

## Working the Numbers

How to Quantify the Value of a Cloud Access Security Broker

ORACLE WHITE PAPER | JANUARY 2017





## The Challenge of Measuring the Return on Investment of Security

Measuring the ROI for information security technology is challenging.

Enterprises often treat information security technology as an insurance policy against the potentially devastating costs of not deploying it. From that perspective, your security technology's ROI is determined by the time it takes for a breach—one with costs equal to or greater than your investment—to occur. Your ROI could be immediate. Or it could be longer term. With that in mind, it is hard to justify yet another security technology, but a move to the cloud suggests that you should.

If you are leveraging cloud technology today, you are likely doing it because it 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 cracking a hole in your security armor that results in industry compliance violations and fees, loss of intellectual property (IP), loss of customer data, and damage to your reputation, brand, and future business.

Whether you are leveraging the cloud for software as a service (SaaS), infrastructure as a service (IaaS), or platform as a service (PaaS), cloud security is a mandatory cost of doing business. In June 2016, Gartner issued a [press release](#) identifying the top information security technologies and included cloud access security brokers (CASBs) at the top of that list. Protecting your data and IP in the cloud is not an option.

Knowing that an ROI for a CASB could be longer term, 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 you to build a business case by walking you through the cost considerations and payback of a CASB. It demonstrates that a CASB provides stronger cloud protection at a lower cost than traditional security processes and tools.



## Why CASBs are Mandatory

Let's take a look at why you need a CASB:

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

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

### Adoption of IaaS is growing rapidly.

IaaS is considered the fastest-growing cloud services market, and the market as a whole was [forecast to reach US\\$22.4 billion in 2016](#). Many enterprises are moving their entire infrastructure to the cloud. For example, GE made a strategic decision to be [100 percent public 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 percent of employers will require employees to [bring their own devices](#). And Cisco believes that there will be a [73 percent growth in mobile devices](#) from 2014 to 2018. Combine these facts with an estimated [86 percent of all workloads](#) existing in the cloud by 2019, and it is reasonable to assume that a high percentage of corporate apps and data interactions are being done by unmanaged users and devices.

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

The top-paying cybersecurity job is a security software engineer with an average annual salary of \$233,333, according to a [May 2015 report](#) from the job board Dice. That tops the salary for a chief security officer, which is \$225,000. And these professionals are an increasingly scarce resource. In 2014, the [Cisco Annual Security Report](#) warned that the worldwide shortage of information security professionals was at 1 million. Michael Brown, former [CEO at Symantec](#), expects that to rise to 1.5 million by 2019. The evidence is mounting that people-centric approaches won't work.

Massive adoption of cloud services means that they are the new norm for holding mission critical enterprise data, IP, and other assets. Because of that, cloud services are now the target of outside hackers and suspect insiders. Securing your growing cloud services with traditional tools and cybersecurity professionals has grown unwieldy, requiring integration and management of 20 or more different security products. In practical terms, success with this approach is nearly impossible because of the time and cost associated with traditional, manual forensics and a dearth of skilled labor.

A CASB uses machine learning and automation to provide a critical control point for the secure and compliant use of cloud services across multiple providers. Centered on delivering visibility, compliance, data security, and threat protection, 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). Instead of relying on manual processes for identifying and remediating risk, the CASB does it for you—saving significant time and eliminating human error.

## Adding Cloud Security To Your Budget

To prevent cloud security from falling through the cracks, your enterprise IT or security budget needs line items for security for both applications (SaaS) and infrastructure (IaaS). If your company ranks security projects according to their value, calculate the value of cloud security and prioritize it relative to other IT and network security projects.

**TABLE 1. HOW TO PLACE A VALUE ON CLOUD SECURITY**

**1. Calculate financial exposure of not having a CASB**

- » *Compliance violations*
- » *Lost IP*
- » *Damage to your brand*

**2. Align cloud security spending with business objectives**

**3. Calculate cost savings for cybersecurity expertise through automation**

The first item above is insurance—that is, the value is realized when you avoid the problem. The second item is based on the business case that you built when you moved to the cloud versus the annual cost of implementing a CASB to provide security for your cloud investment. 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 enterprises need to follow as a course of doing business. When found in violation of these requirements, huge fines and damage to brand reputation can result. In addition, breaches from both external and internal sources can result in 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 in your CASB business case the savings associated with the following:

### Compliance Violations

A number of industries have general compliance regulations about using technology safely in ways that minimize the risk of customer or patient data being compromised. 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.

**TABLE 2. AVERAGE COSTS OF HIPAA VIOLATIONS**

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

Note that some IaaS offerings include compliance options with their services. These are intended to help 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

People are beginning to trust the cloud with their IP, so they need the same level of security controls whether data resides in the cloud or on their premises. A pharmaceutical company might be developing the next generation of drugs or a car manufacturer might be designing the next innovation in vehicle safety. Customer data is also a valued asset. In general, equity losses can be nearly inestimable if trade secrets, patents, intellectual capital, and other corporate-sensitive data are stolen.

### Damage to Your Brand

Brand damage occurs when news of a breach is publicized and customers and partners get cold feet about the safety of doing business with the enterprise. The [Ponemon Institute](#) estimates that US\$239,000 in hourly losses can be attributed to reputation damage and churn.

## Align Cloud Security Spending with Business Objectives


One of the best ways to get your cloud security budget approved is to align cloud security spending with business objectives. Your enterprise is leveraging the cloud today because it enables one or more major business 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 that the organization receives from the cloud, and emphasize that cloud security is mandatory to ensure that agility and cost savings (your business objectives) can be realized.

There's a good chance that you already have a business case for moving to the cloud. Here is an example of a cloud business case from [GE Oil & Gas](#) to demonstrate their cost and operational benefits of moving to AWS. In this example, GE was able to demonstrate year-over-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.

**TABLE 1. GE OIL AND GAS' COSTS AND OPERATIONAL BENEFITS OF MOVING TO 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\$14.2 million invested + 18 months + focus = 311 apps in cloud & US\$14 million annual savings**



If you have an existing cloud business case similar to GE's with an annual savings number, use it. If not, you can calculate the value of the cloud for your enterprise. What can you do using cloud services that you wouldn't otherwise be able to do? What cost savings are you able to realize?

Next, you 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.

## Demonstrate Cost Savings for Cybersecurity Expertise Through Automation

A CASB can automate the detective work, or forensics, related to cloud-related security incidents, accelerating completion of the work from weeks or months to mere minutes. There are generally four phases of forensics:

1. Data aggregation from multiple cloud providers
2. 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
3. Prioritization of the data gathered into actionable recommendations
4. Remediation, or taking action

Traditional approaches to these four forensic steps place a heavy emphasis on manual labor, while CASBs shift the emphasis to codifying events, outcomes, and actions in software.


When human operators analyze, prioritize, 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.

People cost money. And people are slower and more error-prone than automated systems. According to a [Ponemon Institute](#) study, the mean time to identify a data breach is 201 days (with a range of 20-569 days), and the mean time to contain is 70 days (with a range from 11-126 days). That's a total of 2,168 hours at US\$112 per hour, or US\$242,816 for just one breach. A CASB with sophisticated automation capabilities can cut this cost by 20 to 80 percent, depending on the number of cloud providers and number of cloud services in use with each provider.

## Summary

As new risks to the IT environment emerge, it's critical for IT security budgets to account for these risks. Cloud services open up a wealth of capabilities and benefits, but they also introduce new risks that need to be mitigated. If you can determine the value of the cloud services to your organization and subtract what it costs to secure it, you will be left with a net value of using those services. 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.

Automated systems such as CASBs do a better job of securing cloud environments than traditional manual processes. The size and complexity of today's attack surface makes it costly to identify, correlate, categorize, and act on anomalies. These costs are in both hourly forensic analyst wages and the amount of time a cloud service is vulnerable while humans attempt to secure it.



If you find that a CASB aligns with your business objectives for doing business in the cloud, the next step is to find the CASB that's as cost-effective as possible and provides the most comprehensive security available.

### 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, the Oracle CASB Cloud Service platform provides visibility across the entire security lifecycle from infrastructure through applications, ensuring complete visibility and governance for all cloud services including IaaS, PaaS, SaaS. While other vendors use proxy modes that can result in performance degradation and compatibility issues, Oracle CASB Cloud Service was natively built on an API architecture so there is no requirement for hardware, software, or agents. It delivers a multimode CASB through integrations with leading in-line solutions including secure web gateways (SWG), next-generation firewalls (NGF), identity as a service (IDaaS), data loss prevention (DLP), and security information and event management (SIEM).







**Oracle Corporation, World Headquarters**

500 Oracle Parkway  
Redwood Shores, CA 94065, USA

**Worldwide Inquiries**

Phone: +1.650.506.7000  
Fax: +1.650.506.7200

CONNECT WITH US

-  [blogs.oracle.com/oracle](https://blogs.oracle.com/oracle)
-  [facebook.com/oracle](https://facebook.com/oracle)
-  [twitter.com/oracle](https://twitter.com/oracle)
-  [oracle.com](https://oracle.com)

**Integrated Cloud Applications & Platform Services**

Copyright © 2016, 2017 Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0117

Working the Numbers: How to Quantify the Value of a Cloud Access Security Broker  
January 2017