Security at Quip

Quip

A Salesforce Company

Outline

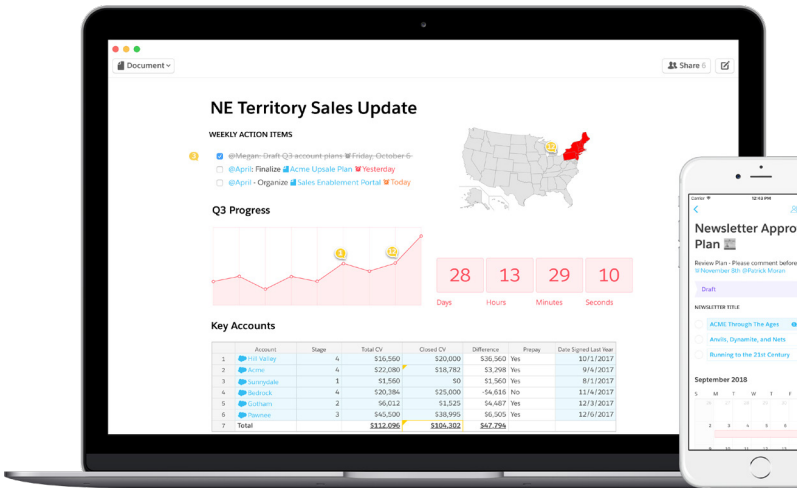
Overview

Quip is Salesforce's mobile cloud documents platform. It's the only collaboration tool to bring together content and communication into a single live workspace that transforms the speed of business decisions. In this whitepaper, we'll introduce the unique **value** Quip brings to organizations, share details on how Quip approaches **security** as a Salesforce company, and outline the **deployment options** available to customers.

Quip Drives Collaboration at Speed

Quip creates value by helping organizations move forward, faster. The tool transforms the way teams work together by putting communication at the center of productivity. Quip engages people deeply, reduces friction, and is mobile-first so your teams spend less time in email and meetings–and more time on the work that matters most. And, only Quip multiplies the speed and impact of Salesforce by bringing together data and conversations.

Quip's full-featured native iOS, Android, Windows, and Mac apps complement our desktop web app and ensure that every person in your organization can be on the same page, whether they're on the go or at their desk.



Security at Quip: Trust Is Our #1 Value

Salesforce is committed to achieving and maintaining the trust of our customers. This mission hinges on us providing a robust security and privacy program that carefully considers data protection matters across our suite of services.

As a Salesforce company, trust is Quip's #1 value. Quip puts our customers' trust first, and this guides everything we do–from how we write software to how we run our business.

Defense in Depth

Quip approaches security through the lens of *defense in depth*, which holds that a system is only as secure as its weakest link–so the best defense is to ensure every aspect of the system is secured in depth. This means that along with building robust protections for every aspect of Quip's service, we also regularly zoom out to look at the entire system, which enables us to develop new solutions that guard against emergent risks to the system as a whole. We use this coordinated, high-integrity approach to keep our customers' data safe.

In this section, we'll outline how regular auditing, our organizational policies and practices, our approach to software development, and our disaster recovery plans all uphold trust as Quip's #1 value.

Audits, Certifications & Compliance

Quip maintains multiple regulatory and auditing certifications:

- SOC 2, Type II Certification
- EU-U.S. Privacy Shield Framework
- Swiss-U.S. Privacy Shield Framework

Customer data entered into Quip is within the scope of a Salesforce's annual certification to the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as administered by the U.S. Department of Commerce. Salesforce's information security control environment applicable to Quip undergoes an independent evaluation in the form of a Service Organization Control (SOC) 2 report. Salesforce's most recent SOC 2 report for Quip is available upon request from your organization's Salesforce account executive. In addition, Quip is GDPR-ready.

Quip's systems are also audited annually by an independent, industry-leading third-party security auditor.

Organizational Policies & Practices

Leadership

Trust starts at the top, with the culture set by executive and senior management. These management functions play important roles in setting the company's focus, and their direct leadership reinforces integrity and ethics as core to Salesforce's corporate culture.

Beyond the responsibility that all executives and senior leaders at Salesforce share to set a tone of putting trust first, Salesforce also dedicates leaders to protecting trust specifically. Salesforce's Chief Trust Officer is responsible for Salesforce's security program and personnel, including information, product, and corporate security, enterprise risk management, and technology audit & compliance. The Global Privacy Counsel is responsible for Salesforce's privacy program, including compliance with applicable privacy and data-protection laws. Additionally, all Salesforce personnel are required to follow Salesforce's confidentiality, privacy, and information security policies.

Hiring Practices

People earn trust through their actions, so Salesforce uses a third-party provider to perform background investigations on all incoming employees in the United States (U.S.) and countries in which Salesforce has employees to the extent permissible by law. The background investigation is initiated with the applicant's informed consent after an offer of employment is extended to the applicant.

The following areas are investigated as part of the current background check packages for the U.S.:

- Criminal background check
- Education verification
- Employment history
- Global sanctions and enforcement check
- Federal debarment check
- Health care sanctions check

Background checks are initiated prior to the employment start date and continued employment is contingent upon successful completion of the background investigation.

Workstation Security

All Salesforce employees are issued securely configured corporate workstations. A full-disk encryption solution is installed on all workstations to encrypt data and users cannot disable the full disk encryption. Remote access sessions into internal and production networks are encrypted. Anti-malware software is installed by default and cannot be uninstalled by individuals. Strong passwords are required for system-wide single sign-on (SSO) and employees are required to rotate them regularly or else be shut out of internal systems. Corporate policy requires that employees lock their workstations whenever they step away from them, and this policy is enforced by leadership.

Two-factor authentication, in addition to strong passwords, is required for all access to Quip operational systems.

Account Provisioning & Modification

Quip maintains an authorization matrix detailing the Quip permission groups, the roles that are eligible for the permission groups, and the access that each permission group has.

Access to the production environment, internal tools, and customer data is restricted to authorized personnel on an as-needed basis, and requires documented approval by management. Privileged access to production is limited to the minimum possible set of employees necessary to reliably operate the system. All access events are logged and audited twice annually for compliance with these policies.

Access Removal

In the event that a Salesforce employee is terminated, an IT helpdesk ticket is initiated that includes the employee's termination date. Access to Quip systems is removed within 24 hours of voluntary termination, or immediately for involuntary termination.

Physical Security

Access to Salesforce buildings is restricted to badged employees and contractors and escorted visitors.

Quip's serving systems are hosted on Amazon Web Services. Physical security of those systems follows the physical and operational security processes detailed in the Amazon Web Services Overview of Security Processes whitepaper. Absolutely no customer servers or services are hosted within Quip's physical offices.

Internal Training & Communications

Defense in depth relies on an alert, educated workforce to continuously monitor the system as a whole and take responsibility for their role in keeping customer data safe. That's why at Salesforce, all employees and contractors are required to complete security awareness training on an annual basis. The security awareness training covers content on relevant security best practices and includes the responsibility of every employee and contractor to communicate security concerns. Weekly reminders are sent via email to personnel who have not completed the training. These reminders are not sent when the training material is due for a revision or is being revised as part of the annual update of the training material.

The Security team presents security awareness information to Salesforce personnel through email, Chatter posts, posters, and in-person instruction throughout the year, which includes, as necessary, details regarding significant changes to security and availability policies. In addition to the security awareness training, new employees have a written job description that includes the responsibility to communicate significant issues and exceptions in a timely manner to an appropriate higher level of authority within Salesforce.

Salesforce maintains internal information security policies and standards to ensure that employees understand their individual roles and responsibilities regarding security and availability and significant events. A dedicated team is focused on security education for employees. Security education includes formal and informal training programs, annual security training for employees and contractors, the use of email messages to communicate time-sensitive information, intranet sites, Quip documents, and periodic meetings.

Information Security Management System (ISMS)

Salesforce, and Amazon Web Services as a hosting provider, maintain formal company-wide information security management systems (ISMS) that conform to the requirements of ISO 27001, including security policies, standards, and procedures. Formal policies, procedures, and job descriptions are documented for operational areas including: data center operations, development, program management, production management, infrastructure engineer, quality engineering, release management, operations, hiring, and terminations. These policies and procedures have been developed to segregate duties and enforce responsibilities based on job functionality.

Policies & Standards

Salesforce has privacy- and security-conscious policies that apply to all of our information handling practices.

Contractual Privacy Protection for Customers: Salesforce's contracts include confidentiality provisions that prohibit us from disclosing customer confidential information, including customer data, except under certain narrowly defined circumstances, such as when required by law. Salesforce agrees not to access customer's accounts, including customer data, except to maintain the service, prevent or respond to technical or service problems, at a customer's request in connection with a customer support issue, or where required by law.

Code of Conduct, Confidentiality Agreements, and Information Security Policies: Every Salesforce employee and contractor must follow Salesforce's code of conduct, sign confidentiality agreements, and follow Salesforce information security policies.

Secure Software Development & Deployment

Access Authentication

Access to production infrastructure is restricted to authorized personnel based on job function. Privileged system access is restricted to a limited number of system administrators and their management.

Authentication to the production environment is performed via modern best security practices utilizing Secure Shell ("SSH") keys and requiring two-factor authentication.

Access to the public cloud management console is restricted to authorized individuals that require access to perform their duties, and requires two-factor authentication.

Access Review

On a semi-annual basis, management or authorized delegates perform an access review of users and permissions to the production network to verify that users have appropriate privileges. Deviations and necessary changes identified during the review are recorded and/or remediated.

Network Access Controls

Access by customers and internal personnel is restricted by defined network access controls configured to enforce defined network security standards. Only required ports are open and all others are denied. Access to change network configurations is restricted to authorized personnel.

Penetration Testing & Bug Bounty

Quip engages a third-party organization to conduct penetration testing on the Quip Services annually. Results are reviewed by management and findings are tracked to resolution. Penetration testing is done in a managed environment, and is never exposed to customer data.

In addition to penetration testing, Quip also manages a bug bounty program through which vulnerabilities are discovered and responsibly disclosed to the Company on an ongoing basis. Submissions are triaged and valid submissions are tracked to resolution.

Encryption

Customer data stored in Quip's service is encrypted in transit and at rest. Transport Layer Security (TLS) encryption is used to protect the security and integrity of information transmitted between the customer's web browser and the Quip Services.

Encryption keys are securely managed and stored in standard cloud infrastructure. Access is controlled via audited Identity & Access Management (IAM) roles. Encryption keys are never stored in source code, and all encryption keys are rotated per industry standards.

Change Management

Quip's engineering team follows a systematic approach to managing change to ensure that changes to the system are reviewed, tested, approved, and appropriately documented and communicated.

Prior to deployment to the production environment, changes are:

- Evaluated to determine if the change might affect the security and/or availability of the system
- Reviewed and approved by authorized approvers

Application builds undergo automated testing and issues identified are remediated prior to release. Mobile application changes require quality assurance testing prior to release. Releases to production are logged and available for review. Employees receive notification of production releases via Salesforce's internal communication channel.

Emergency Changes

Emergency changes to the system that require deviations from standard change management procedures are logged and approved by an authorized approver within 24 hours of the change.

Incident Management

Management has documented incident management policies and procedures to ensure that:

- Potential security events are identified and reported to appropriate personnel for resolution
- Personnel follow defined protocols for resolving security events
- Steps for applying changes and notifying internal and external users are documented
- Incidents are triaged and tracked to ensure timely resolution of incidents

Service Monitoring

The Quip Services are monitored for availability and performance, and will alert the on-call engineering team members if reliability, availability, or performance thresholds are not met.

In addition, the Quip Services are also monitored for security purposes by monitoring production access logs for anomalous behavior. Anomalous behavior, when identified, is followed up on and tracked to resolution. Logins to production systems are logged and reviewed monthly. Suspicious, unexpected, or unusual logins or login attempts are logged, investigated, and remediated. An Intrusion Detection System (IDS) is used to detect and report anomalous behavior.

System capacity for long-term strategic planning is monitored on an ongoing basis.

Disaster Recovery & Business Continuity

The Head of Engineering and management of Quip's engineering team meet on a periodic basis to perform capacity planning and to ensure availability requirements and commitments are managed. Procedures have been implemented for performing backup that include coverage of backup, frequency of backup, management of backup media, and performance of restoration testing.

User data is automatically backed up nightly, both in the primary and the disaster recovery area (DR) sites. Backup restoration procedures have been established and are tested annually. Backups are retained in accordance with the defined schedule in the Quip Backup policy.

A DR plan has been established, in conjunction with the user data backups, and is tested annually. Production data is replicated in near real-time to provide fall-over redundancy.

In addition to the Quip disaster recovery plan, Salesforce has a Global Business Continuity program which is managed by the Business Continuity Team. The Technology and Customer Support business continuity plans are reviewed, exercised, and approved by the respective teams with Business Continuity Management (BCM) coordination annually. This program is overseen by senior management for each of the key functional areas within Salesforce, and is supported by executive leadership at the highest level. Individual teams are responsible for the development and maintenance of their respective plans. The Technology and Customer Support business continuity plans are reviewed, exercised, and approved by the respective teams with the BCM team coordination. Personnel are trained in their contingency roles and responsibilities and receive ongoing refresher training as part of contingency planning testing activities.

Salesforce has a Global Crisis Management Team (CMT) comprised of select executives from key departments globally. The CMT is mobilized when a crisis or significant event occurs, and is responsible for evaluating the situation and responding accordingly. Depending on the severity and nature of an incident, the CMT Leader may request engagement from various support teams to assist with mitigation of the incident. The CMT meets periodically for training education, and review of the documented Global Crisis Management Team Plan, or as required due to a crisis or significant event. CMT members have specified roles and responsibilities and are expected to be available at all times (24/7).

The documented Global Crisis Management Team Plan (CMP) identifies response strategies for any hazard, including pandemics and emerging health threats and incidents that may impact the Salesforce reputation. Exercises are completed annually to test the effectiveness of the CMP and trainings of individual members occur as necessary throughout the year. As part of developing a viable Disaster Recovery plan and program, Salesforce schedules Disaster Recovery exercises which are conducted several times per year with and without customer participation.

Deployment Options

Quip offers three deployment options to meet every organization's needs: Quip Business, Quip Enterprise, and Quip Virtual Private Cloud.

Quip Virtual Private Cloud makes Quip's mobile cloud documents platform an option for companies that need an extra level of IT control, and is particularly relevant for organizations in highly-regulated industries such as Financial Services, Health & Life Sciences, and Government. By deploying Quip's modern collaboration product on isolated virtual private cloud instances, we're able to offer customers completely customized control over their data and network, including physical location, encryption management, compliance with regulatory requirements, and network access policies. To learn more, contact sales@quip.com.

Conclusion

Quip transforms the way teams work together by putting communication at the center of productivity. With a consumer-grade user experience backed by enterprise-grade security, Salesforce's mobile cloud documents platform is the collaboration tool of choice for companies of all sizes across a wide range of industries. And with Quip Virtual Private Cloud, your employees get all the benefits of modern collaboration while your organization gets customized control over your critical content.

To learn more, contact sales@quip.com.

> "Immediately I saw communication pick up and how easy it was to get information out quickly to a large group."
>
> **Dave Markowski**
> Director of Salesforce, Cloud Technologies, The Warranty Group, on using Quip