APPLICATION & INFRASTRUCTURE SECURITY CONTROLS ON THE KINVEY PLATFORM

kinvey

INTRODUCTION

Security and privacy are major concerns when it comes to enterprise mobile applications. A recent survey by InfoWeek found that 61% of enterprises are only moderately confident about the efficacy of their mobile security controls and policies. The use of a secure, enterprise-grade mobile Backend as a Service (mBaaS) solution alleviates these security and privacy risks by isolating and protecting enterprise data sources and networks from client applications running on untrusted devices and their networks.

Kinvey provides comprehensive end-to-end security with automated audit and compliance tracking of users and access. As shown in Figure 1, all of the Kinvey client libraries encrypt all data on the client device using AES-256. Data is encrypted in transport using TLS/SSL. Kinvey platform services secures the data, our cloud services and underlying infrastructure. And, our platform supports a variety of secure connections to your enterprise systems including IPSEC VPN, SSL/TLS VPN and our own secure gateway solution.

Figure 1: END TO END SECURITY WITH KINVEY

This paper describes the security features of the Kinvey mBaaS platform from three perspectives:

1. Applications and communications
2. Kinvey platform services
3. Underlying Cloud infrastructure

As shown in Figure 2, Kinvey is a cloud-based managed service and is available in 3 editions:

Kinvey Business Edition is a multi-tenant, fully managed cloud service.

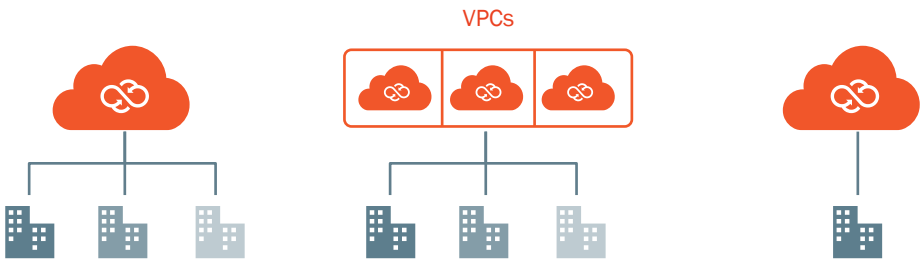
Kinvey Enterprise Edition is a single-tenant, dedicated, fully managed service available in 2 variants:

- Virtual Private Cloud (VPC) - infrastructure is logically separate but physically shared
- Dedicated - infrastructure is logically and physically separate

The Enterprise Edition of Kinvey is recommended for customers with stringent security and compliance requirements like PCI, and HIPAA.

Figure 2: KINVEY DEPLOYMENT OPTIONS

	Business Edition	Enterprise Edition VPC	Enterprise Edition Dedicated
Description	On-Demand	Enterprise grade	Compliance grade
Kinvey Service	Multi-tenant	Single-tenant	Single-tenant
Infastructure	Shared	Physically shared, logically isolated (VPC)	Dedicated
Security	IP Whitelisting Secure with HTTPS	VPN (IPSEC or TLS)	VPN (IPSEC or TLS)
Support	Gold	Platinum (24x7)	Platinum (24x7)
Managed Services	Yes	Yes - SLA Guarantee	Yes - SLA Guarantee



Next: Securing Applications & Communications

SECURING APPLICATIONS & COMMUNICATIONS

Kinvey ensures security at the application level by design. Application level security is critical especially when the applications are running on un-managed devices (i.e., devices not protected by standard Mobile Device Management - MDM). Kinvey provides the following security features at the application levels.

- **User Authentication**
- **Application Connectivity to Enterprise Data & Networks**
- **User Authorization**
- **User Revocation**
- **Data Security & Encryption**
- **Sensitive Data Protection**
- **Application Communications**
- **Data Access Controls**
- **Audit Trail**
- **Access to Enterprise Data Application Security Testing**

USER AUTHENTICATION

As shown in Figure 3 identity can be sourced in three ways using Kinvey Mobile Identity Connect: (1) Kinvey built-in OAuth2 provider, (2) Enterprise identity system, and (3) social providers (Facebook, Twitter, LinkedIn).

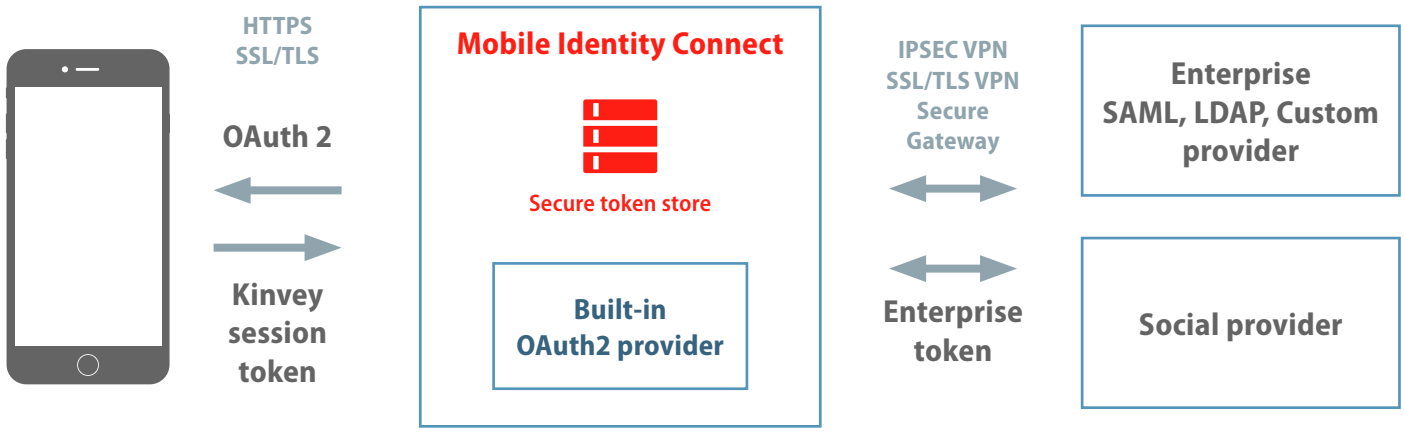
Regardless of the identity provider, all access to Kinvey services is abstracted and authenticated with a Kinvey token, not the originating provider token to ensure secure communications between mobile devices, Kinvey and enterprise services. The session token is generated when a known user logs into the app. Kinvey identifies mobile app users based upon the rules established by the developer and enterprise IT policies.

If an enterprise token is returned from the identity system of record, It is stored in a securte encrypted data store. A Kinvey-generated access token is then passed to the requesting mobile application. All access from the mobile application to Kinvey uses the Kinvey generated token. Any access to enterprise data sources that require authentication uses the securely stored enterprise access token. Kinvey verifies identity on every client request.

In this architecture, the application only works with an anonymized Kinvey-generated token. The enterprise token is never passed to the application. Since the application may be running on untrusted, unmanaged devices, this provides a critical level of protection against the threat of enterprise tokens being comprised on the device.

Enterprises can authenticate via LDAP, Active Directory, SSO or SAML using Kinvey Mobile Identity Connect (MIC). Kinvey MIC supports no-code enterprise identity connections to: PING Identity, CA, Active Directory, Oracle Identity Management, IBM Secure Identity Manager, ForgeRock, OKTA, LDAP and Active Directory as well as supporting enterprise custom identity sources. In cases where a customer has a proprietary identity provider, Kinvey provides the capability to add custom Auth Link Connectors (ALCs) to interface with these identity providers.

Figure 3: USER AUTHENTICATION AND TOKEN MANAGEMENT



APPLICATION CONNECTIVITY TO ENTERPRISE DATA & NETWORKS

Mobile applications delivered with Kinvey do not directly connect to enterprise networks or data. All access is through Kinvey Mobile Data Connect (MDC). This access between Kinvey MDC and enterprise networks is secured using a site-to-site IPSEC VPN tunnel (Figure 4) or the Kinvey Secure Gateway[1] (Figure 5).

The configuration and vendor choice for the VPN tunnel is based on the customer's security requirements. Kinvey supports a wide variety of hardware and software VPN servers. Please contact Kinvey for additional documentation on VPN requirements and compatibility. Note that the VPN tunnel is only available with the Enterprise Edition.

The Secure Gateway offers an alternate secure connectivity solution. The advantage of the Secure Gateway is that it does not require any firewall or network configuration changes on the customer network. The customer would install the Kinvey Secure Gateway in their DMZ and it creates a secure SSL/TLS-based tunnel between the customer network and the Kinvey service. All traffic between the Gateway and the Kinvey service is secured with HTTPS on port 443 and is in the outbound direction only. This is typically open on enterprise networks to enable standard browser traffic.

Figure 4: ENTERPRISE VPN TUNNEL

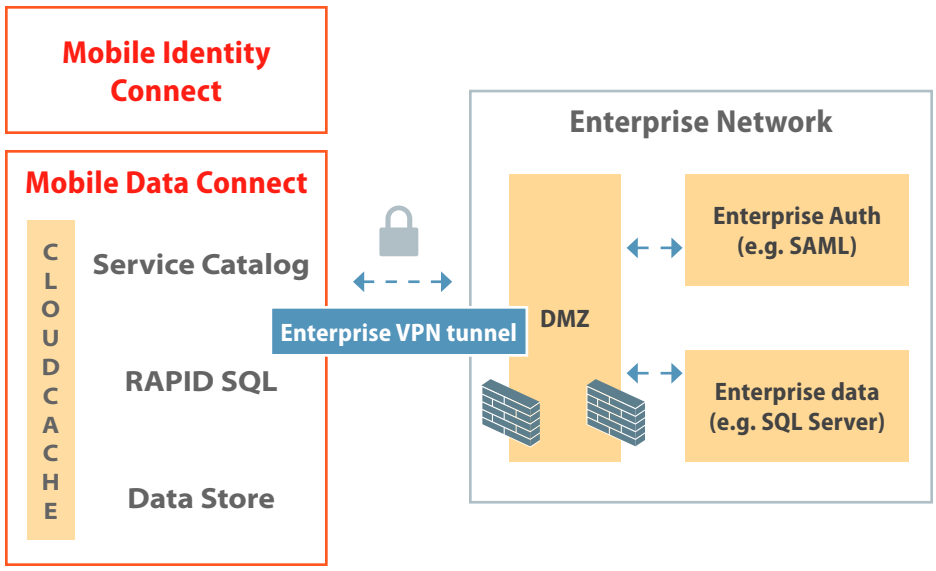
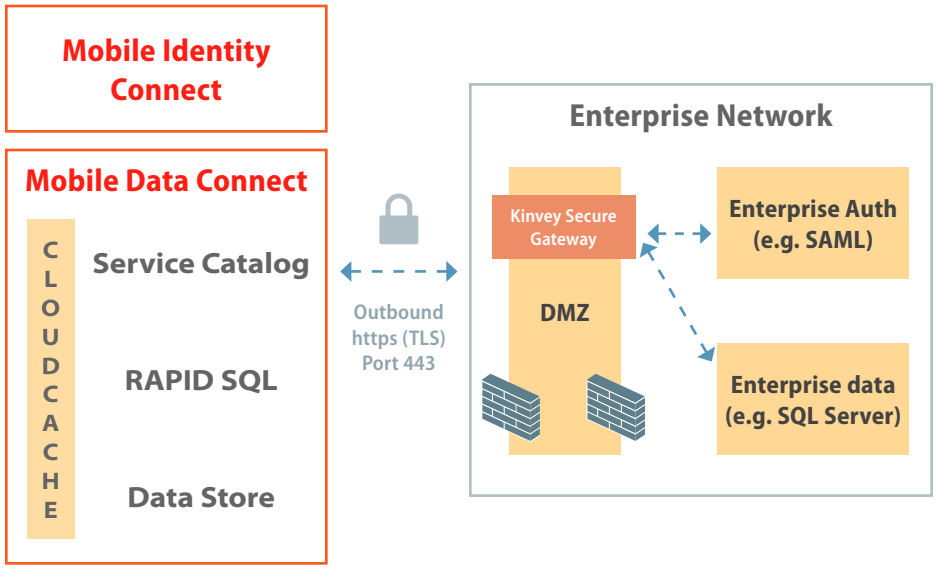


Figure 5: KINVEY SECURE GATEWAY



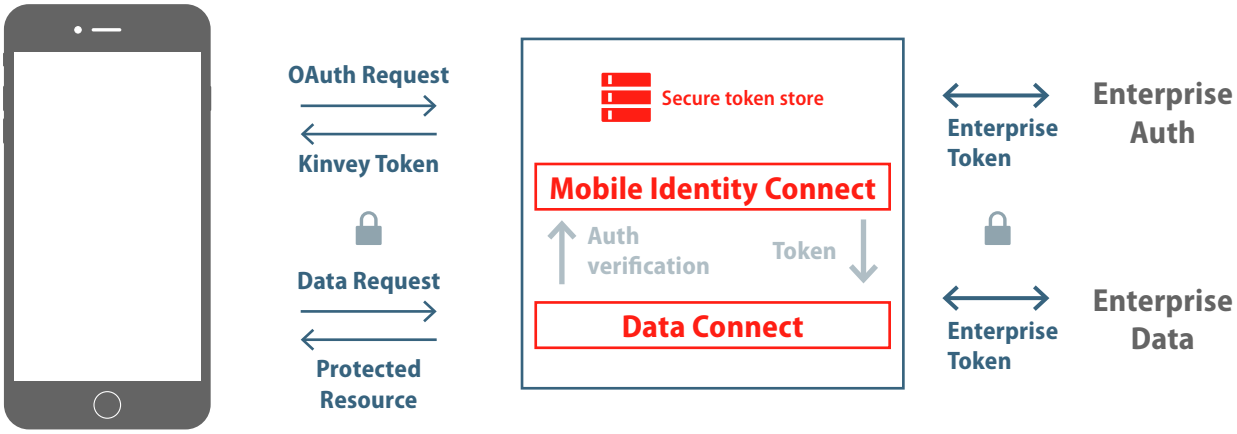
1 The Kinvey Secure Gateway is a new feature and will be available for Early Adopters starting in Feb-2016.

USER AUTHORIZATION

As shown in Figure 6, Kinvey data services handle all incoming requests for data and verifies the authentication/ authorization based on the identity configuration policies invoked in Mobile Identity Connect and then routes the request to the correct data provider.

Data providers can be Kinvey's internal data or file store, enterprise systems via data link connector or an external cloud provider.

Figure 6: USER AUTHORIZATION



USER REVOCATION

User accounts can be individually revoked in the Kinvey console. This enables application developers or administrators to disable rogue users quickly without affecting the entire application user population. The timestamp of the request and the identity of the requestor are available for audit and inspection.

DATA SECURITY & ENCRYPTION

The Kinvey SDKs support the encryption of all offline data (using AES-256) when stored offline in the device (at rest). All data is encrypted during transmission (using TLS/SSL with allowable list of ciphers), to ensure the secure storage of data in the device offline cache.

The libraries can also wipe the local cache and invalidate users when requested by the server. All certificates are required to be signed by a trusted 3rd party. No self-signed certificates are allowed.

SENSITIVE DATA PROTECTION

Passwords, PINs, shared secrets, and other sensitive information are hashed using bcrypt, SHA-1, SHA-2, or SHA-3 based on the type of data. All passwords are "salted" and hashed when stored.

APPLICATION COMMUNICATIONS

All external communications from the mobile application use the Kinvey SDK. All Kinvey SDKs use TLS/SSL protocol and associated encryption to communicate with the backend service.

In addition, the ciphers used are restricted to the following:

TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA25

TLS_RSA_WITH_AES_256_CBC_SHA256

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_AES_128_CBC_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA256

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SH

DATA ACCESS CONTROLS

Developers building applications on the Kinvey platform are responsible for properly restricting access to users of their app by using the appropriate APIs provided and documented by Kinvey. To make this process easier and less error prone, Kinvey has taken great care in providing the right controls to easily enforce the principle of least privilege.

Kinvey has built-in capabilities to create and manage role based access rules for data. Customers can set permissions on a granular level to define which users can access what data and how. Access controls can be set programmatically via our REST API or in a no-code form in Kinvey's management console.

By default, data entered by one app user is readable, but not writable, by other app users, and the read access can be taken away by a single configuration option. Kinvey provides APIs to further fine-tune access rights to individual users.

SECURITY AND COMPLIANCE AUDIT

All mobile app requests for access to corporate data and resources are routed through the Kinvey service. All of these requests and any events associated with these requests are tracked within Kinvey. We have collated this information in a data repository and make it available in the following ways:

- Query of the raw data and log information
- Visualization tools to chart the data in graphs and tables
- Customizable dashboards that aggregate specific visualizations based on use case

All of the information is time stamped and provide details on the type of request, originating IP address and location, and anonymized user information. This provides the required information to be able to create an audit trail.

ACCESS TO ENTERPRISE DATA

Access to enterprise data follows the authentication and authorization provided by the identity management system that is integrated with the application. Kinvey provides out-of-the-box support for enterprise systems like Active Directory/ LDAP, SAML-based providers, and OAuth-based providers.

APPLICATION SECURITY TESTING

Kinvey performs regular application security and penetration testing using Veracode. Any critical vulnerability is immediately corrected. The results of our scans can be made available to our enterprise customers upon request.

Next: Securing of the Kinvey Platform Services

SECURING OF THE KINVEY PLATFORM SERVICES

Kinvey also employs best practices to secure our mobile services running on our multi-tenant and dedicated cloud instances. These security services are outlined in this section.

- ✓ **Protecting Against Intrusions**
- ✓ **Securing Access to Kinvey Services & Servers**
- ✓ **Virus Scanning**
- ✓ **Operating System Security**
- ✓ **Safe Multi-tenancy**
- ✓ **Audits**

PROTECTING AGAINST INTRUSIONS

An intrusion detection system (IDS) is deployed on the bastion host and inside the VPN. The IDS monitors actions such as login attempts and privilege escalation attempts, and alerts or takes action based on the severity. The IDS is updated every 60 days with new signatures to detect malicious activity.

SECURING ACCESS TO KINVEY SERVICES & SERVERS

All Kinvey servers are behind a VPN and are inaccessible directly to the rest of the Internet. Authorized Kinvey staff connect via secure shell (SSH) and a specially configured "bastion host," which is a single machine that controls and limits all access. Within the VPN, connectivity between hosts and outbound connections are disallowed except when essential for running the service.

SSH keys to access the production system are limited to Kinvey operations staff and are rotated frequently according to best practices. The access grants are deployed on the bastion host and inside the VPN. The IDS monitors actions such as login attempts and privilege escalation attempts, and alerts or takes action based on the severity.

VIRUS SCANNING

All systems are automatically scanned for viruses on a weekly basis. Any affected files are either quarantined or removed.

OPERATING SYSTEM SECURITY

Operations staff at Kinvey monitor Common Vulnerabilities Exposures (CVE) databases and install critical patches as soon as they are available, and medium patches on a weekly basis.

SAFE MULTI-TENANCY

Multi-tenant SaaS applications need appropriate safeguards in place to isolate applications from one another from a security and performance standpoint. The data for each customer backend is stored in a separate, password protected database that can only be accessed indirectly and in the context of the unique application keys for that backend.

AUDITS

The entire Kinvey cloud service undergoes penetration testing by an independent vendor on a yearly basis.

Next: Infrastructure Security

INFRASTRUCTURE SECURITY

Kinvey's Mobile Backend as a Service platform runs on cloud infrastructure provided by Amazon Web Services (AWS), the leading Infrastructure-as-a-Service provider, or by VMWare's vCloud Air Hybrid Cloud, the leading enterprise hybrid cloud service. Both infrastructure providers regularly undergo rigorous security audits and have completed the requirements of major security certifications.

This section provides an overview of the physical and compliance features of AWS and VMware vCloud Air.

- Physical Security
- Compliance Certifications
- Data Backup, Retention, and Recovery

PHYSICAL SECURITY

Both providers have been examined and audited to meet the physical security requirements of the following standards:

- ISO/IEC 27001
- SOC 1 Type 2/SSAE 16/ISAE 3402
- SOC 2 Type 2

Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff using video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication to access data center floors. All visitors and contractors are required to present identification, must be signed in, and are continually escorted by authorized staff.

For more information on vCloud Air security please visit: https://vcloud.vmware.com/service-offering/security-overview

For more information on AWS security please visit: https://aws.amazon.com/security/

COMPLIANCE CERTIFICATIONS

Kinvey uses 2 cloud providers for infrastructure (compute, network and storage) - AWS and VMware vCloud Air. Both providers have a comprehensive set of security and compliance certifications. They cover the security and compliance requirements of the infrastructure.

vCloud Air has completed ISO 27001 certification and examinations against SSAE16 SOC2 Type 2 and HIPAA by an independent third party auditor. The Service is in the process of certifying against the SSAE 16 SOC3 and the PCI DSS 2.0 standards. VMware is also setting up a separate community cloud under the vCloud Government Service name that is being certified against FedRAMP criteria by the Joint Authorization Board (JAB) to achieve provisional authority to operate. For more information on VMware vCloud Air compliance certifications please visit: https://vcloud.vmware.com/service-offering/cloud-compliance

AWS has SOC1/2/3 reports available in addition to PCI DSS Level 1 compliance. AWS has achieved two Agency Authority to Operate (ATOs) under the Federal Risk and Authorization Management Program (FedRAMP) at the Moderate impact level. For more information on AWS compliance certification, please visit: http://aws.amazon.com/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/

DATA BACKUP, RETENTION, AND RECOVERY

Data that is critical to the operation of the Kinvey service is backed up hourly. The backup data is retained for thirty days. Longer-term data retention for our Enterprise Edition customers is available on request. Service restoration from this backup data is verified twice a year. The data backups are stored in a geographically separate, secure facility. Any data encrypted at the source remains encrypted in the backup facility.

FOR MORE INFORMATION

Enterprise mobility requires security at every layer from the application itself, through the transport system to the underlying platform. Kinvey takes these requirements quite seriously and provides enterprise-grade security throughout the mobile end-to-end system. If you would like more information please contact Kinvey at info@kinvey.com.

APPENDIX:
KINVEY SECURITY CHECKLIST

General	
Have you designated an individual responsible for information security within your organization?	**Yes**
Have you established training programs to ensure personnel understand their responsibilities regarding information security?	**Yes**
Are managers responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility?	**Yes**

Physical, network and infrastructure	
Does your company implement physical access control mechanisms to ensure only authorized individuals can access facilities?	**Yes**
Does your company have documented infrastructure and information security policies in place?	**Yes**
How frequently are your security policies updated to ensure the policies address new threats and trends?	**Biannually and as required**
Do you immediately terminate personnel access to computing and network resources, facilities, and secure areas when an individual is no longer an employee or contractor?	**Yes**

Are data centers, equipment rooms, and telecommunications closets physically protected so that only authorized individuals can access them?	**Yes**
Are your facilities and data centers protected against damage from fire, flood, earthquake, explosions, civil unrest, and other forms of natural or man-made disaster?	**Yes**
Are power-dependent devices protected from power failure, outages, surges and other electrical anomalies?	**Yes**
Do all networks have appropriately configured firewalls in place?	**Yes**
Do firewalls deny access to all connections that are not explicitly allowed?	**Yes**
Are intrusion detection and/or prevention systems (IDS/IPS) at all connections between internal and external networks?	**Yes. Kinvey servers have IDS protection software installed to protect against attacks. Kinvey uses HIDS in combination with network protection offered by its infrastructure provider**
Are all default passwords changed during or immediately following the completion of hardware or software installation?	**Yes**
Do all remote access protocols used to access information perform encryptions with 128-bit or 256-bit AES or Triple-DES?	**Yes**
How often do you perform vulnerability scans of production internet-facing websites and web applications?	**Continuous scanning**

Logging, monitoring and auditing

Are all systems which store, process or transmit customer information capturing security-relevant events in audit logs?	**Yes**
Do you have external third-party conducted vulnerability scans and periodic penetration testing on your service?	**Yes**

Authentication

Are passwords, PINS, shared secrets and other authentication information always encrypted (or hashed) in storage and transmission?	**Yes.** **Depending on the use case, we would use bcrypt, SHA-1, SHA-2 or SHA-3 based upon the Cipher chosen between the client and server. If we are storing a password, we hash it using SHA-1. We salt and hash all passwords.**
Do you employ a user password length of at least 8 characters and three complexity classes?	**Yes**
Do you support identity federation standards (e.g. SAML) as a means of authenticating/ authorizing users.	**Yes**

Antivirus / Malware

Do you have anti-malware programs installed on all systems which support your service?	**Yes**
Do you monitor Common Vulnerabilities and Exposures (CVE) databases and install patches as soon as they are available?	**Yes**
Do you have procedures for removing or quarantining any affected files?	**Yes**

Change management & SDLC

Do you have a documented Change Management process and supporting procedures in place to control all changes to computing and network resources?	**Yes**
Do you have a documented system development lifecycle (SDLC) which governs the development and deployment of systems and applications?	**Yes**
Are hardware and software systems and components configured to a known baseline configuration?	**Yes**

Do you maintain the baseline configuration of each system?	**Yes**
Do you maintain documentation of configuration changes to each system?	**Yes**
Do you maintain separate development, test and production environments?	**Yes**
Are all software updates and patches researched, tested and verified by appropriate personnel before deployment?	**Yes**

Backup / disaster recovery

Do you maintain a Business Continuity and Disaster Recovery Plan (CoB/DR plan) that will prevent catastrophic data loss and ensure timely restoration of computing services in the event of system failure, damage or destruction?	**Yes**
Do you perform regular data backups on systems processing or storing data?	**Yes**
Do you perform data backups prior to any system upgrade or maintenance activity?	**Yes**
If encrypted information is backed up, does it remain encrypted throughout the data backup process?	**Yes**
How often is the ability to restore data backups tested?	**Every six months**

Security incidents

Do you have a formal security incident monitoring, reporting and response process to identify, report and appropriately respond to known or suspected incidents?	**Yes**
Are the appropriate personnel trained to identify and respond to security attacks?	**Yes**
Do you have a capability to rapidly patch vulnerabilities across your computing devices and systems?	**Yes**

Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	**Yes**
Are all relevant incidents reported to the affected customer in a timely manner?	**Yes**

Application security

Do you have the ability to logically segment customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data	**Yes**
Do you have the capability to logically segment and recover data for a specific customer in the case of a failure or data loss?	**Yes**