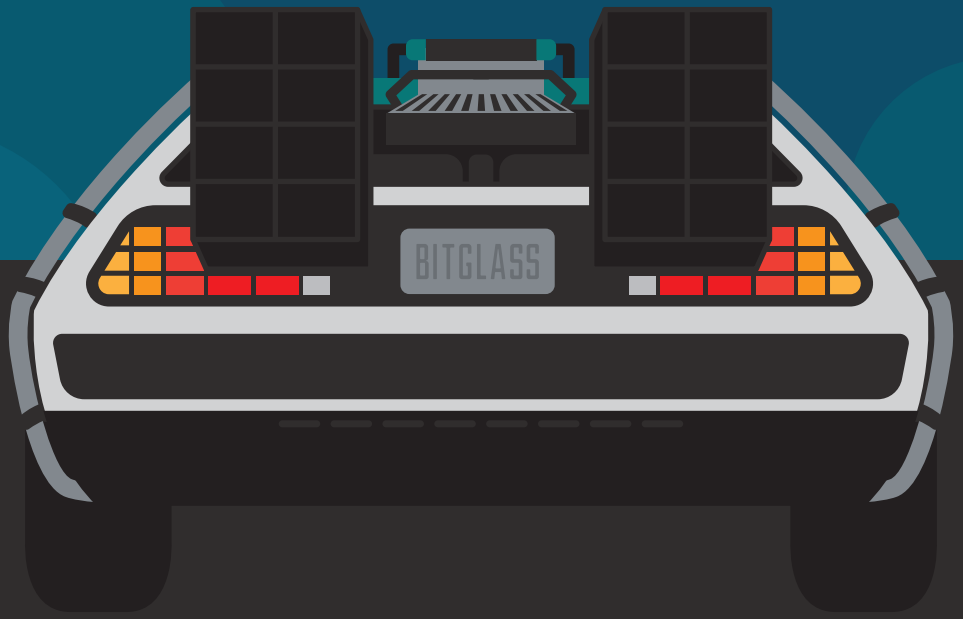
CLOUD IS THE FUTURE

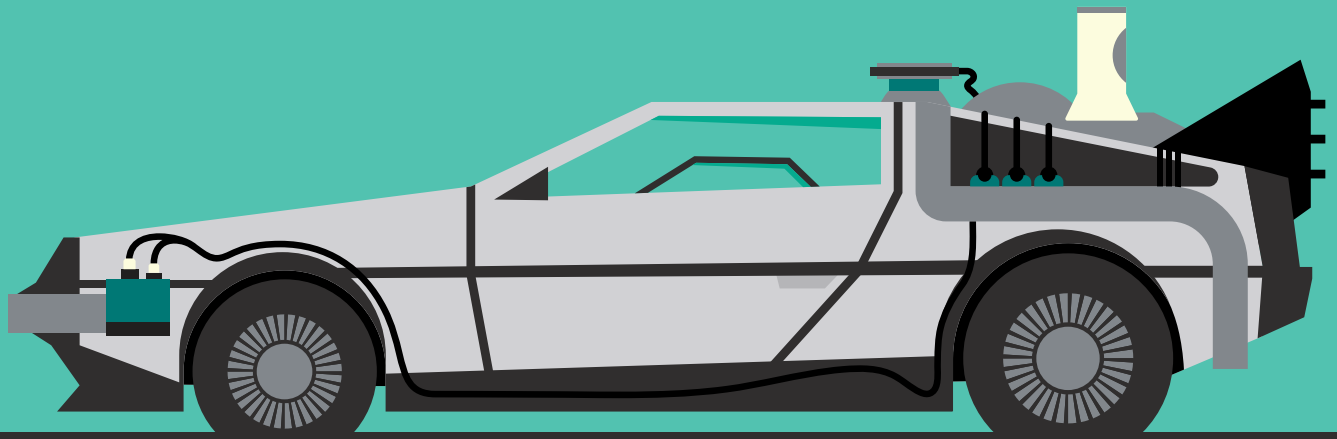


IT PRIORITIES ARE CHANGING FAST

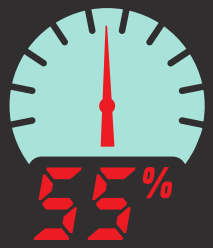
bitglass

In the wake of major breaches in the last several years, organizations have become keenly aware of the need to secure corporate data in the cloud. Given the rise of BYOD and poor MDM adoption, IT departments are turning to new data-centric solutions to secure corporate data in 2016 and beyond.

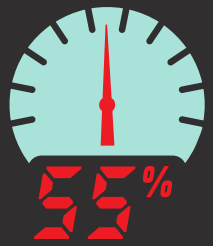
Bitglass surveyed nearly 100 CIOs and IT leaders for this report to get a sense of their future plans for cloud and mobile security and to understand the challenges they foresee heading into 2016.



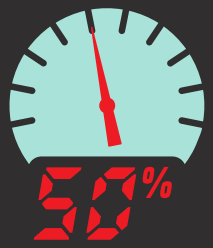
TOP FINDINGS



55% of respondents characterized their organization's 2016 public cloud strategy as Cloud First. Just a few years ago, on-premise solutions were the industry standard, but cloud apps have matured to meet the demand for a secure, easy-to- deploy cloud solution and are now an increasingly important piece of IT organizations' infrastructure. Looking ahead to 2016 and beyond, expect more organizations to take a Cloud First approach to managing their corporate data.



Cloud Access Security Broker (CASB) adoption is rising fast, with 55% planning to deploy a CASB in the future. CASBs like Bitglass offer a comprehensive security solution and visibility over corporate data in public cloud applications like Office 365 and Google Apps. Given the growing demand for BYOD, many IT leaders are looking to CASBs to augment the capabilities of public cloud apps and secure data on mobile devices.



SaaS applications are delivering on much-hyped promises of cost savings. **50% of survey respondents reported some cost savings in 2015.** Heading into 2016, both public cloud applications and CASB solutions are more affordable than ever.

SECURITY SPEND EXPECTED TO RISE

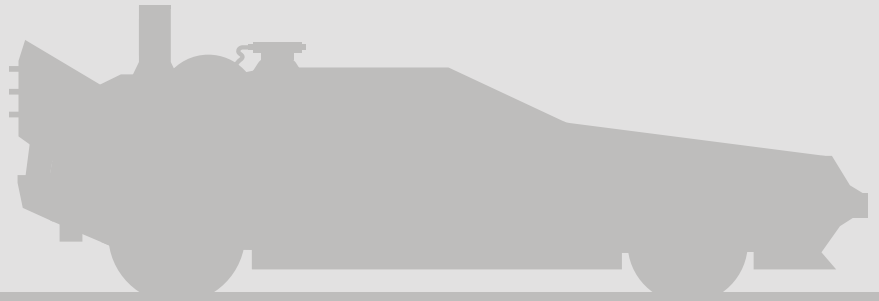
Cost of SaaS applications are lower than on-premise solutions, but the need to secure data is greater than ever.

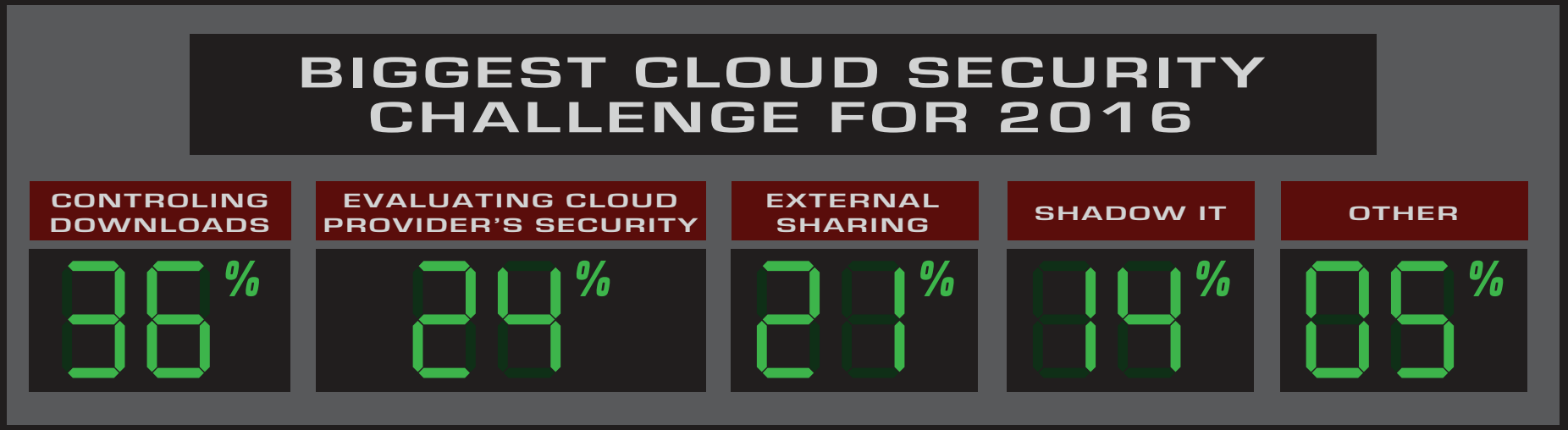
87% of IT leaders expect their overall security spend to rise in the year ahead.

77% planning to increase both mobile and cloud security expenditures.

34% expect to increase spending on cloud security by more than 20% in 2016.

With growing adoption of public SaaS applications, it's no surprise that IT departments need next-gen solutions to achieve compliance.





Looking to 2016, controlling downloads to unmanaged devices is the top concern for **36%** of IT leaders, followed by evaluating security of public cloud providers and controlling external sharing.

Shadow IT, which rose to prominence as the most talked about cloud security concern in 2013 and 2014, has dropped to become a rounding error in the minds of CIOs.

THE FUTURE IS CLOUD.

More organizations are taking a Cloud First approach to their public cloud deployments but are increasingly concerned about downloads to devices, security of public cloud apps, and external sharing.

Cloud Access Security Brokers (CASBs) are meeting a critical need for control and visibility of corporate data in public cloud applications like Google Apps, Office 365, and Box. CIOs are looking to adopt next-gen CASBs like Bitglass that offer total data protection beyond the firewall, with features like integrated DLP and granular control over data on both managed and unmanaged devices.

LEARN MORE ABOUT BITGLASS

ABOUT BITGLASS

In a world of applications and mobile devices, IT must secure data that resides on third-party servers and travels over third-party networks to employee-owned mobile devices. Existing security technologies are simply not suited to solving this task, since they are developed to secure the corporate network perimeter. Bitglass is a Cloud Access Security Broker that delivers innovative technologies that transcend the network perimeter to deliver total data protection for the enterprise—in the cloud, on mobile devices and anywhere on the internet.

bitglass

Phone: (408) 337-0190
Email: info@bitglass.com

www.bitglass.com