




How CASB Can Help You With CCPA Compliance



How CASB Can Help You With CCPA Compliance

eBook Content

What is CCPA?	2
Who Must Comply and Why?	3
What is Personal Information?	4
How Can CASB Help?	5
Visibility to Users and Data Delivers Control	6
Identify, Classify, and Protect Sensitive Data.	7
Zero Trust Encryption is the Strongest Encryption Available to Lock Down PI	8
Manage and Control User Connections by Risk Score, Geo-Location and Device and Mitigate Risky	9
Users Ensure Repositories and Files are Safe from Known Threats and Malware.	10
Simplify Access and Administration to All of Your Clouds.	11
Securely Support the Cloud Mobile World and Position for SASE.	12
Deliver the Functionality and Reporting You Need to Support CCPA Compliance.	13
The Largest Multinationals in the World Use Lookout CASB	14
About Lookout	15



What is CCPA?

The California Consumer Privacy Act:

In 2018, California passed what is considered to be the absolute toughest data privacy law in the United States. The California Consumer Privacy Act, or CCPA, was approved by the California State Governor on June 28, 2018 and went into full legal force on January 1, 2020. CCPA protects the Californians' right to privacy by ensuring the data collected by businesses about consumers now belongs to the consumers, and not the companies that collect the data. Companies that fail to implement and maintain reasonable security controls and processes will be heavily penalized. In late 2019, the California legislature passed two amendments to the CCPA for employee/applicant and "business to business" exemptions that apply until January 1, 2021.

CCPA is considered to be the absolute toughest data privacy law in the United States



Who Must Comply and Why?

The California Consumer Privacy Act (CCPA) law applies to any business that does any amount of business in the State of California, and:

- has more than \$25 million in revenue
- or, buys or sells the personal information of 50,000 or more consumers
- or, derives 50 percent or more of its annual revenue from selling consumers' personal information

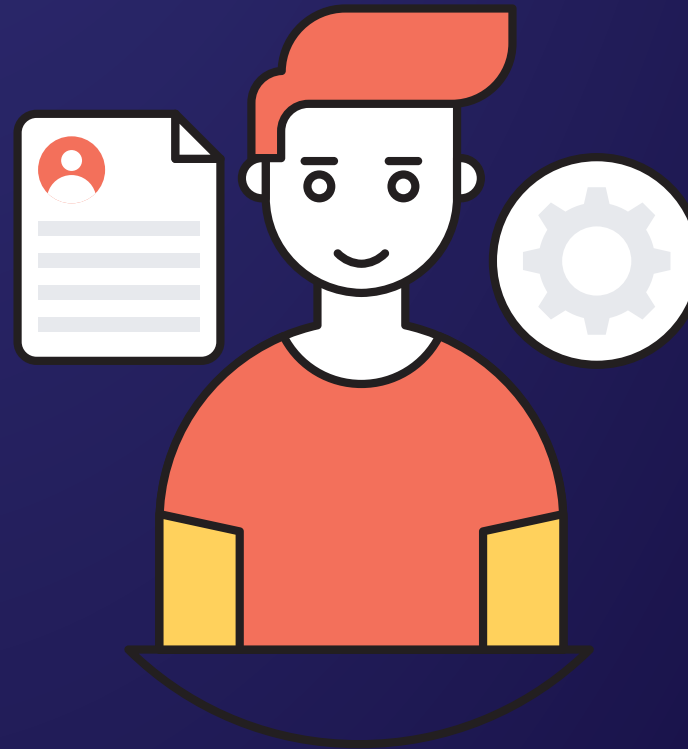




"Data is your responsibility, not the cloud provider's. When things go wrong, you are liable."

Gartner Group

What is Personal Information?



Personal Information (PI) under this law includes real name, alias, postal address, account name, social security number, driver's license number, passport number, and other similar identifiers. PI may also include many other categories of data such as:

- Biometrics and DNA data;
- Internet search and browser data geolocation data;
- and, Employment information and much more.

Business, service provider, or other person who violates its provisions, and fails to cure those violations within 30 days, is liable for a civil penalty under laws

How Can CASB Help?

CASB provides the capability you need to help you address the key requirements of CCPA:



- Securing the cloud-mobile environment, providing the building block for SASE deployment
- Deep visibility into the users and applications' activity
- Identification, classification, and protection of sensitive data with advanced Inline and Email DLPs
- Zero Trust Encryption and Information Rights Management (IRM) to encrypt the PI across the clouds and user devices
- Management and control of user connections by risk score, geo-location, and device, and mitigate risky users
- Protection of repositories and files from known threats and malware
- Simplifying access and administration to all of your clouds
- Drill-down reports needed to support CCPA compliance.

Visibility to Users and Data Delivers Control

- CASB Cloud Data Discovery (CDD) allows organizations to discover and classify historical data already stored in leading SaaS applications.
- CASB enables you to view and log all the activity in your authorized clouds, providing deep visibility into data, users, devices and infrastructure, and sharing the results over live BI backed dashboards and 30+ page detailed CIO/CISO report for audits.
- Sometimes employees may try connecting with unmanaged clouds which have a possibility of running afoul of compliance requirements, let alone fail to adequately protect confidential data. Lookout CASB enables you to see all unauthorized and out-of-policy cloud usage so you can shut it down immediately and maintain compliance.

Lookout CASB supports multi-cloud environments with one unified and consistent Zero Trust approach, providing full visibility of all cloud applications being utilized by your organization.



"Lookout is one of the few vendors that also extends its CASB functionality to email in Office 365 and G Suite, potentially making Lookout attractive to customers interest-ed in a single vendor for SaaS governance and email security." - Gartner Magic Quadrant for CASB, 2019

Identify, Classify, and Protect Sensitive Data

- CASB provides one consistent Data Loss Prevention (DLP) interface that you can use across the broad variety of clouds you deploy. DLPs are essential to identify and prevent the leak of sensitive data.
- Customers can also integrate CASB DLP policy with existing on-premise enterprise DLP systems.
- CASB brings a comprehensive Zero Trust encryption solution that protects data "at rest," in-network transit, in the cloud application layers (API, middleware, memory), and in use. Data encryption keys are strictly retained by you, not shared with the cloud providers.
- CASB protects offline data shares with native Information Rights Management (IRM) support.





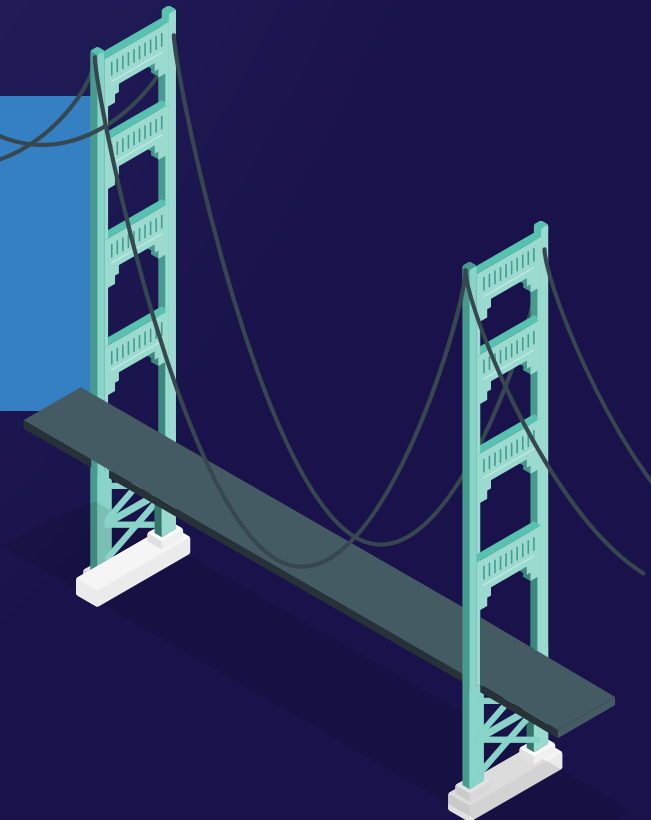
Zero Trust Encryption is the Strongest Encryption Available to Lock Down PI

"It is my strong recommendation that companies and agencies implement encryption as basic protection and reasonable security measure to help them meet their obligation to safeguard personal information entrusted to them."

- **Kamala Harris**
US Vice President

"Use encryption to separate data holding from data usage. Segregate key management from the cloud provider hosting the data."
Cloud Security Alliance

Lookout CASB allows you, and only you, to manage the data encryption keys that protect your data in the cloud. No one else will have any access to your data, including any 3rd party that might be forced to provide access to your data encryption keys which can then unlock your encrypted data.



Lookout CASB continuously profiles data attributes and user behavior to detect activity that is out of the ordinary for your enterprise.

Manage and Control User Connections by Risk Score, Geo-Location and Device and Mitigate Risky Users

- Technologies such as User and Entity Behavior Analytics (UEBA) and Adaptive Access Control (AAC) can identify anomalous behavior by an authorized user with valid credentials and shut down the access in real-time.
- User anomalies include downloading of gigabytes of files at 2 am, or perhaps attempting a valid log-in from Beijing only two hours after logging in from Chicago, Illinois.
- CASB continuously monitors and updates the user risk scores and when a risk score exceeds the threshold and breaks policy, CASB immediately terminates the user connection or prompts the user to reconnect with step-up authentication.



Ensure Repositories and Files are Safe from Known Threats and Malware

- CCASB anti-virus anti-malware (AVAM) solution scans all inbound and outbound clouds for the detection of many types of malware, such as zero-day threats, viruses, spyware, ransomware, worms, and bots.
- Any additional files uploaded to your SaaS applications are protected from carrying malicious content that can affect users.
- As with high-risk users, you can leverage your existing security ecosystem to optimize response to known threats and malware.



Cloud Access Security Brokers (CASB) such as those offered by Lookout brings a single unified platform to provide the necessary visibility, data protection, threat protection, and compliance support for all of your clouds.

The Lookout platform allows you to integrate with existing enterprise security solutions to optimize existing investments.



Simplify Access and Administration to All of Your Clouds

- CASB provides full support for SAML integration and Single Sign-On (SSO) to streamline and protect authentication, and to maintain comprehensive logging of user access.
- CASB provides a single way to administer security across all of your SaaS cloud providers, custom cloud applications, and more.



Lookout CASB combines with IDaaS solutions to deliver end-to-end user and data security from any device, any location, to all trusted cloud applications, providing organizations a first step to achieve Zero Trust Cloud Security.



Securely Support the Cloud Mobile World and Position for SASE

- CASB provides all of the integrations you need to securely share information between systems using native application program interfaces (APIs). This consolidation reduced the extreme complexity of trying to use multiple security solutions. You can consistently administer policies across the cloud and other platforms.
- CASB acts as the cloud security building block, enabling integration with best-of-the-breed network security and network optimization apps for offering a comprehensive Secure Access Service Edge (SASE) solution, enabling accelerated and secure cloud adoption.





Lookout, a leader in cloud security, provides an award-winning cloud security platform that delivers powerful end-to-end protection for data resident in the cloud, threat prevention, visibility, and compliance, so enterprises can adopt the cloud with confidence.

Deliver the Functionality and Reporting You Need to Support CCPA Compliance

- CASB provides detailed logs and reporting on access and download of PI and other sensitive information.
- Specific regulatory compliance is easily achieved.
- Hybrid deployment can uniquely support complex international and local compliance requirements.





The Largest Multinationals in the World Use Lookout CASB

- 5 of the Top 10 U.S. Banks
- 6 of the Top Banks Worldwide
- 3 of the Top 10 Insurance Firms
- 3 of the Top 10 U.S. Health Care Firms
- 3 of the Top 10 Pharmaceutical Firms
- 2 of the Largest Telecommunications
- Firms Government agencies in the United States, United Kingdom, Canada, Australia, and beyond





About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit www.lookout.com and follow Lookout on its blog, LinkedIn, and Twitter.

