REPORT

McAfee
Together is power.

Cloud Adoption and Risk Report

Business Growth Edition

Cloud Adoption and Risk Report

Business Growth Edition

Executive Summary

From the introduction of Salesforce.com and countless cloud services since, we've been seeking ways to leverage the cloud to grow our businesses. It's absolutely working. In this edition of the Cloud Adoption and Risk Report, we'll look at how companies like yours are using the cloud to deliver key measures of business growth, the hurdles they've had to overcome to get there, and what leaders of cloud adoption are doing to accelerate growth ahead of the rest. For our research we surveyed 1,000 enterprise organizations around the world and combined that data with insight from billions of anonymized cloud events aggregated across thousands of customers in our live environment to capture both the perception and reality of these challenges and opportunities. Four key trends jumped out at us:

- The vast majority of companies using the cloud experience business acceleration.
- Security is stronger in the cloud.
- Most cloud customers aren't fulfilling their shared responsibility for security.
- There is a dramatic leap in business acceleration for companies getting ahead of risk and protecting their data in the cloud.

The security budgets at Microsoft, Amazon Web Services (AWS), Box and most other enterprise cloud service providers can be orders of magnitude higher than the customers they serve, and that's paying off. In our survey, 52% of companies stated they experience better security in the cloud. That's great news for the IT industry as a whole. Not only is security better, but 87% said they experience benefits from the cloud that drive business acceleration. Forty-one percent attribute business growth to use of the cloud, and around 30% are able to launch new products, speed up time to market, and expand to new markets. So not only do enterprises say the cloud is more secure, they also state it is actually improving business commercially. So why isn't everyone experiencing this?

The gap between secure enablement and experimental adoption is drawn by the approach to protecting data, which nearly all cloud providers state is the customer's responsibility. Only 36% told us they can currently enforce data loss prevention (DLP) in the cloud. Only 33% said they could control how users collaborate and share data in the cloud. In the case of IaaS, only 26% said they could audit configuration settings, like open access to storage buckets, again widening the gap.

The silver lining here is that companies fulfilling their shared responsibility by protecting their data in the cloud are opening up substantially more benefits than those who aren't taking data protection into their own hands. Companies are 32% more likely to experience business growth from the cloud when using a Cloud Access Security Broker (CASB) to protect their data, compared those who don't. The likelihood of companies being able to launch new products, speed time to market, and expand to new markets with the cloud is all over 35% higher when a CASB is part of their cloud security strategy. Yet only one in three companies we surveyed are currently using one.

Key Findings

- Eighty-seven percent of companies experience business acceleration from their use of cloud services.
- The majority (52%) of companies experience better security in the cloud.
- Only 26% of companies say they can audit IaaS configurations.
- Only 33% of companies say they can control application collaboration settings.
- Only 36% of companies say they can enforce data loss prevention in the cloud.
- Companies are over 35% more likely to be able to launch new products, speed time to market, expand to new markets, and improve employee satisfaction with the cloud when using a Cloud Access Security Broker (CASB).
- Only one in three companies currently use a CASB.

Cloud as a Business Accelerant

There hasn't been a more disruptive technology to enter enterprise IT since the internet itself. Most companies are structuring themselves around the rapid transformation, growth, and agility the cloud delivers. Cloud is making IT more strategic than ever. Instead of building from the ground up we're leveraging the development teams at AWS, Box, Microsoft and countless others to give us the tools we need to run our businesses, from anywhere. Cloud infrastructure is leagues ahead of our on-premises performance. Workers are able to collaborate faster. Software developers are building and deploying applications rapidly in cloud infrastructure. The cloud is moving our businesses forward faster, and for this study we want to show specifically how, so you as a reader can get a sense of what companies leading the charge are experiencing.

In the chart below we asked our 1,000-respondent pool of enterprise IT decision makers how they were benefitting from their use of cloud. First, let's look at one aggregate finding from that question:

87% of enterprises experience business acceleration from their use of cloud services.

What do we mean by business acceleration? We defined it by those who experienced at least one of the following measures:

1. More efficient collaboration
2. Improved employee productivity
3. Business growth
4. Faster time to market
5. Higher employee satisfaction
6. Ability to launch new products
7. Expansion to new markets

Business growth is a leading indicator here. 41% of companies were able to directly attribute business growth to their use of cloud services. Think about that for a moment. Did the last implementation of your on-premises file repository feel like it grew the business commercially? Probably not. But enabling thousands of workers to share files, access from anywhere, and collaborate with external parties using Box just might. Enabling your software development team to build, iterate, and continuously deploy new customer-facing applications in AWS is even more likely to lead to growth.

How Companies Benefit from the Cloud

Figure 1. What benefits does your organization experience from its overall use of cloud services?

In addition to this question, we asked our respondents to tell us what type of cloud services they use, whether software-as-a-service (SaaS), platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS), private cloud, or any combination. Those using IaaS clearly had an edge on business acceleration. Forty-three percent of companies using IaaS experienced faster time to market. Thirty-seven percent were able to launch new products. Thirty-six percent were able to expand to new markets.

Each of these measures of acceleration—time to market, launching new products, and expanding to new markets were around 20-25% above average for companies using IaaS. While we know the collaborative nature of SaaS is a boost to our businesses, the use of IaaS as a new IT environment for customer-facing and internal applications is driving companies forward faster than the rest, and likely adding a competitive edge to those at the forefront of adoption.

How Companies Benefit from the Cloud
with Infrastructure-as-a-Service (IaaS)

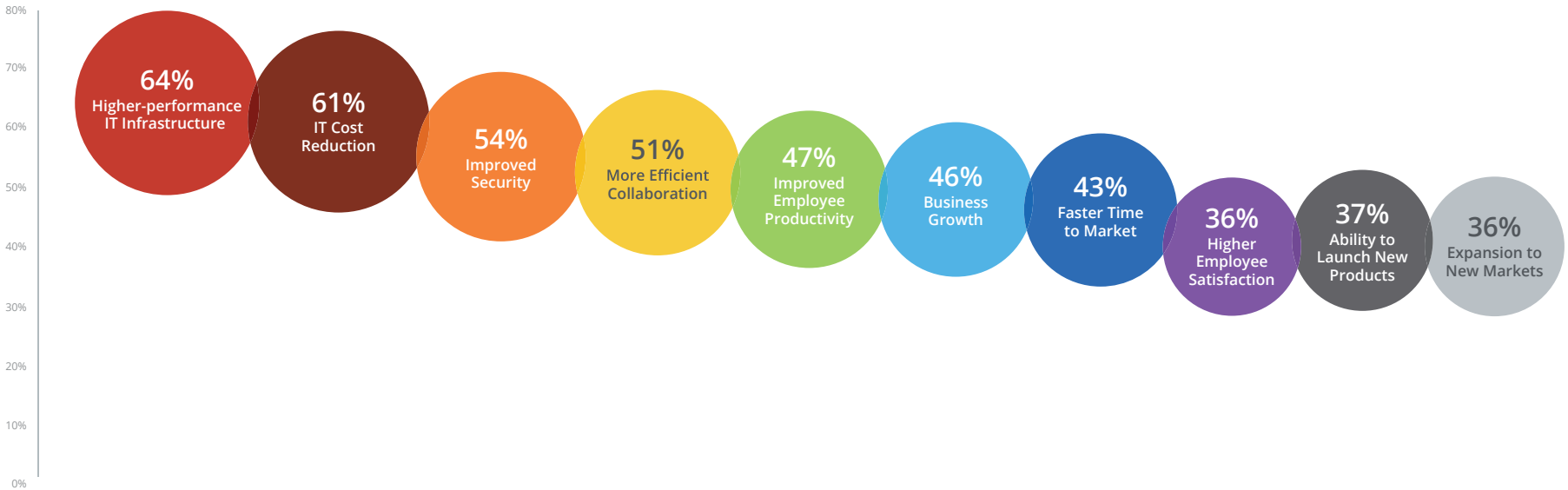

Figure 2. What benefits does your organization experience from its overall use of cloud services? Companies who use Infrastructure-as-a-Service (IaaS)

The State of Security in the Cloud

You may have noticed one compelling finding from the charts above that we left out of the prior discussion:

52% of companies experience better security in the cloud.

It's a stark contrast from the first wave of fear, uncertainty, and doubt we had for the cloud at the early stages of adoption. Fundamentally we all wondered, how can I trust my organization's data to a third-party provider, in an environment where I don't have visibility and control? The concerns were real. Breaches happened. Some companies are still facing the darker side of that reality. Others have come out of the tunnel to see that their trusted cloud providers now dedicate a tremendous amount of resources to security, all to protect their customers and the sustainability of their business model.

So what's left? The one element of security cloud providers can't cover for their customers is how their services are actually used, specifically the data that is stored in them, shared externally, and accessed from a myriad of devices and locations. There are almost infinite variations on what we each consider "sensitive" data, or are required to protect in regulated industries. The requirements for large retail providers to keep their data PCI compliant don't necessarily apply to a government research agency that needs to secure intellectual property.

The responsibility comes back to customers. As cloud users, we need to know what data needs to be protected, where it goes, and who is allowed to access it based on our internal policies and compliance requirements. To give everyone a shortcut, we assessed billions of aggregated, anonymized cloud events we see in the McAfee universe of enterprises to show where sensitive data resides in the cloud, on average:

Where Enterprise Sensitive Data Lives in the Cloud

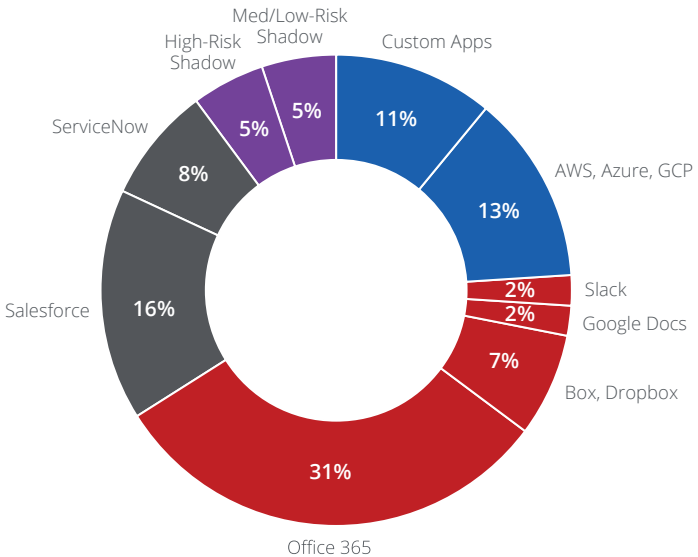

Figure 3. Distribution of sensitive data across cloud service types

Further aggregating this chart into categories, you can see that 65% of sensitive data lives in collaboration and business apps like Office 365, Box, and Salesforce. 25% lives in IaaS like AWS, Microsoft Azure, and Google

Cloud Platform (GCP). And finally, 10% lives in Shadow IT. The shift from early stages of cloud adoption here is dramatic. Before IT teams officially sanctioned applications like Office 365, Box, and others, most enterprise cloud data lived in Shadow IT, because employees simply signed up for apps they wanted to use, ignoring IT. Now that has completely flipped. IT teams are rolling these apps out themselves, effectively fulfilling most needs that were previously unmet. The risk of sensitive data exposure through Shadow IT has been significantly diminished.

We now have a targeted method to begin protecting sensitive data in the cloud. Start with the applications that hold the majority of your sensitive data, and work your way down. Whether your company already uses these apps or is planning to roll them out, you can use this approach to guide your resource planning and maximize risk mitigation.

Bridging the Gap in Cloud Security Shared Responsibility

The challenge for us all now becomes how to effectively implement security for our data in the cloud, spanning across hundreds of services and involving multiple internal and external stakeholders with their own requirements and input. We want to streamline, and we can. First let's look at timing of security implementation, which has unique implications for companies with a DevOps approach using IaaS and PaaS.

Timing of Security Implementation in the Cloud

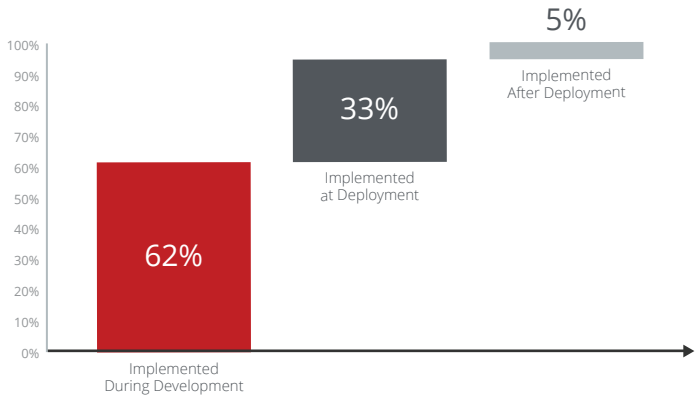

Figure 4. When is security implemented in your organization's cloud applications? Companies with a DevOps approach.

In the chart above, you can see that 62% of companies using a DevOps approach implement security during development of their cloud applications, 33% at the time their cloud applications are deployed, and 5% after their cloud applications have been deployed. Clearly there is a movement to shift security "left" in the software development lifecycle to get ahead of problems before they go live in production cloud environments. We love this finding, because it supports what we believe to be a best practice for security in the cloud. In IaaS and PaaS, run code and configuration checks during development so you can fix issues rapidly and cause minimal disruption to the continuous delivery of new software. We hope more companies pick up on this trend.

Next, let's look at what our enterprise survey respondents said about their security practice in the cloud today:

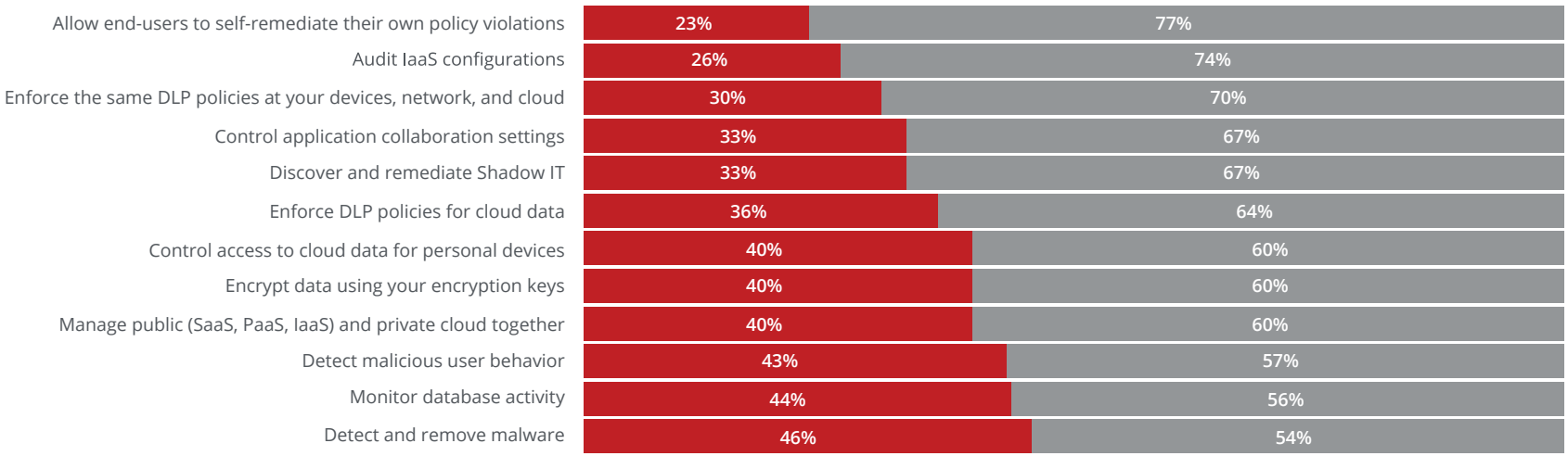

Figure 5. Can your organization's current cloud security solution(s) conductany of the following in the cloud?

Here we have some significant gaps directly related to the shared responsibility we're all supposed to uphold as cloud customers. Fulfilling the responsibility of protecting your own data in the cloud can come in many forms, but it is clear many companies are behind. Only 33% said they could control collaboration settings, like when someone creates a file sharing link with open access to anyone in the world. Only 36% said they could enforce data loss prevention in the cloud. For the survey we only recruited respondents from companies 500 employees and above, most of which are likely to have a DLP practice for devices and other on-premises locations. The majority are far behind in the cloud. Lastly, 40% of companies said they could control access to cloud data from personal devices. The remaining 60% are letting a black hole form that is invisibly siphoning their data, with no way to get it back. Sensitive data that goes to an unmanaged, personal device is gone forever, and that can be devastating.

How Leaders in Cloud Adoption are Growing Business Faster

The gaps in security practice we just highlighted were alluding to a specific category of technology that we'll discuss here, that being the role of Cloud Access Security Brokers (CASB) in cloud adoption in business growth. In short, companies that use the cloud with a CASB to protect their data are accelerating faster than everyone else, and it's having a material impact on their business. Let's start with a few fundamental findings.

First, companies use 49% more cloud services with a CASB. The idea here is that by having a solution for protecting cloud data, IT teams are able to roll out more services, faster, because their security requirements are met from the start. Keep in mind that the chart below reflects "self-reported" cloud services, most of which are sanctioned and excludes hundreds of increasingly-erroneous Shadow IT applications.

Estimated Number of Cloud Services in Use

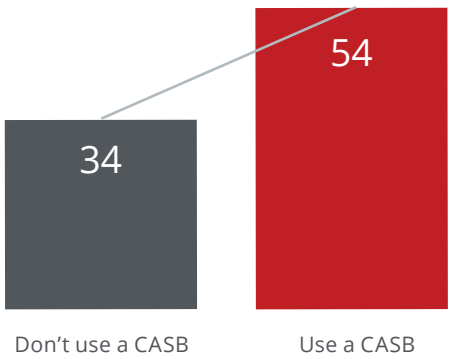

Figure 6. Please estimate how many public cloud services (SaaS, PaaS, or IaaS) are currently in use by your organization (averages shown).

Next, companies with a CASB run 56% more custom apps in IaaS. With the ability to audit IaaS environments for misconfiguration, the risk of data exposure is minimized, and developers are empowered to do more in environments like AWS. Data stored in S3 buckets can become part of a DLP practice, giving further confidence to push forward with innovative development in the cloud that won't put the company at risk.

Estimated Number of Custom Apps in IaaS

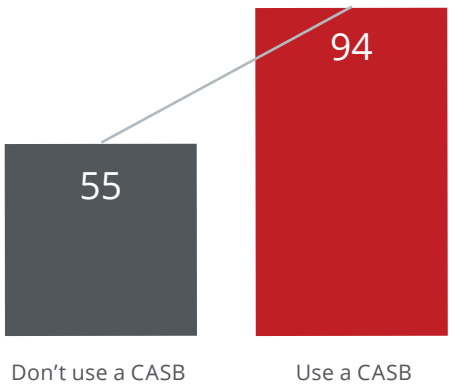

Figure 7.Please estimate how many applications your organization runs in IaaS (averages shown).

Let's now return to the start of our discussion on business acceleration. The vast majority of companies using the cloud stated they experienced forces of acceleration from their use of the cloud. We were surprised however, by how much faster companies were moving when they used a CASB:

How Companies Benefit from the Cloud
with Cloud Access Security Broker (CASB)

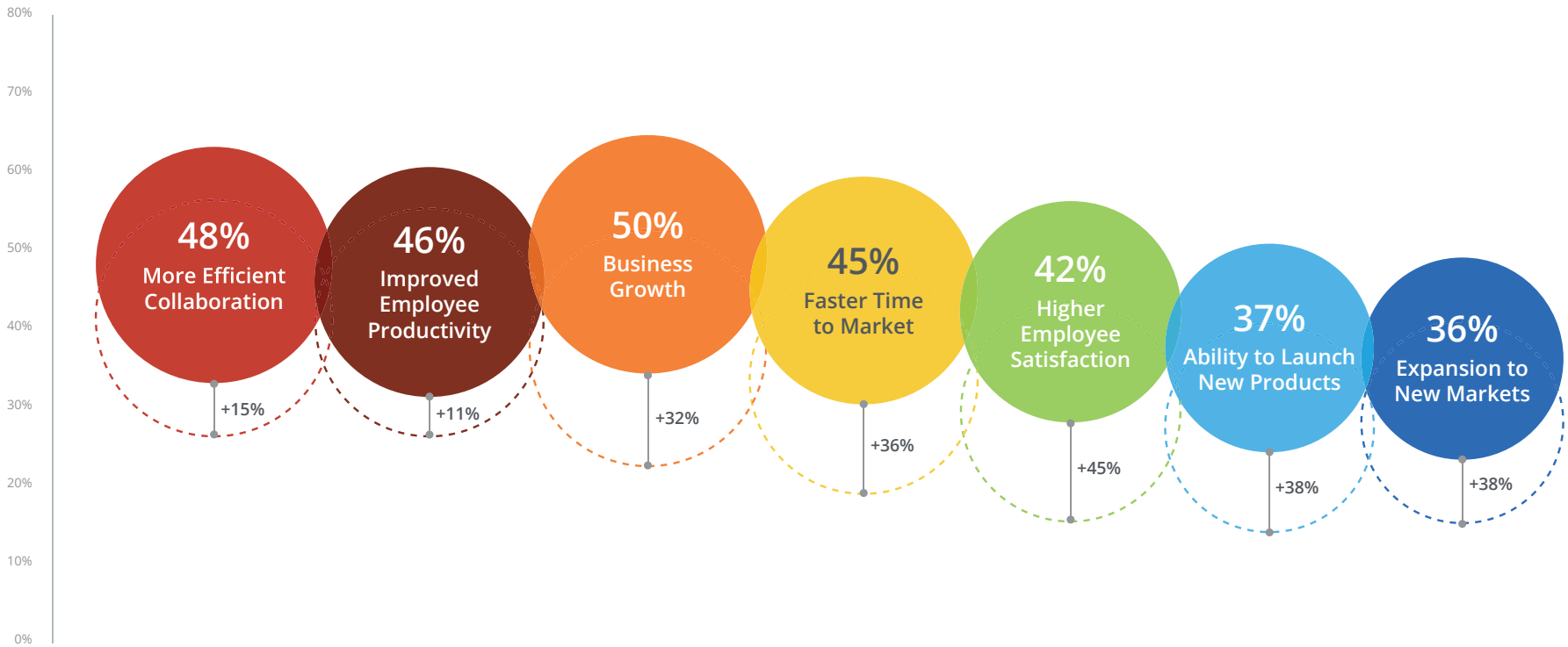

Figure 8. What benefits does your organization experience from its overall use of cloud services? With Cloud Access Security Broker (CASB) vs without.

There is a significant jump in each force of business acceleration for companies who use a CASB. Companies were 45% more likely to increase employee satisfaction with the cloud when using a CASB. As we just showed, companies using a CASB also used more applications, fulfilling more employee needs. They were 40% more likely to be able to launch new products, 38% more likely to expand to new markets, 36% more likely to have a faster time to market, and 32% more likely to experience business growth, all contributors to commercial success. Whether it is the increase in IaaS applications, improved collaboration, or simply a culture of speed and innovation, companies are accelerating faster using the cloud with a CASB. Yet only one in three companies we surveyed use one.

Recommendations

It should be clear from our data at this point that cloud services are contributing in material ways to the success of most companies. The goal here is to guide towards more successful cloud adoption by demonstrating that mitigating risk can increase the potential for business acceleration.

1. **Find out where your sensitive data lives in the cloud.**
   We gave you a head start above; however it is still worth assessing your own unique environment so you can be precise in your security practice.
2. **Audit your IaaS deployments early.**
   Get ahead of misconfiguration by auditing IaaS rollouts early, at the development phase. That will save your developer and operations teams time by preventing retroactive change requests from the security team after their apps are already live. That extra time can allow for more innovative development at your company.
3. **Roll out cloud apps with a CASB.**
   Get in the habit of deploying your cloud apps with collaboration, access, and data controls in place from the start. That will increase your velocity of cloud adoption and as we saw, raise the likelihood of business acceleration.

Business acceleration with the cloud is a dominant force, and companies protecting their data with a CASB are moving faster than the rest. IT is more strategic than ever as a business enabler. Use the data and recommendations in this report to help move your business faster with the cloud.

Methodology

To bring you these findings, we surveyed 1,000 IT professionals in 11 countries selected to represent a diverse set of industries and organization sizes. Fieldwork was conducted from March to May 2019 by Vanson Bourne. These results were used in comparison to aggregated, anonymized cloud usage data for over 30 million McAfee MVISION Cloud users worldwide, who collectively generate billions of unique transactions and policy events in the cloud each day. Both of the datasets represent companies across all major industries including financial services, healthcare, public sector, education, retail, high tech, manufacturing, energy, utilities, legal, real estate, transportation, and business services.

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com