



Why Do Companies Need a CASB?



White Paper
February 2019



Why Do Companies Need a CASB?

If your company uses the cloud, a Cloud Access Security Broker (CASB) is mandatory. In fact, the world's leading research and advisory firm, Gartner, Inc., ranks the CASB as #1 on its list of Top 10 Information Security Technologies companies need today.

Massive adoption of cloud services and applications has created new targets and threats like never before. Do your employees use Office 365 or Salesforce? How about Dropbox, Facebook, Twitter, LinkedIn, Google Drive, Evernote or iCloud? If so, your company needs a CASB.

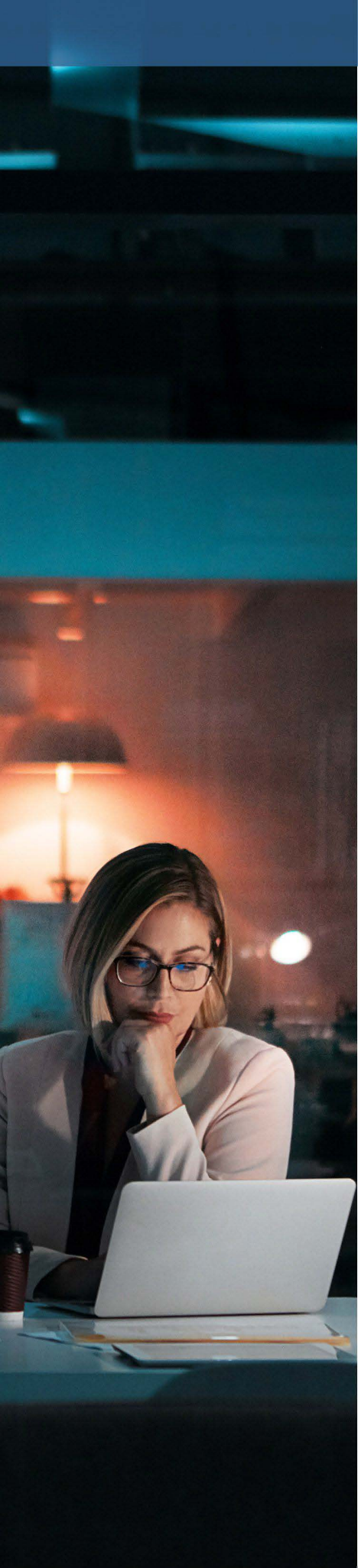
What's more, the widespread use of mobile devices is the new reality: companies regularly interact with users they don't manage. Your systems, applications and data are in regular contact with mobile phones, tablets and laptops you do not control. In fact, an estimated 86% of workflows are in the cloud today.

Gartner predicts that 95% of all security failures in the cloud will be from human error. Manual and people centered cloud security approaches will not work. They need to be augmented by automation.

Enter the CASB.

Using machine learning and automation, the CASB provides critical control points for secure and compliant cloud use across multiple providers. This protection centers around four key components of cloud security: Visibility, Compliance, Data Security and Threat Protection. Instead of relying on manual processes to identify risk, the CASB does it for you -saving significant time and human error.

Due to some faulty assumptions, enterprise security budgets don't always include Cloud Security. Many companies assume their cloud services provider will handle all the security they need. This is not true. Cloud service providers are responsible for security of the cloud, you are responsible for the security of your own content in the cloud. They also assume the enterprise SIEM security investment includes cloud security. This is not necessarily true. The good news is a CASB integrates with existing SIEM enterprise security to maximize your protection.



To better understand why companies need a CASB, it's important to answer some key questions and evaluate the true cost of not protecting your data with a CASB:

Visibility

- Who is accessing what applications?
- Who is accessing unsanctioned applications?
- What are unmanaged users doing?

The CASB discovers compromised credentials, and malicious sites. It calculates risk and assesses enterprise readiness to manage threats.

Compliance

- Are my DEvOps compliant?
- Are my access keys non-compliant?
- Are there any over privileged users in my systems?

The CASB insures you remain compliant with data regulations based on your industry. Nearly half of all cloud application activities originate from a mobile device. One third of all DLP policy violations occur on a mobile device.

Data Security

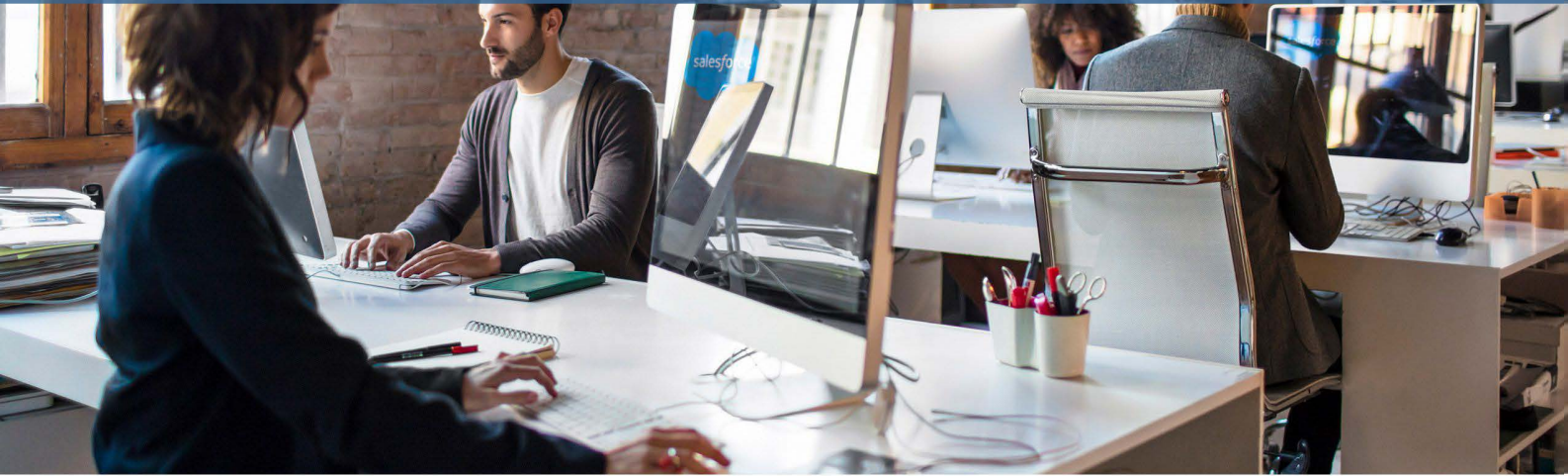
- Who is sharing data publicly?
- Am I sharing in the security responsibility with my cloud provider and SIEM solution?
- Are there any security holes in my DevOPs?

The CASB encrypts sensitive data at rest and in motion across the network. It protects confidential data in sanctioned applications and prevents IP upload to unsanctioned applications.

Threat Protection

- Who are risky users in my systems?
- How fast can I stop risky user activities?
- How fast can I stop risky applications?

The CASB shares threat intelligence with other technologies such as endpoint detection and response (EDR) and sandboxes. It blocks or remediates malware in both sanctioned and unsanctioned applications, and it detects and remediates ransomware.



If your security team cannot answer these important questions around these four pillars of cloud security, you need a CASB to provide a cost effective way to make sure you can answer them effectively.

From a business perspective, the ROI of a CASB far outweighs its cost. What would be the financial cost of a data breach? What is the financial exposure of not having a CASB? What would be the cost of compliance violations, lost intellectual property, or damage to your brand from a cloud security breach?

Here are just a few examples of business justifications for a CASB:

Preserves Brand & Protects Intellectual Property

What would be the cost to your brand if a malicious insider or outsider stole your intellectual capital such as trade secrets and patents? The true cost of intellectual property loss is estimated to be 40 million dollars per incident. Research also shows that reputation damage and lost customers due to a data breach can cost approximately \$239 per hour.

Prevents Compliance Violations

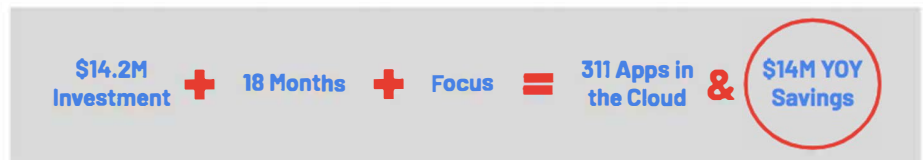
The CASB solution helps enterprises avoid the costs from violations posed by international security regulations such as HIPAA, PCI Data Security Standard and GDPR. In the healthcare industry, its estimated that just one HPA violation could cost over 1.5 million dollars per year.



Maximizes Cloud Investment

The cost of protecting your data in the cloud is small when compared to the annual savings of operating in the cloud. The CASB is your insurance policy that ensures you can continue to realize the business benefits and cost savings of operating in the cloud.

What's your business case for being in the cloud?



Annual Cloud Savings > **Annual Cost of a CASB**

* GE Oil & Gas Case Study

A cloud access security broker provides full visibility into general cloud application usage, data protection, and governance over your complete cloud environment so you can ensure your data is safe while avoiding costly breaches or non-compliance fines.

The Largest Multinationals in the World Use Lookout

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.