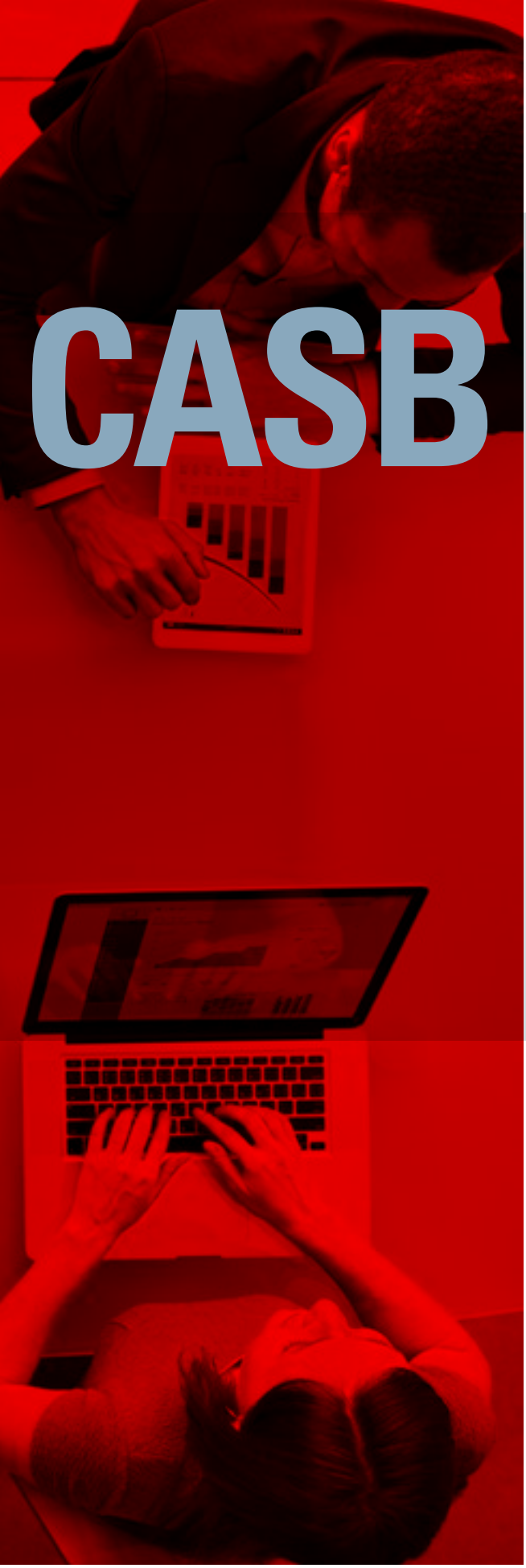
ORACLE

Making the Case for a Cloud Access Security Broker (CASB)



What is a Cloud Access Security Broker (CASB)?

Cloud Access Security Brokers are one of the fastest growing security technologies today because they provide cloud service visibility, data security, threat protection, and compliance. CASBs are an effective and easy way to mitigate the top cloud security threats and security practitioners look to trusted CASB providers as strategic partners to help advise on key cloud security decisions.

According to Gartner, by 2020, 85% of large enterprises will use a cloud access security broker solution for their cloud services, which is up from fewer than 5% in 2015.

> *"By 2020, 85% of large enterprises will use a cloud access security broker solution for their cloud services"*
>
> Gartner.

The Real Costs of Security

Leveraging cloud technology enables your enterprise to be more agile and competitive while significantly reducing costs. However, there are risks associated with these benefits. Getting new capabilities quickly is worth far less if it means exposing vulnerabilities that result in regulatory compliance violations and fees, loss of intellectual property (IP), loss of customer data, or damage to your reputation, brand, and future business.

Whether using software as a service (SaaS), platform as a service (PaaS), or infrastructure as a service (IaaS), cloud security is a mandatory cost of doing business. In June 2016, Gartner issued a press release identifying the top information security technologies and CASBs are at the top of that list. Protecting your data and IP in the cloud are essential.

Quantifying the Value of a CASB

How do you quickly quantify the additional value a CASB provides so that it gets a high priority in your already stretched information security budget?

This white paper helps build a business case by highlighting the cost considerations and payback of a CASB. It demonstrates that a CASB can provide stronger cloud protection at a lower cost than traditional security processes and tools.

Why CASBs Are Mandatory for Cloud:

The rise of SaaS is no longer a surprise—it's pervasive.

The Cisco Global Cloud Index reports that by 2018, 58% of all cloud workloads will be SaaS. Even the financial services sector—long considered a laggard in SaaS adoption—now uses SaaS for 42% of its apps. Equally important, employees are using unsanctioned cloud applications (those installed without the permission of the IT group) at an alarming rate.

Adoption of IaaS is growing rapidly.

IaaS is considered the fastest-growing cloud services market. The market was forecast to reach US$22.4 billion in 2016. Many enterprises are moving their entire infrastructure to the cloud.

The network perimeter has eroded.

Your employees use smartphones and tablets and work at remote locations around the globe. Gartner predicts that by 2017, 50% of employers will require employees to supply their own devices for work rather than using company-owned devices. As well, Cisco states there will be a 73% growth in mobile devices from 2014 to 2018.

Plus, with an estimated 86% of all workloads in the cloud by 2019, most corporate application and data interactions will be done with unmanaged users and devices.

> *"Estimated 86% of all workloads in the cloud by 2019, most corporate application and data interactions will be done with unmanaged users and devices."*

You can't hire your way out of this problem.

IT security talent is in short supply. The ISACA, a nonprofit information security advocacy group, predicts there will be a global shortage of 2 million cybersecurity professionals by 2019. Every year in the US, 40,000 jobs for information security analysts go unfilled, and employers are struggling to fill 200,000 other cybersecurity related roles, according to cybersecurity data tool CyberSeek. The evidence is mounting that people-centric approaches won't work. In practical terms, success with this approach is nearly impossible because of the time and cost associated with manual forensics and the lack of skilled labour. Instead a CASB does it for you—saving time and eliminating human error.

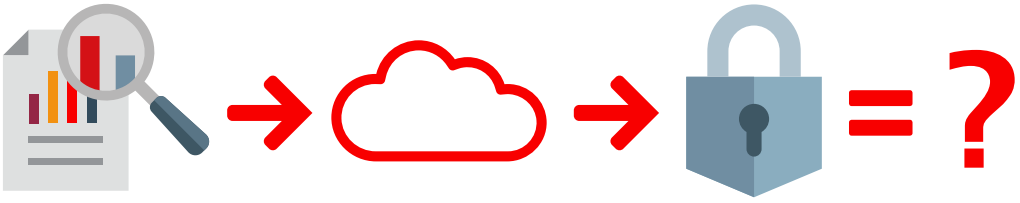
A CASB uses machine learning and automation to provide a secure and compliant use of cloud services across multiple providers and technologies. For example, a CASB should include integration with your existing enterprise security solutions such as security information and event management (SIEM), identity as a service (IDaaS), and next generation firewalls (NGFW).

SHORTAGE OF 2,000,000 CYBERSECURITY PROFESSIONALS BY 2019

"The ISACA, a nonprofit information security advocacy group, predicts there will be a global shortage of 2 million cybersecurity professionals by 2019."

Adding Cloud Security to Your Budget

Your IT or security budget must cover protection for applications (SaaS), platform (PaaS), and infrastructure (IaaS). Leading organizations often rank security projects according to their overall value to the business. Let's examine how to calculate the value of cloud security and prioritise it relative to other IT and network security projects.



1 Calculate the financial exposure of not having a CASB • Compliance violations • Lost IP • Damage to brand • Disruption to business	**2** Align cloud security spending with business objectives	**3** Calculate cost savings for cybersecurity expertise through automation

TABLE 1: Valuing Cloud Security

The first item above is insurance—how much you save when you avoid the problem. The second item is based on the business case you built when you moved to the cloud versus the annual cost of implementing a CASB to provide cloud security.

The third demonstrates the dollar savings for skilled cybersecurity professionals.

Demonstrate the Financial Exposure of Not Having a CASB

There are numerous regulatory and compliance requirements that organizations need to follow as a course of doing business. Violations can mean huge fines and damage to brand reputation. In addition, breaches from both external and internal sources can lead to IP and data theft, causing equity loss and fees from potential lawsuits.

The cost of compliance violations, damage to brand and reputation, and the loss of future business can be substantial. It's important to calculate and include the following costs you would potentially avoid as part of a business case for a CASB:

Compliance Violations

A number of industries have general compliance regulations about using technology safely to reduce the risk of compromising customer or patient data. A CASB imposes controls on cloud usage to ensure compliance with specific industry regulations such as the Health Insurance Portability and Accountability Act (HIPAA) for the healthcare industry. The table below shows current average penalties that a breach of patient information can incur.

VIOLATION	FINE
Health and Human Services (HHS) fine	Up to US$1.5 million per violation per year
Federal Trade Commission fines	US$16,000 per violation
Class action lawsuits	US$1,000 per record
State attorney generals	US$150,000 to US$6.8 million

TABLE 2: Average Cost of HIPAA Violations

Note that some IaaS offerings include compliance options with their services. These are meant to keep you in compliance with your industry requirements, but they do not set compliant configurations on your behalf. You must review their instructions and do it yourself. And the compliance setups provided by vendors pertain only to the IaaS cloud infrastructure, not to those users who access the data. Compliance rules and capabilities can instead be built into the CASB and automated so that you are fully compliant and avoid these penalties.

Lost Intellectual Property

Organizations are beginning to trust the cloud with their IP and they require consistent hybrid cloud security. This means having the same level of security controls on premises that they have in the cloud.

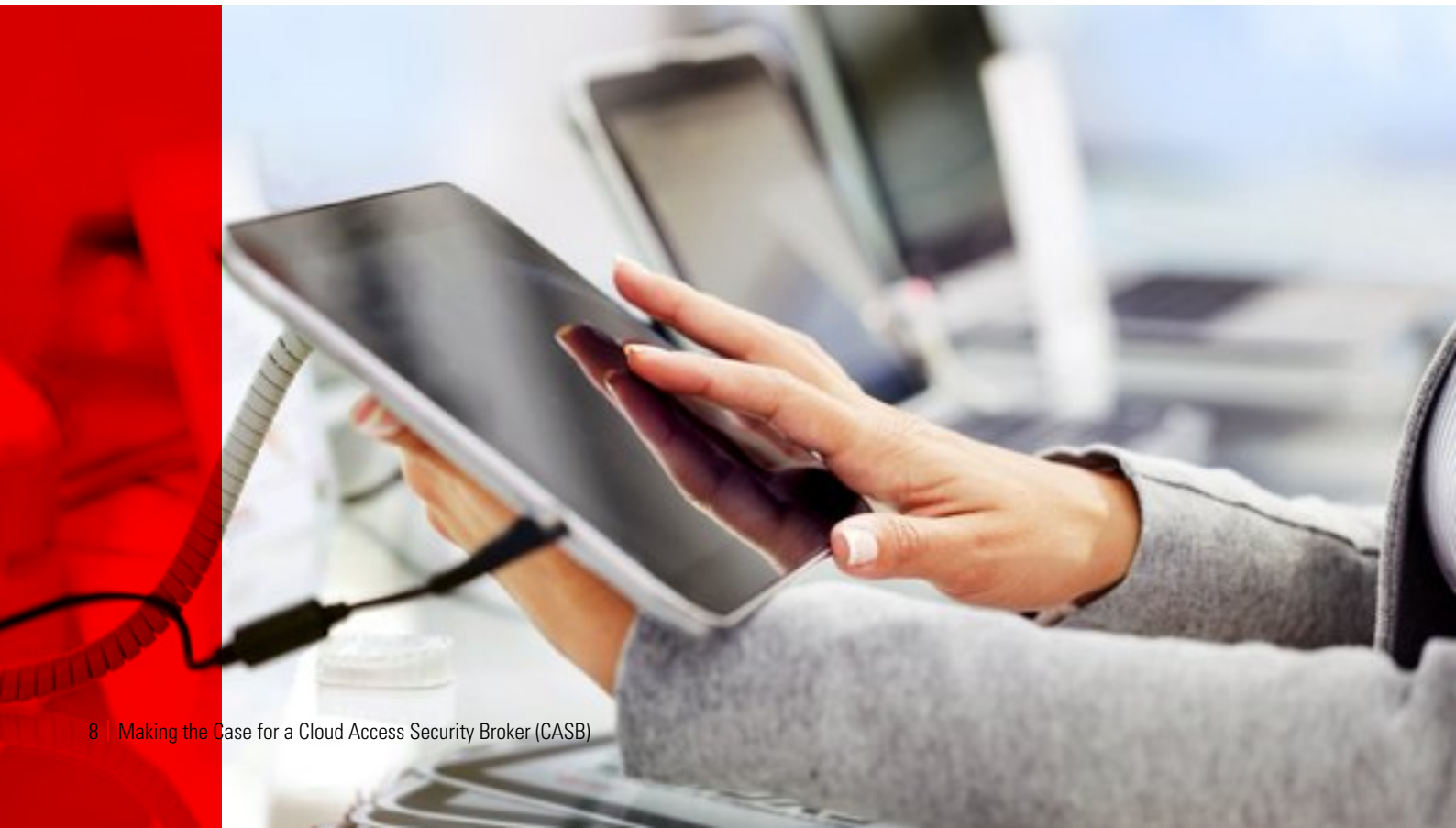
Losses can be nearly inestimable if trade secrets, patents, intellectual capital, and other corporate-sensitive data are stolen.

Damage to Brand

Brand damage occurs when news of a breach or loss of sensitive data is publicised and customers lose trust. The Ponemon Institute estimates that US$239,000 in hourly losses can be attributed to reputation damage and churn.

Disruption to Business

With organizations moving critical data and applications to the cloud, any disruption to their cloud environment will have direct impact on the overall business. E-tailers who process orders via their website hosted on IaaS can experience sudden stoppage of orders. Organizations relying on SaaS, such as Microsoft Office 365, may no longer be productive. Such disruptions can result in significant loss of business as well as customers and partners.



Align Cloud Security Spending with Business Objectives

One of the best ways to get a cloud security budget approved is to align cloud security spending with business objectives. Your enterprise is leveraging the cloud today because it enables business's objectives—most likely improved agility or cost savings.

You need to make a business case that cloud security expenses are minimal compared to the value from the cloud, and emphasise that cloud security is mandatory to ensure that agility and cost savings can be realized.

There's a good chance that you already have a business case for moving to the cloud. The following example from a major energy company demonstrates cost and operational benefits of moving to the cloud with a year-on-year savings of US$14 million. While not every company has that type of savings, chances are your company is enjoying tremendous savings from the cloud.

BUSINESS AGILITY	OPERATIONAL RESILIENCE	COST AVOIDANCE	WORKFORCE PRODUCTIVITY	OPERATIONAL COSTS
77% faster to deliver business applications	98% reduction in P1/P0 events	52% average TCO savings	15 automated bots developed	35% reduction in compute assets (792)
Rapid experimentation	Improved security posture	80% cloud first adoption	8 cloud migration parties	59 applications decommissioned
Reduced technical debt	15 cloud services created		Shift to self-service culture	US$14 million year-over-year savings
Streamlined M&A activity	Improved performance		DevOps in practice	US$14 million year-over-year savings
US$14.2 million invested + 18 months + focus = 311 apps in cloud & US$14 million annual savings				

TABLE 3: A Major Energy Company Costs: Operational Benefits of Moving to the Cloud

After calculating the cloud business case for your organization, you will need to calculate the cost to implement and maintain a CASB. A CASB vendor can help assess your environment and requirements. Be sure to ask the vendor for a no-cost proof of value.

Once you have analyzed the value and the cost, subtract the cost of the CASB from the cloud business case. Cloud security can be easily justified when measured against the advantages of the cloud. You will be able to demonstrate that the cost of a CASB (which is a mandatory control to ensure that you achieve your business objectives) is a fraction of the benefits that you will realize from the cloud.

"According to a Ponemon Institute study, the average time to identify a data breach is 201 days, and the mean time to contain it is 70 days. That's a total of 2,168 hours at US$112 per hour, or US$242,816 for just one breach."

US$242,816 FOR JUST ONE BREACH

Cost Savings for Cybersecurity Expertise Through Automation

A CASB can automate the detective work—or forensics—for cloud-related security incidents, accelerating completion of the work from weeks to minutes.

There are generally four phases of forensics:

1	2	3	4
Data aggregation from multiple cloud providers	Analysis of the aggregated data, such as comparing events against known threats, finding patterns of deviation, and identifying the most likely causes of an incident	Prioritization of the data gathered into actionable recommendations	Remediation, or taking action when human operators analyze, prioritise, and act on events, they spend significant time up front learning about the cloud parameters. On average, it takes 2 to 3 weeks for an engineer to learn security parameters, and it might be months before an engineer can absorb them all.

TABLE 4: The four phases of forensics

Remember, people cost money, are slower and more error-prone than automated systems.

A CASB with sophisticated automation capabilities can cut this cost significantly

If the cost to own and maintain a solution or the cost of deterring a breach is greater than the value you derive from your cloud service, your enterprise computing expenses are out of balance.

CASBs, designed to secure cloud services, are better equipped to secure modern businesses than traditional security appliances. The size and complexity of today's attack surface makes it costly to identify, correlate, categorise, and act on anomalies. These costs surface in hourly forensic analyst wages and the amount of time a cloud service is vulnerable while humans struggle to secure it.

If you find that a CASB aligns with how your business uses the cloud, the next step is to find the CASB that's as cost-effective and secure as possible.

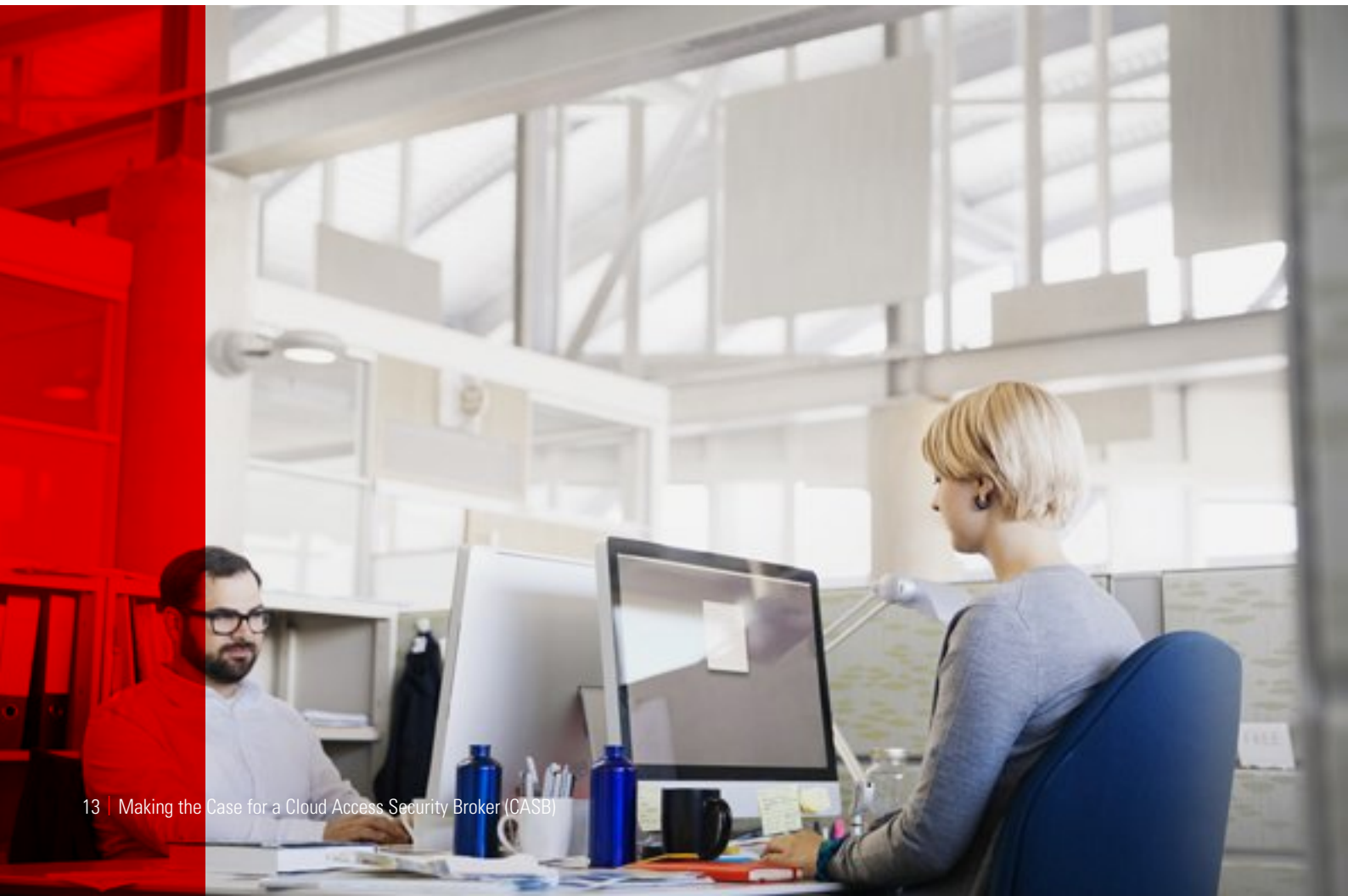
Oracle CASB Cloud Service

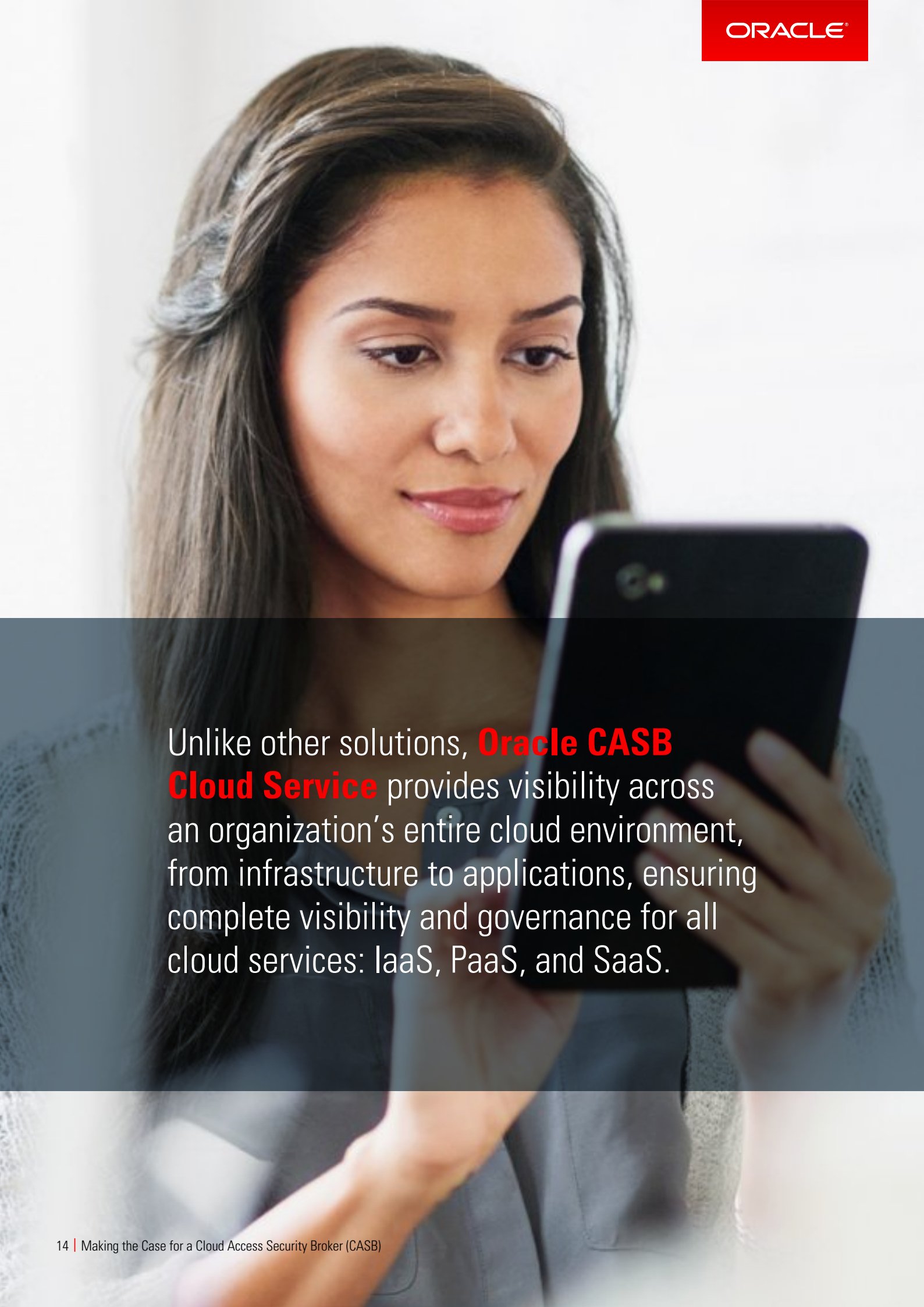
Not all CASBs are created equal, so it is important to carefully evaluate your alternatives before selecting a CASB partner. Oracle is the leader in CASB and cloud security automation, securing both sanctioned and unsanctioned cloud applications.

Unlike other solutions, Oracle CASB Cloud Service provides visibility across an organization's entire cloud environment, from infrastructure to applications, ensuring complete visibility and governance for all cloud services: IaaS, PaaS, and SaaS.

While other vendors use proxy modes that can result in performance degradation and compatibility issues, Oracle CASB Cloud Service is natively built on an API architecture, so there is no need for hardware, software, or agents.

Oracle CASB Cloud Service is a multimode through integration with leading in-line solutions, including secure web gateways (SWG), next-generation firewalls (NGFW), identity as a service (IDaaS), and security information and event management (SIEM).





Unlike other solutions, **Oracle CASB Cloud Service** provides visibility across an organization's entire cloud environment, from infrastructure to applications, ensuring complete visibility and governance for all cloud services: IaaS, PaaS, and SaaS.

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

oracle.com

Integrated Cloud
Applications & Platform Services