



Research Report Conducted By

VansonBourne



2018 Enterprise Cloud Trends



Five Trends Influencing
Enterprise Cloud Adoption

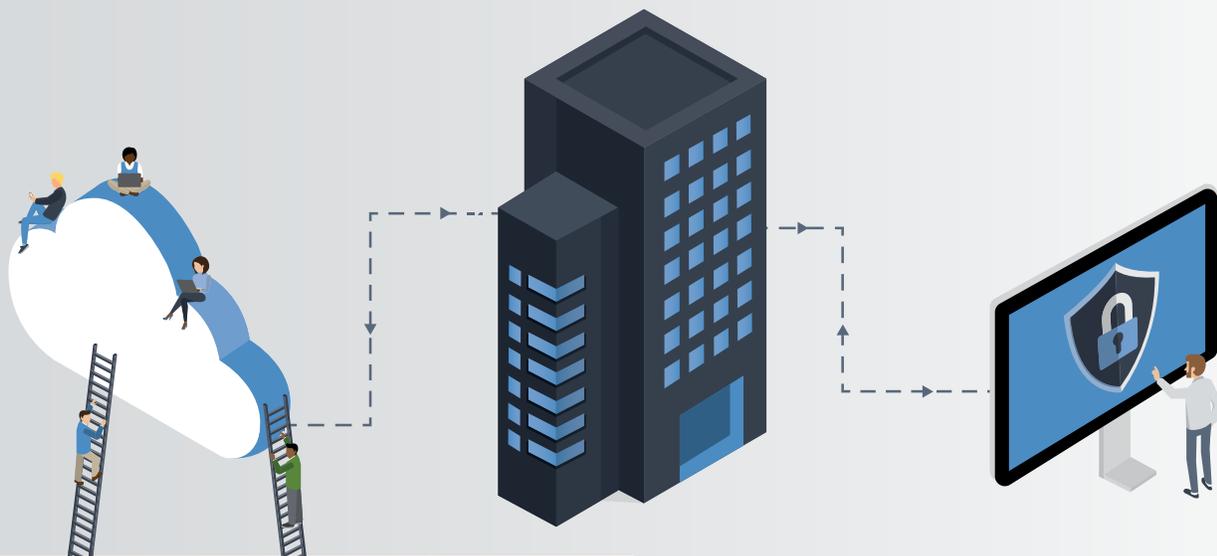
EXECUTIVE SUMMARY

Companies across industries and verticals are investing more in cloud, with nearly every organization polled in our latest survey planning to increase enterprise spend in the areas of cloud and SaaS over the short and long term. Despite increased adoption, companies are still fundamentally misunderstanding many of the nuances of the cloud and how these services are delivered. Specifically, data privacy and asset security are the top concerns for ITDMs, which is reflected in their misunderstanding of how cloud products use and secure their sensitive corporate data.

KEY FINDINGS

- 1 SaaS use is growing at a faster pace than most enterprise IT teams can securely support it**, despite most respondents anticipating exponential investment into SaaS to continue for the foreseeable future.
- 2 Companies are embracing remote work, leveraging cloud applications, and implementing SaaS tools en masse** to connect employees and branch offices wherever they may be, further distributing enterprise network architectures.
- 3 Despite remote work policies and security protocols, “Shadow IT” is rampant across enterprise networks**, as office workers are prone to bypassing network security and IT to access a new tool or application.
- 4 As the rate of cloud and SaaS adoption increases, IT teams are primarily concerned with data privacy**, driven by fears of sensitive corporate data being compromised in non-secure cloud environments.
- 5 All office workers polled view SaaS favorably**, with many happy to access the applications they need to do their job rather than work with IT to assure safe implementation and protection of corporate assets.

Five Trends Influencing Enterprise Cloud Adoption



Cloud Use in Organizations

On average, surveyed IT decision makers (ITDMs) cite that their organization is currently spending 26% of their IT budget on cloud. In addition, ITDMs indicate that their organization's spend will grow to an average of 31% in the next 12 months, with an expected average of 39% in the next 24-36 months.

The clear majority (94%) of ITDMs interviewed have/had at least one concern about their organization moving to the cloud. The most common concerns are/were data privacy (61%), cost of maintenance (41%) and/or cost of migration (35%). Other concerns include compliance with data protection regulations (31%) and/or complicated infrastructure (25%).

Almost all (99%) surveyed ITDMs say that there is or was at least one driver for their organization moving to the cloud. More than eight in ten (83%) ITDMs believe that their organization's IT department is fully comfortable supporting the changes required to adapt security policies to a cloud-based environment. However, most (91%) of surveyed ITDMs still acknowledge that their organization's security policies need to improve to operate fully in a cloud environment – even if they are confident in their team's ability to adapt.

Use of SaaS

ITDM respondents are most likely to say that their organization is currently or planning to keep accounting (29%), firewall (28%) and/or antivirus (26%) applications on-premises.

On average, 21% of ITDM respondents' organizations' applications are currently SaaS. In addition, respondents believe that the percentage will grow to an average of 28% in the next 12 months, with an expected average of 36% in 24-36 months.



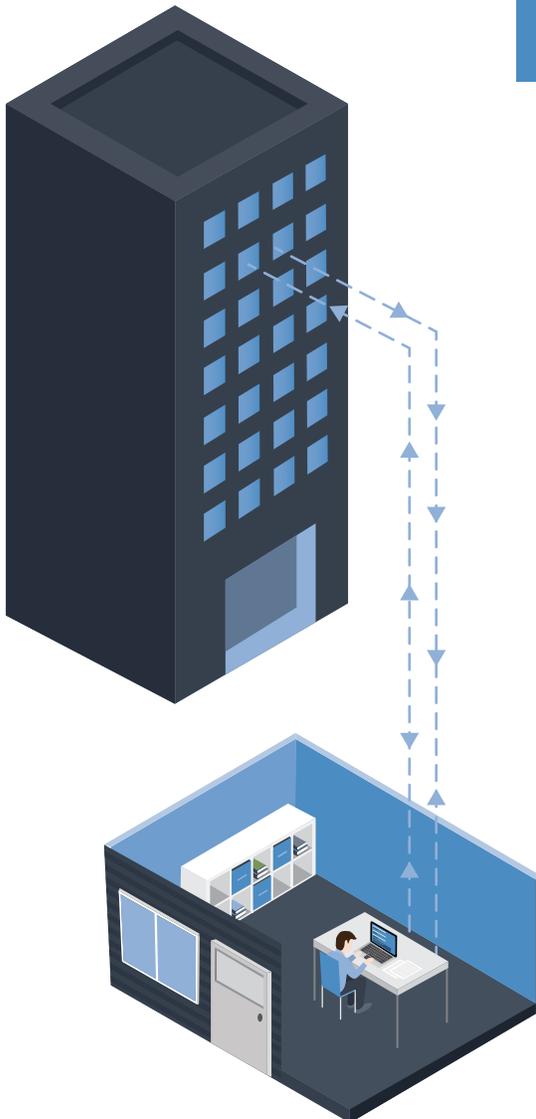
Remote Workers and SaaS Vulnerabilities

One of the hallmarks of SaaS adoption is that it's made it easier for enterprises to embrace remote working initiatives, contributing to the distributed nature of contemporary networks.

Almost all (99%) ITDM respondents report that at least some of their organization's employees can be remote/mobile workers, with 28% of employees having the ability to do this, on average. In comparison, the vast majority (96%) of office worker respondents work remotely away from the office, with 57% who do this three days a week or more.

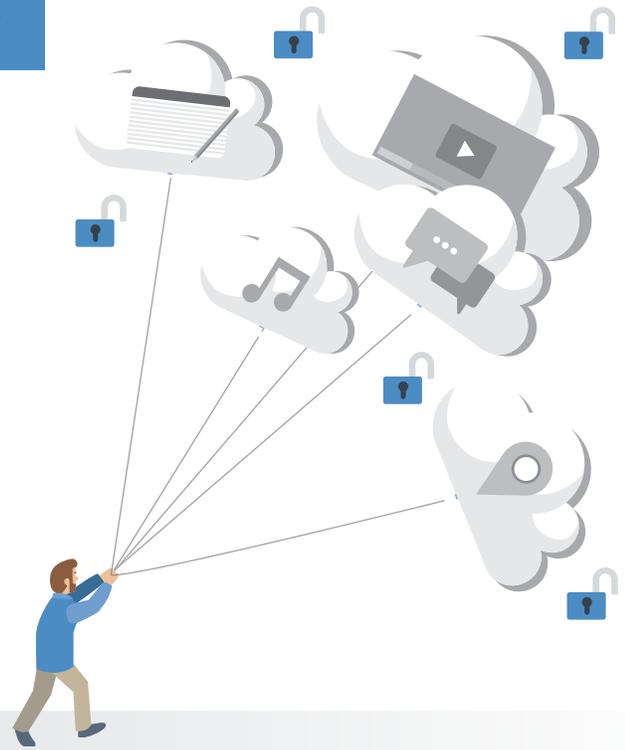
A large proportion (92%) of surveyed office workers confirm that their organization has a 'remote working' policy in place. Of office worker respondents who work remotely, more than six in ten (62%) say that their organization requires them to use a VPN every time they work remotely.

However, the vast majority (82%) of the same respondent group reveal that they have accessed a SaaS application when working remotely without using their company's VPN at least once, with approaching half (46%) admitting that they do this regularly. Office worker respondents who have accessed a SaaS application outside of their company's VPN say that they have done so because their VPN has restrictions on certain sites they need access to (47%) and/or their VPN connection often disconnects (40%).



SaaS Security Challenges

More than seven in ten (73%) ITDMs interviewed agree that their organization's data is more secure using on-premises, purpose-built appliances compared to a SaaS solution. For those who feel that their organization's data is more secure using on-premises, purpose-built appliances compared to a SaaS solution, the most likely reasons for this feeling are that their data is less secure when using a SaaS solution because SaaS solutions store their data on shared servers (66%), SaaS does not always fully integrate with their existing infrastructure (42%) and/or security isn't a priority for SaaS solutions (27%). More than six in ten (64%) ITDMs agree that their organization's SaaS adoption is outpacing their ability to secure it, yet nearly half (49%) agree that their organization is hesitant to adopt SaaS-based security solutions.



Shadow IT

Most (87%) of ITDM respondents believe that at least some of their organization's employees access and use applications that are outside of the IT department's knowledge.

Additionally, more than three fifths (62%) of office worker respondents concede that they have bypassed the IT department to get access to a new tool or application without their knowledge or consent. Around half (49%) of office workers who have bypassed IT to get access to a new tool or application without IT's knowledge or consent say that it is because the IT department takes too long to do anything.

Approaching three in four (72%) surveyed office workers agree that it is more important for them to get access to applications they need to do their job effectively than to tell the IT department what applications they are using. More than half (53%) agree that the IT department is more interested in putting up barriers to the use of new applications than helping set them up properly and securely.



IN SUMMARY

ITDMs report that their organization plans to increase their current SaaS usage over the next 12 months (from 22% to 28% of apps, on average)

This is despite 73% of ITDMs stating that they feel their organization's data is more secure using on-premises, purpose-built appliances compared to a SaaS solution

Around nine in ten (91%) surveyed ITDMs say that their organization's security policies need to improve to operate fully in a cloud environment

Which could be why a similar proportion (89%) plan to keep at least some applications on-premises

Nearly all (99%) ITDMs report that their organization enables remote working, while 96% of office workers actually take advantage

However, of those office workers who are required to use a VPN while remote, 82% have bypassed it

Additionally, 48% of office workers have broken their remote working cybersecurity policy; ITDMs only believe that 36% of remote workers have bypassed security policies, on average

Approaching nine in ten (87%) ITDMs say that their organization's employees access and use applications that are outside of the IT department's knowledge

This may be happening because the majority (53%) of office workers believe IT is more interested in putting up barriers to the use of new applications than helping set them up properly and securely

Ultimately, it's over three quarters (77%) of ITDMs who report that shadow IT is a major security concern for their organization's IT department

ITDM respondents expect that organizations can expect to see cost savings (55%) and better security (47%) through the use of SaaS applications

Furthermore, ALL (100%) of office worker respondents state that there is a minimum of one benefit to be seen through using SaaS

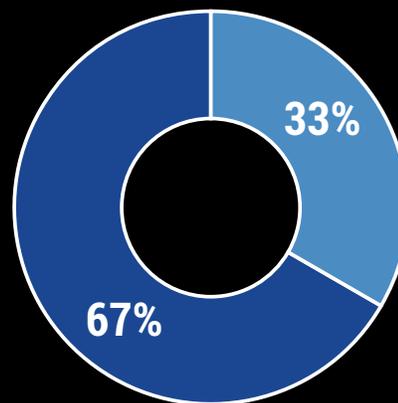
CONCLUSION

The benefits of cloud and SaaS tools are clear to most enterprises. However, there remains a fundamental misunderstanding about how the cloud works and where the burden of data security falls – the cloud or SaaS provider, or office workers and ITDMs directly. Still, as the adoption of cloud continues to ramp up, the variety of cloud types and delivery methods for SaaS services will become more familiar to businesses across industries. This will include a greater understanding of how to securely leverage these products from stakeholders and users across organizations, which will inevitably bridge the gap between office workers and IT in understanding and adhering to best practices.

Cloud is here to stay. Learn how to secure it.

Survey Methodology

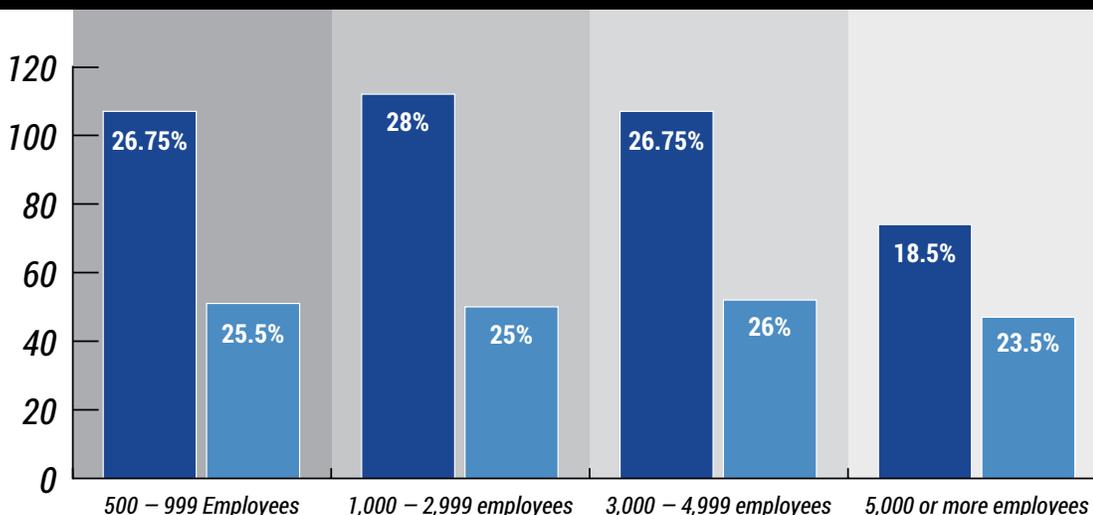
200 IT decisions makers (ITDMs) and 400 office workers in the US were interviewed in February and March 2018, employing approximately-even sample groups across industries/sectors while targeting large enterprises in four size categories: 500-999 employees, 1,000-2,999 employees, 3,000-4,999 employees, and 5,000 or more employees.



Survey Split

(ITDMs vs. Office workers)

- Office Workers
- IT Decision Makers



Headcount Comparison

(ITDMs vs. Office workers)

- Office Workers
- IT Decision Makers



About iboss

The iboss Distributed Gateway Platform is a web gateway as a service that is specifically designed to solve the challenges of securing distributed organizations. Built for the cloud, iboss leverages a revolutionary, node-based architecture that easily scales to meet ever-increasing bandwidth needs and is managed through a single interface. The iboss Distributed Gateway Platform is backed by more than 110 patents and protects over 4,000 organizations worldwide, making iboss one of the fastest growing cybersecurity companies in the world.

To learn more, visit www.iboss.com or contact iboss at sales@iboss.com