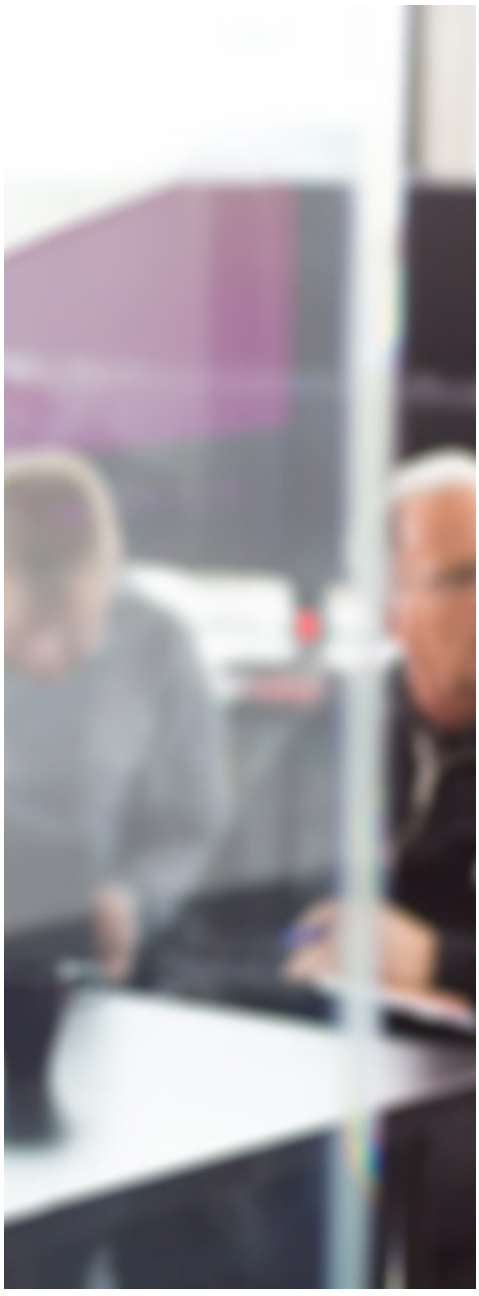
SPOKE

Security Whitepaper



Introduction

At Spoke, we understand that the confidentiality, integrity, and availability of our service are the highest order of priority for our customers, and for us as a company.

When we were starting Spoke, we discussed and understood that privacy and security would be two of the largest mandates for our organization - items that needed to be built into the very DNA of the company.

We understand that we're not only asking companies to trust us with their sensitive information and to provide them with critical business communications, we are also asking their employees to trust us with their personal information.

Part of that trust is an assurance to employees that we will keep their personal information and activity separated from their work activity, and ensure that their employer has no access to personal content or interactions. This later promise to employees is critical to customers succeeding in implementing a widely adopted BYOD communications environment.

As part of our employee on-boarding, the focus on security and privacy of information is a key theme, and is indeed threaded throughout their working day at Spoke. From the tools, processes, and everyday interactions with data and each other, security and privacy is at the forefront. As an example, 2-Factor Authentication is required for access to every system, and that access expires at least every 30 days.

Our goal is to take a comprehensive, multi-layered approach to security, ensuring that every element of your data is secure, and that our service in the cloud is as secure (if not more secure) as when they were when run on premise.

Security and privacy are and always will be moving targets. As different threats and compliance standards emerge, organizations need to respond and to be continually questioning their processes and practices. Spoke will continue to be vigilant and diligent across all aspects of security and privacy, always looking for improvements we can make to raise the bar higher.

Information Security Program

Governance

At Spoke we believe that the security of our customer data is the responsibility of the entire organisation. Security governance is lead by the CTO and the senior engineering team with representation from other areas including the CEO, HR and legal. The entire team is tasked with proactively reviewing, auditing and continuously improving our security, operational and engineering procedures.

Our security program covers all aspects of our business that involve access to confidential customer data. This includes our software, the infrastructure that supports our platform, our internal processes, how we hire, onboard and train employees, how we manage customer accounts and data, and how we engage with third party suppliers and partners.

Privacy and Trust

Our internal procedures limit access to sensitive information only to staff that have a need to know. These protections also extend to protecting the security of sensitive customer data with third party contractors and suppliers. We require all third party vendors to make security assertions and provide assurances similar to our own, with these assertions being enforced contractually. Our comprehensive privacy policy is available publicly online here.

Application Security

Application Architecture

All Spoke modules (web sites, web applications, mobile applications and back-ends) are tiered into logical segments that separate presentation from business logic and underlying data storage. Each layer is independently secured via network policies and authentication/authorization processes.

Secure Development

Spoke follows best in class development practices. All source code is stored in a source code repository with versioning control. Access to repositories is strictly controlled with rights only granted to engineers who have a direct need to commit to the code base. All check-ins are reviewed by at least one other senior engineer to ensure it complies with all requirements, including checking for necessary security controls.

Test Processes

Our test processes are implemented using a layered approach. Our engineering team is responsible for developing unit and integration tests and these are committed alongside changes to the code base. In addition to automated tests, team members responsible for quality test all new functionality and complete full regression testing prior to code being released to our production environment. We leverage

third party organisations to comprehensively test our applications and infrastructure against known vulnerabilities and common penetration techniques.

Build Processes

Our build pipeline includes a number of automated quality gates that prevent sub-standard code from being released onto any environment (development, quality or production). These gates include unit and integration tests all passing, meeting minimum test coverage requirements, and all code including third party dependencies being scanned for known vulnerabilities. Any failures at any of these gates will result in the build failing and prevent the code from being deployed to any environment.

Upgrade and Deployment Procedures

Our deployment procedures are all scripted and fully automated and use a standard build pipeline across all environments. This is by design and reduces the risk of human error during deployment. The process to develop deployment scripts follows our standard secure development process to ensure all changes are fully reviewed and tested. We use a blue/green model so that when new code is deployed into production, our end-users do not notice any interruption to service. If a critical error has made its way into production, the blue/green model allows us to easily (and silently) fall back to the previous version. We do not have scheduled downtime or maintenance, even for system upgrades or migrations.

"Spoke follows best in class development practices. All source code is stored in a source code repository with versioning control."

Data Security

Spoke uses encryption to safeguard and protect customer data when in transit and at rest.

Data In Transit

All communications between our applications (web and mobile) and Spoke services and APIs, are made under HTTPS, using TLSv1.1 or TLSv1.2. All underlying access from APIs to database instances, storage layers and other services is also performed using encrypted transports (HTTPS or SSL encrypted connections).

Data At Rest

Our use of the Amazon Web Services platform allows us to take advantage of the numerous at-rest storage protection options available. All data storage including database systems is fully redundant across multiple availability zones (and where feasible, regions), and databases are backed up daily at a minimum.

For data stored on Amazon's Simple Storage Service we leverage S3 Server Side encryption which uses one of the strongest block ciphers available - 256 bit AES (Advanced Encryption Standard). Every object is encrypted with a unique key; this key itself is encrypted with regularly rotated master key.

For data stored in Amazon's Relational Database Service we leverage encrypted instances. This includes the underlying storage of a database instance, its automated backups, logs, Read Replicas and snapshots.

Identity and Authentication

We leverage Amazon Cognito to provide user authentication to all Spoke services. Cognito provides logical and physical separation of user credentials from our other core systems. All communications with Cognito are secured using HTTPS and authentication uses the secure SRP protocol - see here (wikipedia) and here (ietf). SRP eliminates the need for the client to exchange the password over the wire with the server, and provides for storage of secure verifiers instead of cryptographically hashed passwords. The SRP protocol prevents man-in-middle attacks, and because a password-equivalent is not stored on the server also ensures that theft of server data does not allow an attacker to masquerade as the client without brute forcing the password.

"Every object is encrypted with a unique key; this key itself is encrypted with regulary roated master key."

User Authorisation and Roles

All Spoke systems are designed with a deny by default security posture. During the authentication process the user identified is granted short living encrypted security tokens that include role-based claims which then restrict access to APIs and underlying services and data.

Role-based security is implemented using a multi-layered approach where restrictions are both applied at the API and data storage layer ensuring that both horizontal and vertical restrictions are applied so that 1) a given user can only take actions appropriate to their assigned role and 2) each user's information is protected from all other users.

Secure Administration

Spoke's account portal provides access to our customers and gives them access to the tools required to securely manage their service. Our role-based access control allows your account administrators to easily:

- Add and remove Spoke users
- Grant and revoke user privileges and roles
- Set and manage access to additional modules and phone numbers

Operational and Network Security

Our network and operational environment is designed to ensure that all data is protected against tampering, eavesdropping and theft.

Personnel Authentication and Account Management

At Spoke, all staff access to systems, whether development, quality or production is strictly controlled through a deny-all, grant-restricted policy. Our staff accounts are required to have a strong password policy enabled, with frequent password rotation and two factor authentication enabled for all systems. Any staff accessing Amazon Web Services services must first authenticate through a Bastion account before assuming a role in the environment they are attempting to access. This allows for swift and efficient elimination of access rights if required.

Production System Access

Access to production systems is only granted to authorised staff members. Access to these systems is logged and audited via Amazon Cloudwatch, and access to these logs is restricted to senior staff members only.

Network Segmentation

Our network infrastructure has been designed to enforce strict segmentation between all environments (development, quality, production). Following best practice guides for Amazon Web Services networks, each environment is isolated to its own Amazon account, with each account having its own Virtual Private Cloud (VPC) with separate public and private subnets. By enforcing environmental isolation at the account/VPC level, and by having separate private and public subnets with separate ingress and egress rules, we strictly control what traffic and who is allowed into and out of our network.

Failover and Redundancy

Our system has been designed with redundancy in mind. The platform is underpinned by AWS Lambda, which is a serverless environment that provides us with a number of operational benefits, including capacity provisioning, monitoring of fleet health, applying security patches to underlying server resources, easy scaling, and multi-region high availability.

We leverage multiple third party carriers internationally to provide redundancy for call traffic, and all third party carriers have been rigorously review by our security team to ensure they meet or exceed our own redundancy and security requirements.

Change Management

Our change management process for operational environment changes follows our secure development process. All changes to networks, systems and processes are fully scripted, are tracked in our version control systems and are fully reviewed by one or more of our senior engineers. These changes, including patches, are applied to tests environments prior to being deployed into production.

Monitoring, logging and altering

Our environments are configured with multiple layers of monitors, probes and alerts that help us to detect system issues. Any major or critical issue is automatically sent to our 24x7x365 on-call engineering staff, with escalation policies in place to ensure rapid response.

"At Spoke, all staff access to systems, whether development, quality or production is strictly controlled through a deny-all, grant-restricted policy.

Physical Security

Amazon Web Services

Our websites, web applications, mobile application back-ends, and all other back-end services including data storage run on Amazon Web Services. The Amazon Web Services platform is designed and built to run on a shared security responsibility model. This means that AWS is responsible for securing the underlying infrastructure that supports our platform, including facilities, network, hardware, and operational software. The infrastructure that Amazon provides is designed and managed in alignment with security best practices and variety of IT security standards, including SOC 1,2 and 3, PCI DSS level 1, and ISO 27001. For more information on Amazon's security processes, please see this white paper.

SPOKE