system for regularly updating patches on servers. Our deployment process always builds a brand new server in AWS which has the latest hardened OS and patches. Once running, the servers self update with the latest patches.

Intrusion Detection System

Along with Cloudflare, PipelineDeals also leverages Amazon GuardDuty. GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior against our AWS accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. GuardDuty also detects potentially compromised instances or reconnaissance by attackers.

External Security Tests

PipelineDeals is committed to conducting external penetration tests by 3rd party security firms at a minimum of once a year.

Web Application Penetration Test

Web Application Assessment incorporates the Web Application Vulnerability Assessment and attempts to exploit our applications, highlighting the underlying flaws. Web Application Assessments utilize the PTES Penetration Testing Methodology for a defined, repeatable, and high-quality assessment. This process utilizes both commercial and proprietary tools to analyze and test the security of web applications. These industry-standard tools, such as BurpSuite and Metasploit, are used for the initial mapping and reconnaissance of the site, as well as aiding in vulnerability scanning.

For unique vulnerabilities, custom tools and scripts are created and utilized as well. Once enumeration and vulnerability data has been collected, the manual analysis piece begins.

At this point, assessors attempt to leverage discovered vulnerabilities and test for key security flaws, including the OWASP Top 10 Vulnerabilities:

1. Injection Flaws
2. Broken Authentication and Session Management
3. Cross Site Scripting (XSS)
4. Insecure Direct Object Modules (DOM)
5. Security Misconfigurations
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. Cross-Site Request Forgery (CSRF)
9. Components with Known Vulnerabilities(Libraries, Frameworks, etc.)
10. Invalidated Redirects/Forwards

External Network Penetration Testing

External AWS testing utilizes the PTES penetration testing methodology for a structured, repeatable assessment. With Amazon's approval, the auditor implements a range of scanning and enumeration tools to fingerprint the targets. The auditor gathers information on perimeter systems, focused on AWS instances and APIs. The security analysts then filter the information and port it to a vulnerability scanner, using industry-standard techniques to identify potential weak-points in these systems. The list of vulnerabilities accompanies manual analysis, testing, and verification. Using a variety of techniques and a vast internal knowledge base, they then attempt to exploit identified flaws safely. We do so to highlight and demonstrate the associated level of risk.

The following are types of vulnerabilities that may be identified during the verification and exploitation phase:

- Misconfigured AWS S3 Buckets
- Weak AWS Identity / Access Management settings
- Hardcoded API keys
- Remote Code Execution (RCE) - buffer/ stack overflows, off-by-one errors
- Insufficient patching/updating

- Weak and reused passwords
- Web & application server vulnerabilities
- Database server vulnerabilities
- Weak encryption algorithms
- Usage of insecure/unencrypted protocols

Disaster Recovery and Backups

Live DR Tests

Annually, PipelineDeals runs through at least one live Disaster Recovery test. The goal is to provide a live site with no data loss in a completely different AWS Region. Our primary AWS region is in the East, Virginia. The failover is in the West, Oregon. We exercise all of our automated operations scripts to spin up machines against real time database replicas. This ensures all of our procedures and backups are accurate.

Tabletop DR Tests

Annually, PipelineDeals runs through all of our DR plans and processes and runs a risk assessment against each plan. This ensures our process has not become stale and we know exactly where and at what level any risk to the business lives.

Backups

At any one time we have 5 full copies of data backed up in real time:

- All data volumes are backed up to encrypted volumes in AWS six times daily.
- We run a 3 cluster database configuration with each node in the cluster in a different availability zone.
- We run a slave DB off of the 3 cluster master.
- We run a database replica outside of the Galera cluster in different regions for geographical redundancy
- We push database snapshots to both separate AWS accounts and separate AWS regions daily.

Employee Security

Device policy

- Set screensavers with 5 minute lock
- Encrypted hard drives required via FileVault
- iCloud Find My Mac is enabled for remote wiping of data
- Multi-Factor Authentication required.

Employee Password Policies

Required to use Lastpass password manager to create non-repeated strong passwords (Two factor authentication into Lastpass is required.)

Security and Compliance Training

All employees go through an annual security and privacy training.

Social Engineering Tests

PipelineDeals conducts Social engineering penetration testing as well. This is the practice of attempting typical social engineering scams on our employees to ascertain the organization's level of vulnerability to that type of exploit.

Social engineering pen testing is designed to test employees' adherence to the security policies and practices defined by management. Testing provides PipelineDeals with information about how easily an intruder could convince employees to break security rules or divulge or provide access to sensitive information.

Coding Practices

QA and Testing

PipelineDeals has a very DevOps oriented culture that is built around a Continuous Integration/ Continuous Deployment (CI/CD) pipeline to allow for production releases as soon as code is ready. We use test automation tools such as rspec, Cypress.io, and Circle CI to ensure code is tested immediately upon being committed to the repository.

We also run security monitoring tools to inspect our code for security bugs in real time.

All code is peer reviewed prior to going to production using Github Pull Requests as the method for communication and review.

Questions?

Talk to a real person at **+1-866-702-7303**.