Security, Risk, and Compliance: Engine Yard

WHITE PAPER

ENGINEYARD.COM / 1-866-518-9273

Table of Contents

Engine Yard Overview

Engine Yard Cloud Platform as a Service--commonly referred as PaaS--is built on top of Amazon Web Services IaaS (Infrastructure as a Service). When you create an instance with Engine Yard, you are booting up an EC2 (Elastic Compute Cloud) instance. Engine Yard boot this instance for our Customers, automatically configuring it with the appropriate Engine Yard stack components for your environment. Other Engine Yard software handles key functions including cluster management, load balancing, high availability, database replication, and monitoring and alerting.

Instances on Engine Yard Cloud are dedicated to running your Ruby, Node.js, or PHP application in the cloud. Instances can be configured to serve your application tier, database tier, cache tier, background processing and utilities, and more. Instances are available in various configurations to meet your CPU, memory, and disk space needs.

Security Commitment

Engine Yard is committed to maintaining a safe and secure platform for our Customers, business partners, and the broader Internet community. Engine Yard has developed an in-house information security and compliance function that complements the controls that our IaaS provider, AWS, provides.

The following information is based off an internal assessment of Engine Yard Cloud to the ISO 27002 2005 Standard control objectives.

Shared Responsibility

An Engine Yard Customer cluster is isolated from other Customer clusters, and is a self-contained environment that includes compute, storage, and database services. No functionality is shared between virtualized instances. In our single tenancy model, Customers own and operate their own instances, including full administrative access, much like a server that is racked in a data center. Because of this, Engine Yard, our IaaS providers, and our Customers jointly share security responsibilities across different domains. These responsibilities include:

IaaS Provider (AWS)

- Virtualization layer
- Network security (including DDOS, spoofing, and port scanning mitigation)
- Physical and environmental security

More details on AWS's security can be found at: **https://aws.amazon.com/security**

PaaS Provider (Engine Yard)

- Operating system security
- Database security
- Network security (ports/protocols)
- Vulnerability management (including testing and patching)
- Support access

Customer

- Access Control
- Application code (nonplatform related)
- Compliance

It is possible for Customers to enhance their security and/or meet more stringent compliance requirements by working with Engine Yard to add third party technologies such as host based firewalls, host based intrusion detection/prevention systems, two-factor authentication, encryption, and key management. The nature of this shared responsibility can provide Customers flexibility in meeting industry-specific certification requirements.

Security Policy Management

Policies are important for setting the tone and direction of the organization, establishing clear responsibilities, and demonstrating accountability to our stakeholders. Engine Yard takes information security seriously and has established Information Security policies that include requirements on:

- Information security objective and scope
- Information security roles and responsibilities
- Policy development, maintenance, and distribution
- Information classification
- Internet usage
- Access management
- Customer data protection
- Risk management
- Compliance

Engine Yard's Security and Operations (SecOps) Team owns Information Security policies and delegates multiple operational responsibilities to different members. Information security policies are reviewed annually, and updated as necessary to address new threats or findings from our risk assessment process. Information security policies are required to be read and acknowledged via signature by all Company personnel. Policies are published on our internal wiki, and are available to all Company personnel.

Security Responsibilities

Engine Yard has made an active commitment to information security through the establishment of an information security and compliance function that reports directly to the CEO. The responsibility for the Company's information security strategy and related projects is allocated to the Senior Governance Risk and Compliance Analyst. This function's charter is to protect the confidentiality, integrity, and availability of Engine Yard's data and computing assets. This includes data that may be housed internally, as well as information that may be shared with external parties. The primary responsibilities of the information security and compliance organization include:

- Security governance
- Security architecture
- Security strategy
- Vulnerability management
- Incident response
- Security awareness
- Risk assessment and audit
- Vendor due-diligence
- Compliance
- Information security community involvement
- Customer concerns and tickets related to security and compliance

Engine Yard has allocated engineering staff to develop, test, and deploy security projects for the Company. Additionally, many of Engine Yard's support engineers are formally security-trained, and have attained the CISSP certification--the industry's de facto security credential.

Engine Yard performs regular risk assessments. The scope of these assessments varies, and, depending on the need, is performed either in house, or by a third-party. Keeping up to date on the latest developments is important to Engine Yard, and the Company is involved with a number of cloud security organizations. Additionally, Engine Yard maintains relationships with a number of other Company's security organizations; often granting us immediate notice of security issues.

External Parties

External parties whom Engine Yard may share sensitive data with are required to sign a nondisclosure agreement with Engine Yard prior to any conversations. External third parties Engine Yard may directly contract with are required to go through our vendor security due-diligence process. Prior to moving forward, all high-risk findings must be mitigated to a level acceptable to Engine Yard.

Information Classification

For simplicity, Engine Yard has established three levels of information classification for the organization that applies everywhere that data is stored. Our standard includes requirements, by classification level, for protecting data in transit, data at rest, access, and the handling of information. These classification levels are as follows:

Classification:	Definition:
Public	Intended for public consumption. For example, marketing materials or the public website.
Internal Use Only	Disclosure is not welcome, but would not cause an adverse impact to the Company or personnel.
Sensitive	Requires special precautions to ensure the integrity and confidentiality of the data by protecting it from unauthorized modification or deletion. Requires higher than normal assurance of accuracy and completeness. If information is shared with a third-party, requires the signing of the Engine Yard NDA.
Confidential	For use within the Company only. Unauthorized disclosure of data could seriously affect the Company.

Asset Management

Engine Yard maintains an inventory of information technology tools that include: tool ownership, information classification level, and any specific access or data protection requirements.

Human Resources Security Management

Background Checks

Engine Yard performs a background check on any new Company personnel (including full-time employees, part-time employees, and contractors). This check evaluates past criminal and social media history along with reference validations.

Security Training

During new hire employee onboarding, security awareness training is given that addresses each employee's security responsibilities. Topics include:

- Importance of policies
- Ensuring customer data protection
- Corporate security considerations including confidentiality of information, the use of social media, and intellectual property protection
- Understanding common logical threats including malware and phishing
- Understanding physical threats
- Importance of laptop security measures including hard drive encryption, VPN access, and regular patching
- Reporting security incidents

Off-boarding

Engine Yard has assigned individuals with the responsibility to off-board terminated Company personnel. This process includes notifying IT of the termination, removing logical access to IT systems, removing any SSH public keys from the Engine Yard Cloud, and ensuring that all Company assets are returned.

Physical and Environmental Security Management

Engine Yard does not host Customer data in its corporate or remote offices, but rather in AWS data centers that have been certified to meet industry security standards. AWS provides the physical and environmental controls for data centers that handle Engine Yard Customer data.

Physical Controls

Customer Data Locations

Engine Yard's physical infrastructure is hosted and managed by AWS via their secure data centers. AWS continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. AWS's data center operations have been accredited under:

- ISO 27001
- SOC 1/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

AWS has years of experience in designing, constructing, and operating large-scale datacenters. They operate the following controls:

Area:	Controls:
Physical Security	• AWS datacenters are housed in nondescript facilities. • Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. • Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. • All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. • AWS only provides datacenter access and information to employees and contractors who have a legitimate business need for such privileges. • When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. • All physical access to datacenters by AWS employees is logged and audited routinely.

Physical and Environmental Security Management

Area:	Controls:
Fire Detection and Suppression	• Automatic fire detection and suppression equipment has been installed to reduce risk. • Fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. • Data center environments are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.
Power	• The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. • Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. • Data centers use generators to provide backup power for the entire facility.
Climate and Temperature	• Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. • Data centers are conditioned to maintain atmospheric conditions at optimal levels. • Monitoring systems and data center personnel ensure temperature and humidity are at the appropriate levels.
Management	• Data center staff monitor electrical, mechanical and life support systems and equipment so issues are immediately identified. • Preventative maintenance is performed to maintain the continued operability of equipment.

Physical and Environmental Security Management

Engine Yard Corporate Location

Engine Yard's corporate headquarters building is located in a shared physical facility. The building's entrance is kept locked during non-business hours, and is further protected by a security guard 24 hours a day, seven days a week. Security cameras are visibly placed in high trafficked or sensitive locations. During regular business hours, the office doors are open and monitored by a front desk personnel. During off hours, Engine Yard doors require badge access prior to granting entry. Local police enter and look for suspicious activity three times each night. All doors are alarmed and will alert our vendor and the police if a disturbance is detected. Physical access is audited every quarter.

Hard copy Customer receipts and invoices are stored in locked file cabinets that are only accessible by the Finance department. Shredders are available to employees to securely dispose of sensitive information.

Emergency Response

Engine Yard maintains an emergency response plan. The vast majority of our Customer and internal tooling is run from the Cloud, so the Customer impact of a physical or environmental threat to our corporate headquarters is considered low. Still, Company personnel's safety and availability are mission critical. Engine Yard stores a significant amount of food, water, and health supplies for emergency purposes. Additionally, Human Resources maintains an emergency contact list to aid in locating personnel in the event of an emergency. Engine Yard has employees spread across the globe to maintain 24/7 Customer support.

Development & Testing

Engine Yard employs pair programming and review, as well as continuous integration tools to perform automated bug testing. Multiple staging environments have been established to facilitate manual testing. Additionally, a formalized and independent Quality Assurance (QA) function is established at Engine Yard. This organization performs structured testing when a major function, feature, or higher risk change is to be introduced into our environment. As an agile development shop, Engine Yard maintains processes and tools to roll back changes in case problems arise from a production deployment.

Engine Yard engages qualified and reputable third parties to perform penetration tests against key application interfaces. The frequency and areas of testing are commensurate with known risk. Third-party testing traditionally occurs when major changes are introduced that could impact Customer data locations (for example the Customer's dashboard), or when a particular application or interface has not been tested recently. The scope of the assessment includes code review as well as controlled attacks against Engine Yard's replicated production environment. As issues are discovered, tickets are filed and remediation is initiated. After fixes are implemented, the third-party conducts retests to ensure that significant risks are mitigated and that no new security weaknesses were introduced during remediation efforts.

Malware Mitigation

Engine Yard's IT consists of a combination of Linux and Apple OSX operating systems. While malware has not traditionally been a significant threat to the security of these systems, Engine Yard is aware that no platform is invulnerable to a malicious attack. To combat these threats, the information security and compliance function receives feeds from various information resources including newsgroups, blogs, and security-focused web sites. When a threat is discovered, the SecOps Team evaluates the issue to determine impact and likelihood, and establishes a mitigation approach. For any high-risk vulnerability, a communication is sent out to all Engine Yard personnel discussing the issue, the steps necessary to test for the issue, and the recommended fix. Additionally, Engine Yard employees are encouraged to install only reputable software, to regularly patch their preferred browser, and to regularly run Mac OS's Software Update.

Snapshots and Backups

Application code and databases are written out to persistent storage volumes. Engine Yard automatically mounts these volumes and takes backups for our Customers. Both the data mount on the application master instance and the database mount on the database master instance(s) are persistent. Engine Yard takes advantage of AWS's EBS storage allowing Engine Yard to take regular disk snapshots of both of these volumes. If the need arises to ever rebuild instances from scratch, the Customer has the ability to restore both of these volumes from previous snapshots.

Engine Yard utilizes AWS's S3 service for backups. By default, database backups are taken daily and are rotated every 10 days. However, Customers can customize their backup schedule to meet their needs within the dashboard. If a requirement, backups can be stored using PGP encryption.

Data Retention and Destruction

Engine Yard Customers have the freedom to define what data applications store and the ability to purge data from databases to comply with any data retention requirements. If a Customer deprovisions an application and the associated database, Engine Yard maintains the database's storage volume for 90 days after which time it's automatically destroyed rendering the data unrecoverable.

Decommissioning hardware is managed by AWS using a process designed to prevent Customer data exposure, including techniques outlined in DoD 5220.22-M ("National Industrial Security Program Operating Manual") and NIST 800-88 ("Guidelines for Media Sanitization") to destroy data.

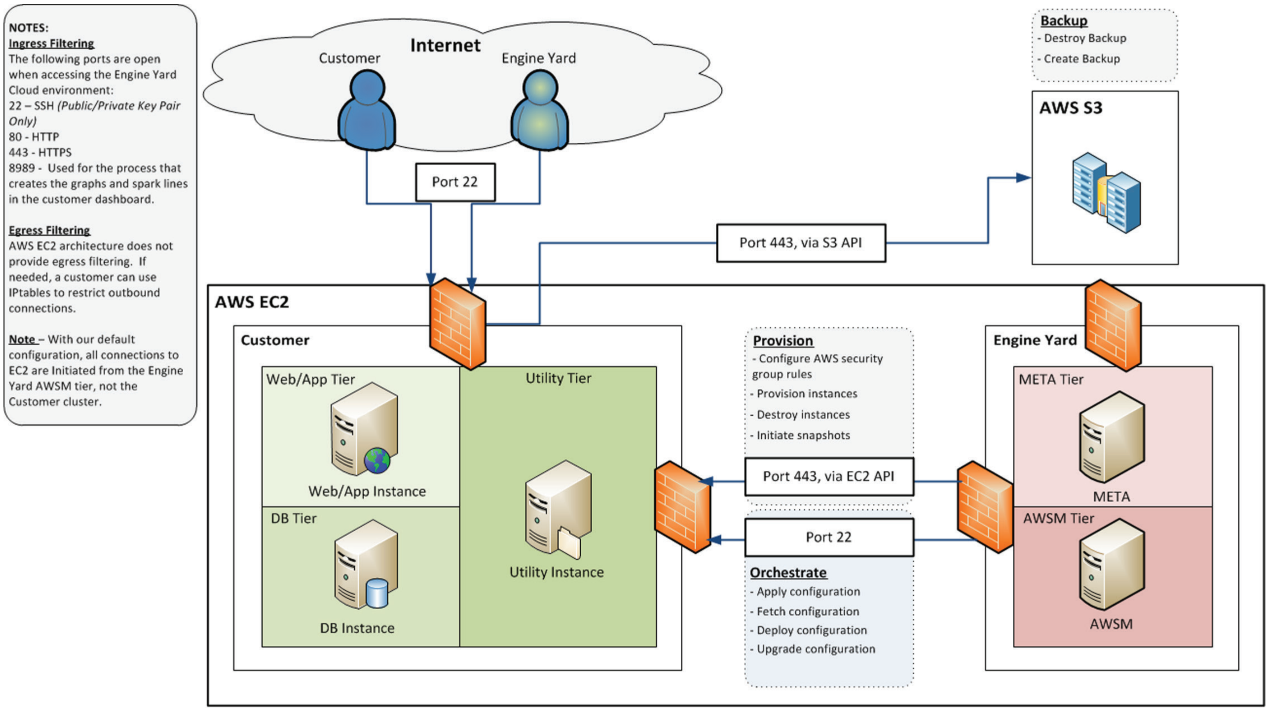
Network Security

AWS provides network security controls, while Engine Yard performs the configuration of the AWS security groups.

Firewalls

Each Customer cluster is protected by an AWS security group, which provides ingress network filtering from the broader Internet. By default, all access is denied with only explicitly defined ports (22, 80, 443, 8989) and protocols permitted

to enter the Customer environment. Database ports are not exposed to the Internet. Additionally, Customers can choose to configure a host-based firewall (with IPtables being the most commonly used) to further isolate traffic on individual instances. See below diagram for a visual representation of the Engine Yard Cloud environment.



NOTES:
Ingress Filtering
The following ports are open when accessing the Engine Yard Cloud environment:
22 – SSH *(Public/Private Key Pair Only)*
80 - HTTP
443 - HTTPS
8989 - Used for the process that creates the graphs and spark lines in the customer dashboard.

Egress Filtering
AWS EC2 architecture does not provide egress filtering. If needed, a customer can use IPtables to restrict outbound connections.

Note – With our default configuration, all connections to EC2 are Initiated from the Engine Yard AWSM tier, not the Customer cluster.

Distributed Denial of Service (DDoS) Mitigation

Engine Yard relies on AWS's proprietary DDoS mitigation techniques to lessen our Customer's exposure to successful DDoS attacks. Also, AWS's networks are multi-homed across a number of ISPs to provide further Internet access diversity. Further DDoS mitigation can be expanded through the use of third-party services.

IP Spoofing

Engine Yard instances are unable to send spoofed network traffic. The AWS-controlled firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.

Port Scanning

AWS maintains the capability and responsibility for detecting illicit port scans against Engine Yard Customer environments. When unauthorized port scanning is detected, AWS blocks the scan and notifies Engine Yard via their abuse process. Port scans of Engine Yard instances are generally ineffective because, by default, the majority of inbound ports on Engine Yard instances are closed.

Engine Yard has an established arrangement with AWS that permits our Customers to conduct vulnerability scans against their environments in order to meet their specific security or compliance requirements. Customers can file an Engine Yard ticket to start this process.

Packet Sniffing

The AWS virtualized infrastructure prevents a virtual instance, running in promiscuous mode, to receive or "sniff" traffic that is intended for a different virtual instance. While Customers could place their interfaces into promiscuous mode, the hypervisor will not deliver traffic that is not explicitly addressed to them. Even two virtual instances that are owned by the same Customer located on the same physical host cannot listen to each other's traffic. Attacks such as ARP cache poisoning do not work within the Engine Yard environment.

E-commerce Services

All connections to Engine Yard applications services are over SSL using high-grade encryption (128 bit, RC4). Our billing page transparently redirects to Braintree for payment processing services. Engine Yard does not receive, process, or store Customer credit card information within its infrastructure.

Password Controls

Customers establish, upgrade, and monitor their computing clusters via the Engine Yard dashboard. Access to this information is confidential, and requires a strong username and password to gain access. Engine Yard requires that all dashboard passwords be:

- At least 8 characters long
- A mixture of numbers, letters, and symbols or spaces

To perform a password reset, a user must know the email address that the account was signed up with. A reset email will be sent to the email address on file, which is time-limited, and can be used one time only.

Logging and Monitoring

Logs are created and stored on the individual instances, and are available for the Customer to review. Engine Yard syncs our clocks with AWS using NTP to ensure log integrity across instances. Engine Yard maintains extensive logs including those specific to the application, operating system, and database layers. From a security perspective, this includes syslog, auth.log, HTTP connections to application logs, and writes to the database server.

By default, the infrastructure is using logrotate to rotate and archive old logs. Customers can configure logrotate to fit their needs. Additionally, utility instances or a third-party service can be used to enhance logging analytics and centralized storage.

Internal Tools Access

Engine Yard information systems contain data that is crucial to our ongoing operations. The Company has an obligation to protect such data from inappropriate disclosure. To that end, Engine Yard IT maintains a list of internally used applications, along with the application's designated owner. Application owners are responsible for maintaining the user access lists and authentication subsystems for their assigned applications. For any given application, each user is assigned an account for their exclusive use, and access

to all applications must uniquely identify the individual and, at a minimum, require a valid password before granting access.

Managers or supervisors are responsible for reviewing access granted to Company personnel to ensure access rights are current and accurate. Managers or supervisors have the rights to request access grants or revocations. Access must be removed within 24 hours of revocation notice.

The information security and compliance function reviews access on a regular basis, including when someone leaves the Company. Access to systems is based on the security principles of "least privilege" and "need to know".

Customer Environment Access

Engine Yard is absolutely committed to keeping our Customer's data protected at all times. Customer data is considered "confidential" information and is handled securely by our Company personnel. Customer data is not copied to employee computers or any other Company assets. Any troubleshooting that needs to be performed on Customer data is performed in the Customer's environment. When Company personnel access Customer environments a ticket is generated indicating that Support accessed the instance, why the interaction was necessary, and what work was performed.

Engine Yard utilizes an internal tool to allow support engineers to request

and provision access to Customer environments. This tool places the support engineer's SSH key on the instance and notifies the engineer when this action is complete. All requests to place SSH keys are logged and the history is maintained in a central system. Actions by Company personnel on a Customer's system are limited to resolving the Customer need, and nothing more. Once a Customer is satisfied with the result, and the ticket is closed, access is automatically removed following the next chef run.

Customers manage their own organization's access to the Engine Yard dashboard, and their instances. Customers can create multiple accounts and are aligned with two specified roles:

"Owner" role	• Is associated with one user and is considered the administrative role for the account. • Can invite and remove users to the account. • Can update billing information. • Can file a ticket to promote a "Member" to "Owner". • Can upload SSH public keys and assign them to a specific account.
"Member" role	• Can be associated with many user accounts. • Can invite and remove users to the account, but cannot impact the "Owner". • Can upload SSH public keys and assign them to a specific account.

To maintain authentication security and eliminate the threat of brute force attacks, Engine Yard does not allow SSH password authentication. Additionally, Customers must first connect to their operating system environment, prior to authenticating to their DBMS.

VPN Access

Engine Yard grants Company personnel VPN access back to the corporate HQ. This connection provides a fully encrypted tunnel that restricts the client to the corporate HQ Internet Gateway for outbound connections. This control allows our global support team, and traveling employees to utilize a trusted network connection when working from an untrusted location. All crucial applications that impact our Customers need to be accessed through a trusted site (our offices) or through VPN.

Network Access

Engine Yard uses wireless networking at its corporate HQ, and remote locations. Engine Yard has established both "guest" and "corporate" networks to segment sensitive corporate traffic, from public traffic. Wireless networks utilize WPA2 encryption, and keys are rotated on a quarterly basis.

Security Architecture

Engine Yard continually looks to improve and enhance its security architecture. Engine Yard subscribes to the PDCA (Plan, Do, Check, Adjust) cycle, a tenet of the ISO 27001 Information Security Management Standard. Through this process, Engine Yard has developed a security strategy (Plan) and related security projects (Do) that address risks identified during the annual risk assessment process (Check). Additionally, new Engine Yard architecture projects involve the information security and compliance function to assist with risk assessment and controls design in order to mitigate risk to an acceptable level.

Laptop Security Controls

Engine Yard exclusively uses Mac laptops within the corporate environment. To maintain the security and integrity of our workforce and data, Engine Yard has implemented the following controls:

- Hard drive encryption
- Password locked “Administrator” account
- Standardized password authentication requirements
- VPN access
- Remote backups

Vulnerability Management

Engine Yard utilizes the Gentoo Linux distribution to host Customer applications. The Gentoo Foundation demonstrates their security commitment by frequently updating their host operating system to address security issues. Additionally they maintain a list of known security vulnerabilities on the front page of their web site.   More information is available here: http://www.gentoo.org

Engine Yard receives information related to vulnerabilities through a combination of:

- Newsgroup, mailing list, blog, and subscription notices
- Internal and external assessments
- Customer testing
- Responsible disclosures by non-Customers

When a vulnerability is discovered, the information security and compliance function reviews the vulnerability for risk and applicability to the Engine Yard environment. Risks are ranked based off a number of considerations including:

"Is it remotely accessible?"
"Is authentication required to exploit?" and
"Is there a possibility for data to be exposed, if successfully exploited?"

Once ranked, tickets are filed and assigned to Engineering to determine fix options, and perform additional testing. Since Engine Yard is sensitive to the impact that security patches may have on our Customer's environments, the Customer is notified before pushing a fix. Depending on the criticality of the issue and the fix approach, different communication methods may be used including dashboard messages (our typical approach), engineyard.com notifications, and/or email notification via helpdesk tickets.

Responsible Disclosure

Engine Yard welcomes the involvement of the security community in protecting our platform, and has created a "Responsible Disclosure Policy" to direct how individuals can best share vulnerabilities with us via a controlled manner. To those individuals who follow our "Responsible Disclosure Policy," Engine Yard commits to:

- Promptly acknowledge receipt of the vulnerability report
- Provide an estimated timetable for resolution of the vulnerability
- Notify the researcher when the vulnerability is fixed

More information is available here:
http://www.engineyard.com/legal/responsible-disclosure-policy

Source Code Controls

Dependent on the source code risk and audience, Engine Yard maintains its source code at different locations including GitHub and internal private repos. Only Company personnel have access to Engine Yard's private repos. Access is audited on a regular basis, and when an employee or contractor leaves the Company. Engine Yard personnel do not have access to Customer's GitHub repositories.

Information Security Incident Management

Engine Yard maintains an “Incident Response Plan” that contains specific steps to address any type of security incident. These processes are grouped by function to:

1. Detect incidents
2. Analyze incidents
3. Contain incidents (including reporting)
4. Eradicate incidents
5. Learn (including root-cause analysis)

Incident Reporting

Engine Yard is committed to reporting any incident that may impact our Customers as soon as possible, especially when Customer data may be involved. Once a suspected incident is classified a confirmed incident, our communications process begins. This includes sharing the issue and impact with Engine Yard management, engaging with Support on the appropriate means to contact affected Customers, and, as necessary, initiating media communications via our contracted public relations firm.

Incident Management

Engine Yard maintains a security incident email distribution list that includes:

- Key members of the executive management team
- Customer support representatives
- Engineers who would assist in the analysis and eradication phases during a security incident.

Any potential security incident is run through our security incident process, and the incident is not declared resolved until all steps are completed. At the conclusion of the incident, a post mortem is conducted to assess underlying causes, determine longer term needs, and discuss other applications or systems that could also be affected by a similar incident in the future. All known issues are fed as inputs into the Company’s risk management process.

Engine Yard's architecture provides automatic failover that can replace a failed master application instance with an existing application slave. "Takeover" is the Engine Yard failover process for recovering from failure of an application master instance. Takeover occurs when Engine Yard detects that your application master is unable to reliably respond to requests. For example, this can happen because of an AWS EC2 issue or because the instance froze. If the instance does not recover within a short time, Engine Yard does the following:

- Terminates the problem instance.
- Promotes an application slave to master.
- Assigns the old master's IP address to the new master.
- Replaces the application slave instance that was promoted. (The new application slave uses the same version of the stack as the other instances in that environment.)

All Engine Yard Cloud supporting infrastructure is located in multiple availability zones. Within the dashboard, Customers can select from different regions to establish their computing clusters. Once a region is selected, the Engine Yard provisioning system distributes the instances among multiple AWS availability zones.

Compliance Management

Privacy

Engine Yard has developed and published a privacy policy that defines what data is collected and how it is used. More information is available here: **http://www.engineyard.com/legal/privacy**

Specific Compliance Initiatives

Payment Card Industry Data Security Standards (PCI DSS)

Engine Yard uses Braintree, a PCI compliant payment processor, for encrypting and processing credit card payments. Engine Yard's infrastructure provider, AWS, is PCI Level 1 compliant.

Statement on Standards for Attestation Engagements (SSAE 16)

AWS has their SSAE 16 SOC reports completed and available. Engine Yard is currently engaged with a third-party auditor in order to complete an updated SOC 2 Type 1 report following a SOC 2 Type 2 report. Our SOC 2 Type 1 report is available to our Customers and potential Customers with an NDA.

Safe Harbor Certification:

Engine Yard is Safe Harbor certified.
http://www.engineyard.com/legal/eusafeharborprivacypolicy

Contact

EngineYard.com

1-866-518-9273

Engine Yard
PO Box 77130
San Francisco, CA 94107-1713