Quip Shield

Overview

Modern technology and productivity tools are transforming the way employees collaborate in real-time, on any device, across the globe. But while technology increases productivity, it leaves businesses vulnerable to new security risks with serious consequences. With more sensitive data being stored and managed in the cloud, compliance requirements and penalties also become increasingly complex. Quip Shield helps address these competing factors by providing the strong security required to protect business-critical data, while still empowering teams to work quickly and collaboratively to drive business forward.

The State of Cloud Security

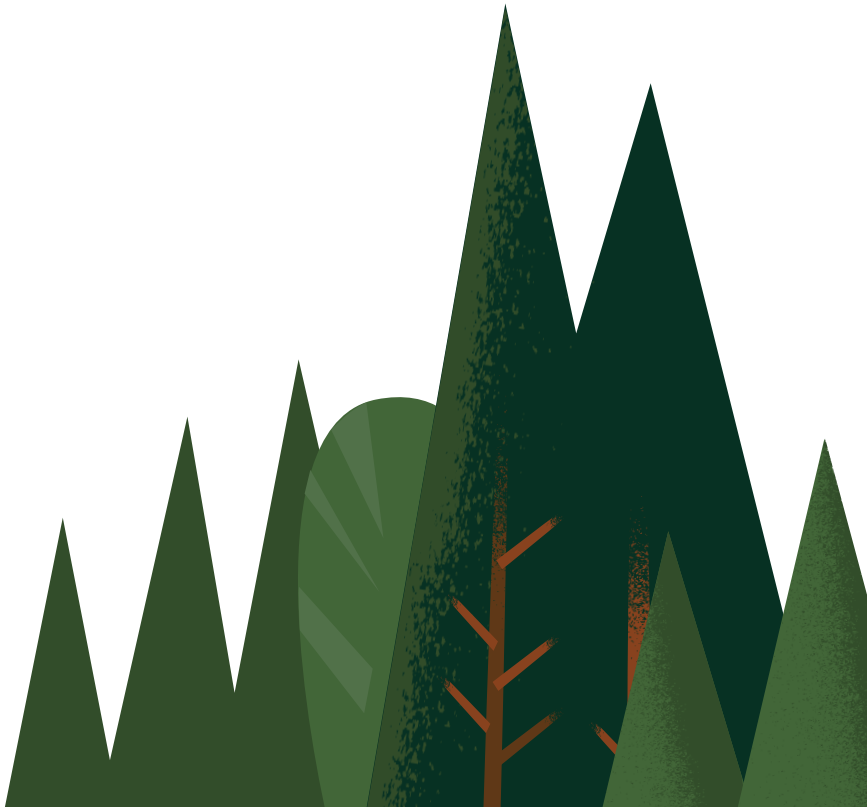
- **1 in 4**
  organizations confirmed they experienced a cloud security incident in the past 12 months*
- **39%**
  of IT leaders view legal and regulatory compliance as their biggest security concern*
- **$6 trillion**
  per year by 2021 in global losses from security breaches, including lost productivity, are forecast to double from $3 trillion per year in 2015**

* ISC2 Cloud Security Report, 2019
** Bromium CISO Report, 2017

The Quip productivity platform combines modern collaboration and best-in-class security, making it easy for teams to securely connect and collaborate – anytime, anywhere, on any device.

Quip Shield delivers an additional layer of advanced security measures to help enhance trust, transparency, compliance, and governance for the most security-conscious organizations – without impacting productivity.

- **Control and manage access to your data:** Create, manage, and control your own encryption keys. Enjoy unparalleled control of and visibility into your data privacy and utilization.
- **Enforce security and compliance policies:** Monitor critical business data via real-time, auditable event logs. Enforce regulatory compliance by triggering security policies to take specific actions against immediate threats.
- **Prevent data breaches and cyber attacks:** Control access to your corporate data, monitor for suspicious employee activity, and actively protect against malware and ransomware attacks.



salesforce

The World's Most Secure Productivity Platform

All data stored in Quip is fully encrypted and controlled out-of-the-box. From secure infrastructure services to granular permissions and external sharing controls, Quip has you covered from day one. From there, it's easy to customize the platform to meet your specific security and compliance needs, with API support for eDiscovery, Data Loss Prevention, SCIM provisioning, and more. Quip can also be deployed to your very own private cloud, providing data isolation and additional custom network controls that let you define all the rules of your cloud.

On top of all that, Quip Shield adds an additional level of security, insight, and control to help enterprises meet the highest compliance standards.

Quip Shield	Application Services	Private Cloud Services	Infrastructure Services
Enterprise Key Management	Platform Encryption	Data Isolation	Secure Data Centers
Event Monitoring	Single Sign-On	Geography Control	Backup and Disaster Recovery
Antivirus Scanning	Managed Sites	Network Egress	Third Party Certifications
	Granular Permissions	Firewall Rules	Security Audits
	External Sharing Controls	IP Restrictions	

Quip Shield is designed to help security-conscious organizations appropriately manage sensitive customer or corporate data against strict regulatory requirements, industry standards, corporate policies, and other compliance measures.

- **Financial Services companies:** Customers' PII, credit card details, health history, wealth information, and more.
- **Healthcare companies:** Protected health information (PHI) such as health history, treatment records, and personal information such as ID numbers, social security numbers, and more.
- **Manufacturing companies:** Sensitive client information, intellectual property, trade secrets, roadmap details, and more.
- **Organizations in the public sector:** Social Security numbers, fingerprints, government IDs, confidential national security details, and more.

Quip Shield Includes Three Premium Services

Enterprise Key Management
Strengthen data privacy with unparalleled control

Event Monitoring
Enforce compliance and mitigate data loss with greater visibility

Antivirus Scanning
Proactively detect and prevent malware incidents

Enterprise Key Management

Strengthen Data Privacy with Greater Control and Visibility

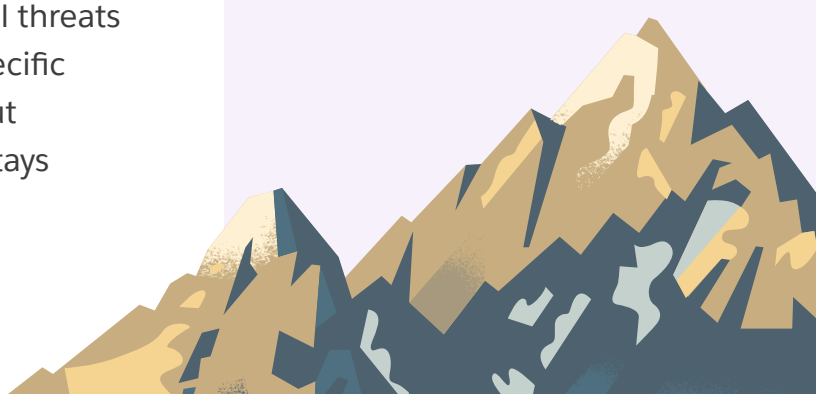
Whether they lead to exposure of confidential customer data or loss of intellectual property, data breaches represent the most financial and reputation risk to any business. As you store more sensitive and business-critical information in Quip, Quip Enterprise Key Management (EKM) ensures the privacy and confidentiality of that data to meet both external and internal compliance requirements.

Quip Enterprise Key Management (EKM) enables you to independently create, manage, and control access to your own encryption keys in Amazon Web Services (AWS). With EKM, you have greater control over who accesses your data and how, making sure your business-critical data never falls into the wrong hands. Not only do you maintain full visibility into key usage via immutable logs, but you are empowered to respond to potential threats by granularly revoking access to specific content in Quip at any time, without impacting productivity. Your data stays protected while work keeps moving forward.

The State of Cloud Security

- 27%
  of reported security incidents were related to data exposure*
- 82%
  of IT leaders say data privacy is their top security challenge*
- 95%
  of IT orgs have increased security investments due to public concern over data privacy**

* ISC2 Cloud Security Report, 2019
** Salesforce State of IT Report, 2017



FEATURES & BENEFITS

- **Key management:** Create, control, rotate, and manage the encryption keys used to encrypt your data in AWS. Maintain full control over data privacy by defining specific key policies with corresponding access and permissions.
- **Key storage and security:** Customer keys are housed in Amazon Web Services Key Management Service (AWS KMS) or AWS CloudHSM, in redundant systems that are designed with 99.99999999% durability and availability. Your keys are never stored in plaintext and are never held in memory for longer than 5 minutes, though you have the power to forcibly clear the cache at any time.
- **Granular key access controls:** Per-document encryption at the application level allows admins to revoke access to specific pieces of content in Quip, rather than revoking access to the entire service. In the case of an incident, teams experience minimal disruption while admins work to isolate and secure data, and business keeps running as usual.
- **Immutable key audit logs:** Integration with AWS CloudWatch and AWS CloudTrail provides immutable audit logs of key usage for regulatory and compliance activities. Have complete visibility into how and why your keys are being accessed and utilized, every step of the way.

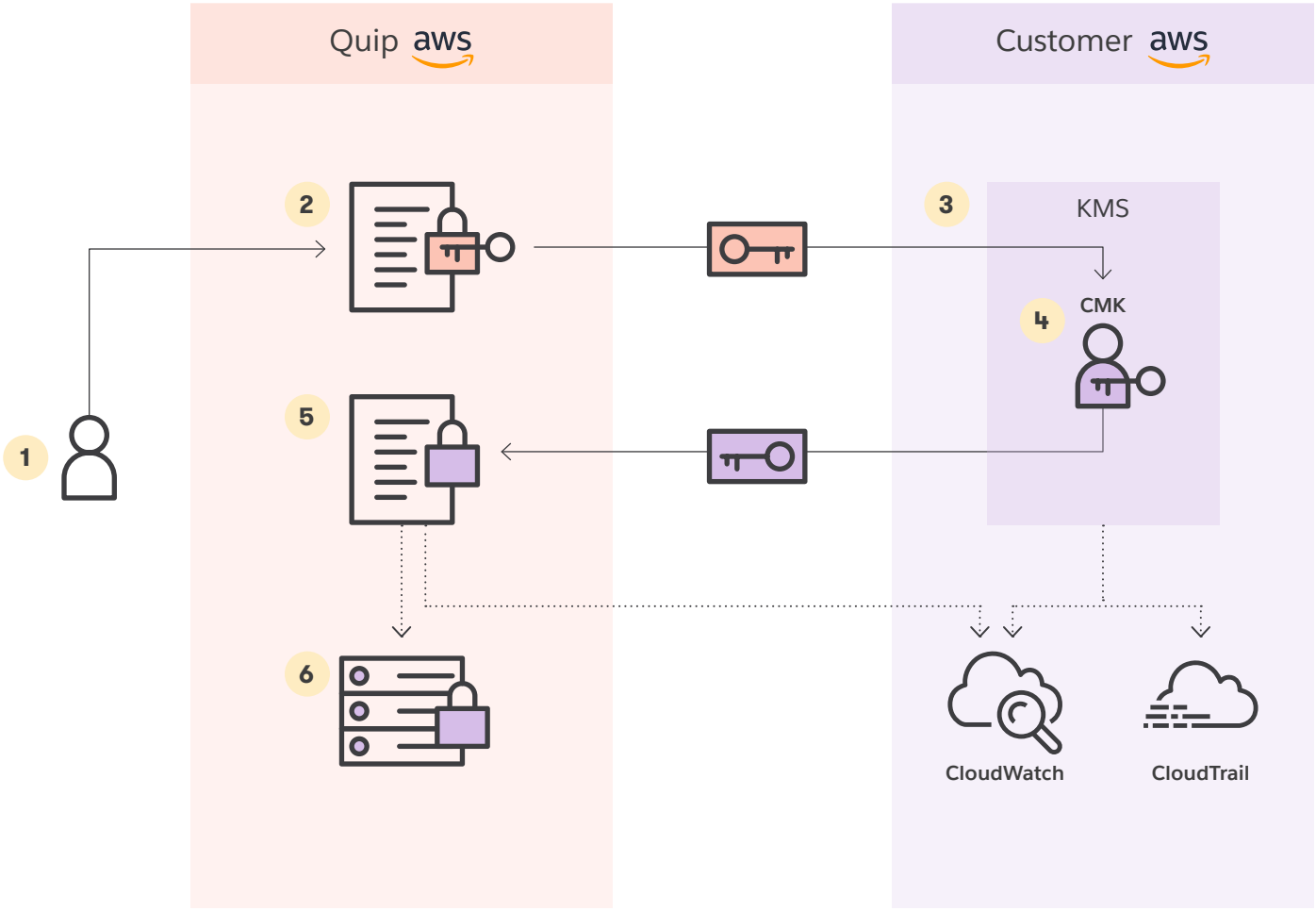
How It Works

Manage key actions in AWS

1. Create and rotate keys in KMS
2. Set up logging in CloudWatch and CloudTrail
3. Revoke key access in KMS

Manage Quip actions in the Quip Admin Portal

1. Upload Amazon Resource Names (ARN) to set up EKM
2. View encryption status
3. Clear caches and downloads



Encryption via EKM

1. Data is entered into the Quip app and sent to Quip servers
2. Quip retrieves the encrypted content-specific key using content ID
3. Quip makes an API call through the AWS KMS API**, sending the encrypted content-specific key
4. The content-specific key is decrypted using the Customer-Managed Key, and the decrypted content-specific key is sent back to Quip
    a. Use of the Customer-Managed Key is logged in CloudWatch (and optionally in CloudTrail)
5. The content-specific key is used to encrypt the content
    a. Use of the content-specific key is logged in CloudWatch
6. The encrypted data is stored in Quip databases

** If the key has been used in the last five minutes, it will be retrieved (in plaintext) from cache instead (bypassing the API call). The cache hit and KMS API bypass will be logged in CloudWatch.

System Requirements

- Available for Quip Enterprise or Quip for Salesforce
- Individual user licenses not available for purchase
- Requires subscription to Quip Shield or Quip Encryption
- Requires subscription to AWS KMS or AWS CloudHSM (not included)

Event Monitoring

Mitigate Data Loss and Strengthen Data Integrity for Compliance

Protecting against data loss can be particularly tricky. Not only do you have to protect against malicious external attacks, but you also have to mitigate risks posed by employees who can expose the organization as easily as carelessly sharing a document – or their login credentials – with the wrong person. Whether malicious or inadvertent, data loss incidents represent potentially catastrophic consequences for enterprises – particularly those that handle large amounts of sensitive data or those subject to data security regulations and regular audits.

Event Monitoring through Quip Shield empowers you with greater visibility into user activity and data usage via real-time event logs. Programmatically monitor real-time activity in Quip and set custom rules to automatically flag and address suspicious behaviors. Event Monitoring enables you to monitor for malicious or non-compliant activity, surface threats as soon as possible, and take immediate action to enforce your security policies. In the event of a security incident, easily

The State of Cloud Security

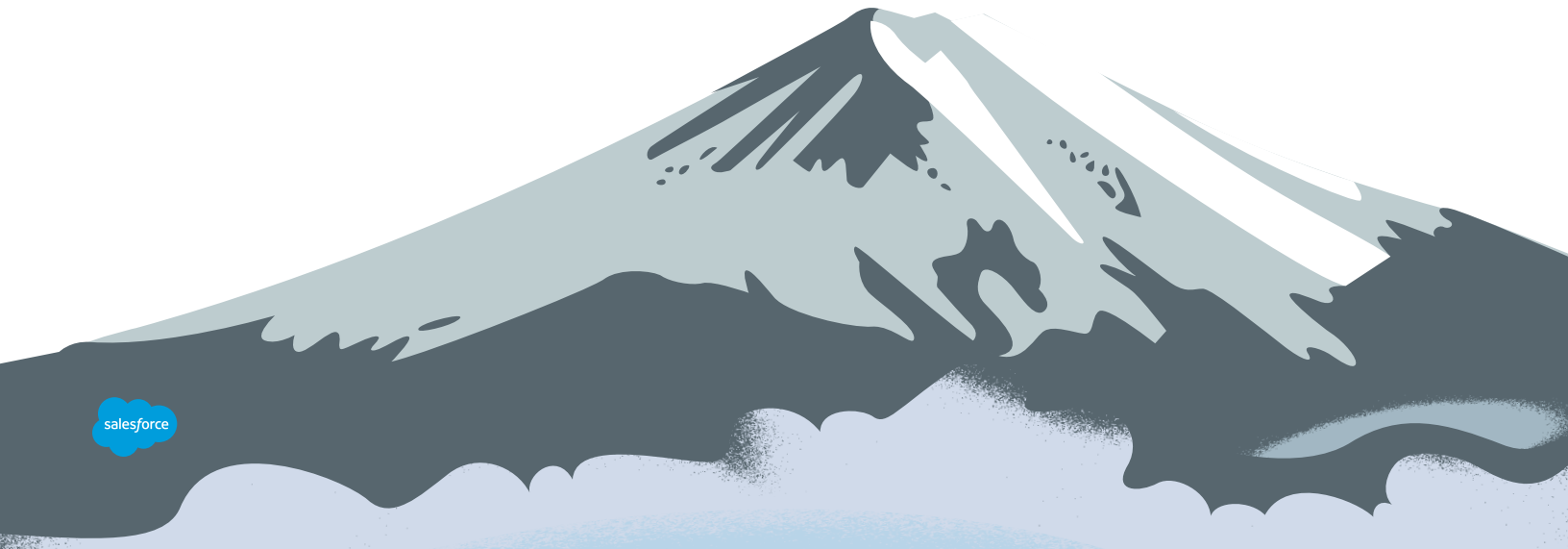
- 85%
  of IT leaders say internal security threats are as serious as external ones*
- 78%
  of IT orgs monitor how employees access and use customer data*
- 64%
  of IT leaders say data loss is their top security concern**

* Salesforce State of IT Report, 2017
** ISC2 Cloud Security Report, 2019

demonstrate compliance by delivering auditors, government regulators, or legal teams the appropriate information in an auditable format.

Feature & Benefits

- **Historical events:** Access historical logs for any event that happened more than two hours ago for retroactive investigations.
- **Near real-time events:** Access logs for events that have happened within the past two hours. Set up an ongoing stream of events to ingest the logs right after the corresponding actions happen in Quip.
- **Data visualization and analysis:** Analyze and visualize events in the tool of your choice. Event Monitoring data can be easily imported into data visualization and application monitoring tools including Splunk, GoodData, CASB providers, and more.
- **Information governance:** Easily demonstrate compliance with internal policies and industry regulations. In the event of a security incident, quickly supply auditors, government regulators, or legal teams with the appropriate information in an auditable format.



How It Works

Quip Event Monitoring provides access to API endpoints that can be used to retrieve log data for Quip actions performed by your site members.

1. Monitor data access and usage
2. Track documents and folders created, deleted, moved, copied, and shared with other users
3. Detect login compromise
4. Get alerts on usage behavior
5. Block user actions based on customizable policies
6. Identify performance concerns

System Requirements

- Available for Quip Enterprise or Quip for Salesforce
- Individual user licenses not available for purchase
- Requires approved access to the Quip Admin API*
- Subscription to data visualization and application monitoring tools not included

*Note: If you have approved access to the Quip Admin API but have not purchased Quip Shield or Quip Event Monitoring, you are **not permitted** to use the Events and Near Real-Time Events endpoints of the Admin API.

Antivirus Scanning

Proactively detect and prevent malware incidents

Increasingly sophisticated malware infections not only disrupt business operations, but can result in revenue loss, legal consequences, and reputational damages. Quip Antivirus Scanning helps protect your system from known and unknown threats, providing additional safeguards designed to prevent users from downloading potentially malicious file attachments onto their local machine.

The State of Cloud Security

- **20%**
  of reported security incidents were malware infections*
- **27%**
  of IT leaders view malware/ransomware as their biggest security threat*
- **Every 40 seconds**
  a business falls victim to a ransomware attack**

* ISC2 Cloud Security Report, 2019
** Kaspersky Security Bulletin, 2016

How It Works

Admins must enable Quip Antivirus Scanning in the Quip Shield Advanced Security tab of the Quip Admin Portal. Once the feature is enabled:

1. Files uploaded to quip are scanned for potential viruses upon initial upload
2. Users are prevented from downloading potentially infected file attachments

System Requirements

- Available for Quip Enterprise or Quip for Salesforce
- Individual user licenses not available for purchase
- Requires subscription to Quip Shield or Quip Antivirus Scanning

Quip A Salesforce Company

For more information on Quip Shield, please contact your sales representative. Visit quip.com or call 1-844-597-6576.

Quip
Salesforce Tower
415 Mission St
San Francisco, CA 94105