

The State of SMB Cloud Security in 2016

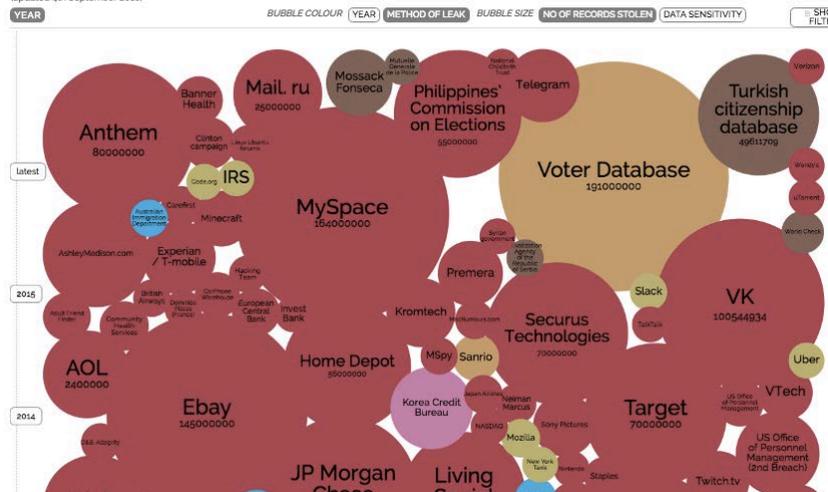
SMBs are lagging in adoption of cloud application security

Google Apps and Office 365 most widely used apps

2016 has been a challenging year for IT professionals. Even though business technology needs have skyrocketed, budgets aren't increasing to meet new security demands. Risks are accumulating and breaches are spilling over into the media. While the largest breaches and hacks make news, Small and Mid-size businesses (SMB) are definitely not immune. SMBs don't need to be singled out in order to be a target. A rogue employee or a bot crawling the web for known vulnerabilities will exploit businesses of any size. Breaches, leaks and attacks have always been a concern for large enterprises, but for SMBs these security concerns are just now becoming the new normal.

World's Biggest Data Breaches

Selected losses greater than 30,000 records
(updated 4th September 2016)



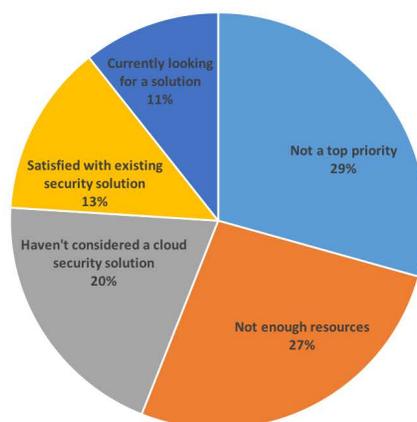
While cloud app providers normally take reasonable security precautions with user data, cloud security issues relating to the way users utilize cloud apps aren't their responsibility. These providers have a shared responsibility model that eschews responsibilities for data in transport and at rest in the cloud. The responsibility of what data is uploaded, how the data is stored and the user access control rests squarely with users.

Regulations like HIPAA, FERPA and PCI have strict rules on how businesses use cloud apps. And, most SMBs aren't aware that a cloud apps' regulatory compliance isn't the same as their own compliance with cloud app use (92%). The question remains as to when SMBs will decide to do something about it.

A big problem not just for big businesses

This year, enterprises appear to be closing the gaps between new technologies and the security problems that they create. Gartner forecasts that the vast majority of enterprises will deploy cloud security solutions to address their cloud risks by 2020. Despite the concerns of the SMBs surveyed, almost none of them had a cloud-specific security solution in place to address their cloud security risks (<2%). They cited several reasons for lacking a cloud specific security solution:

Reasons for Not Having a Cloud-Specific Security Solution

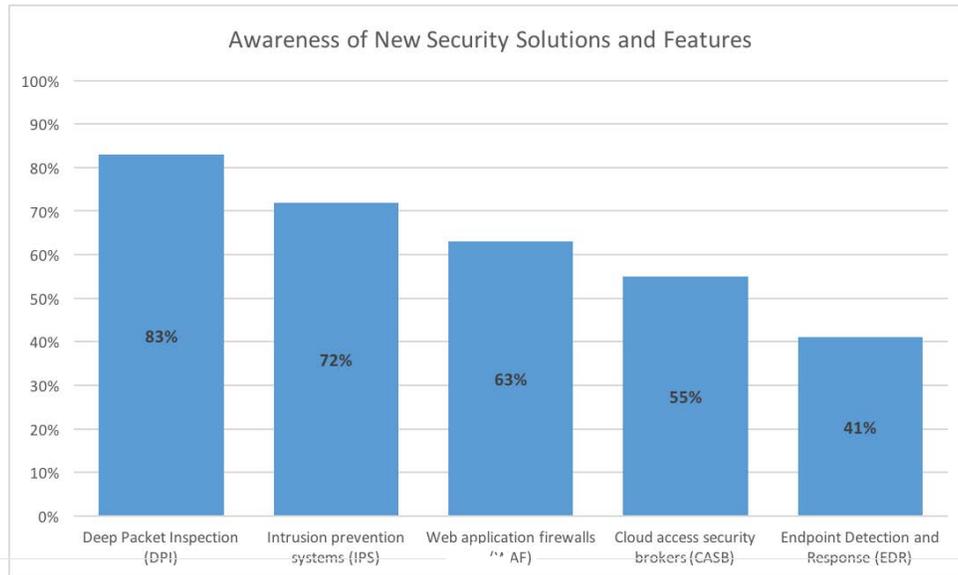


Most security providers assume SMBs are comfortable with a higher level of IT security risk. The results of why SMBs don't have a cloud specific security solution seems to back up that assumption. But, we were surprised to learn that SMBs' slow pace of cloud security adoption isn't due to a lack of demand. Among the respondents who had reported looking for a cloud security solution in the past, 74% said that they weren't satisfied with their choices.

SMBs want enterprise class security, but ...

Most cloud security solutions were developed with large enterprises in mind. The economics of cloud security solution development favored enterprises because the cloud created more pressing compliance problems for publicly traded companies. Enterprises also had the resources available to allocate towards solutions. Cloud security solutions designed for SMBs that are easy to deploy and affordable to maintain are beginning to emerge, but the market is still catching up to demand. Even though SMBs are less risk averse than their enterprise counterparts, that doesn't mean they aren't willing to adopt better security measures when they are available.

Most SMBs we surveyed had malware protection and a firewall in place (89%). But, those who didn't have a cloud security solution were either not happy with their current security stack (61%) or were actively looking to replace them with a next generation firewall (NGFW) / unified threat management (UTM) system (28%). The SMBs were generally aware of new security solutions and features, such as:



As awareness about new security solutions increases and discontent with existing security solutions among SMBs grows, the marketplace will adapt.

Chasing the marketplace

2016 is the year that the enterprise security market reaches a new saturation point. Incumbents will have the advantage and newcomers will divvy up a smaller fraction of the pie. Downmarket competition will force vendors to rethink their offerings.

As SMBs become aware of the risks, or incur the consequences of them, the drive for security solutions that fit SMBs specific needs will take foot, and new security solutions built for them will reach maturity. Next year, SMBs are likely to be the driver of new security solutions since they'll provide the opportunity for the most growth.



About ManagedMethods

ManagedMethods develops [Cloud Access Security Broker \(CASB\) solutions](#) that provide organizations visibility and control over Shadow IT and sanctioned cloud apps. ManagedMethods' solutions provide DLP, Threat Protection, Malware Scanning, Policy Enforcement and Discovery, and complement your existing network security investments (NGFW, UTM). Our solutions can be deployed on-premise or 100% in the cloud. Based in Boulder, Colorado, ManagedMethods solutions are available today through [managedmethods.com](#) or your trusted value-added reseller. Learn more at [managedmethods.com](#).