




Trust in Office 365

trust  *noun* \ˈtrəst\
: belief that someone or something is reliable, good, honest, effective, etc.

Trust is the foundation of every good relationship. That’s as true in business as it is in friendship. Today, more than 1.2 billion people worldwide trust Microsoft Office to provide a reliable productivity solution with commercial-grade privacy, security, and compliance features to help keep their data secured. Included among these people are a number of organizations that have enabled their employees to work from anywhere, anytime and on all of their devices with Office 365.

In the last 12 months, 75 percent of Fortune 500 companies have purchased Office 365. They trust us because we are committed to doing the best job of answering the three key questions below. Read on to learn more about how we can help with security, privacy and compliance when you move your organization’s data to the cloud and how our primary competitor, Google Apps for Work, has more limited capabilities in these areas.

1. How does Office 365 help my organization protect its privacy?

We recognize that you need transparency about and control over who accesses your organization’s data in the cloud. This is why we contractually commit to not use your organization’s data for any purpose other than to provide you with the services you pay for and to **give nobody standing access to your data**. We also provide you controls to limit who accesses your data when it is distributed with our services. Controls such as ‘Set Permissions’ in Outlook let email senders restrict copying, printing or forwarding of emails containing confidential information. Controls such as ‘Policy Tips’ alert email senders if their drafts contain certain sensitive content such as credit card numbers or personal health information that should not be widely distributed. We even enable IT administrators to set policies to automatically encrypt such content.

We have a rich history of offering and honoring privacy-friendly terms with our services, and we continue to play a leadership role in this area. Office 365 was the first cloud business-productivity service to address the rigors of the U.S. healthcare privacy and security requirements, and to help customers comply with the Health Insurance Portability and Accountability Act (HIPAA). We did so by convening experts from the academic, public, and private sectors in a joint effort that

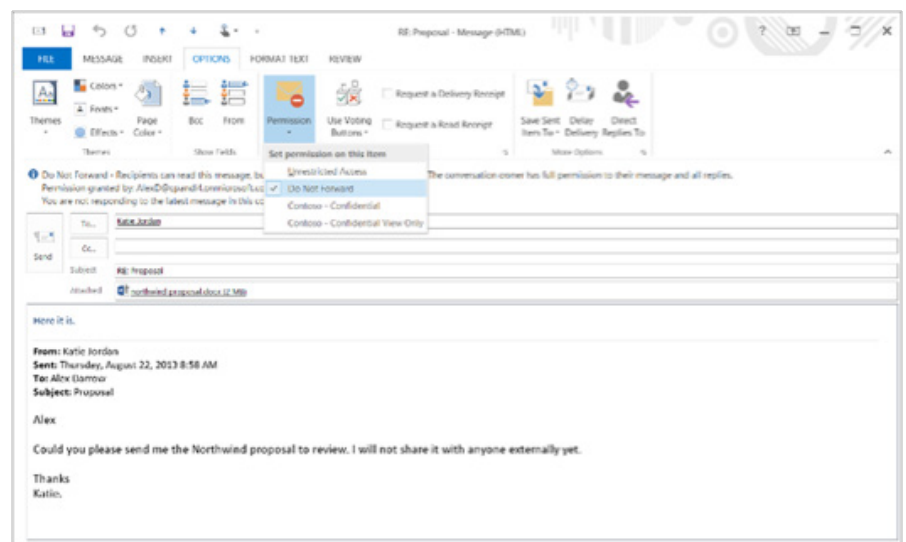


Figure 1 With Office 365, email senders can restrict others from sharing sensitive information. Permissions can be set via Outlook or OWA on every device: laptop, phone or tablet. Gmail offers no such capabilities.

resulted in crafting a business associate agreement (BAA) that satisfied the needs of regulated entities. We were also the first to receive **written validation from the European Union’s data protection authorities**, confirming that Microsoft’s enterprise cloud contracts meet the high standards of EU privacy law. Recently, we signed the **K-12 School Service Provider Pledge** to Safeguard Student Privacy, again being the one of the first cloud business-productivity services to do so.

In contrast, Google Apps for Work appears to offer limited controls in their technology, and limited terms in their contracts to assure customers that their personal data in Google Apps will not be used for purposes other

than providing the service. Google has been embroiled in lawsuits arising from questionable usage of user data. In **Gmail litigation**, Google is being accused of crossing a “creepy line” by using information gleaned from the scans to build “surreptitious” profiles of Apps for Education users that could be used for such purposes as targeted advertising. In **privacy policy litigation**, Google is being accused of misleading consumers by combining user data across several products and sharing it with advertisers without user consent. In response to the former litigation, Google’s lawyers first argued that Gmail users have no ‘legitimate expectation of privacy’ in email, but later, perhaps due to public outrage,

revised some of the data processing clauses in Google's terms of service for Google Apps for Work and Education. However, it is important to be aware that Google still doesn't offer its best terms upfront to all enterprise customers and requires them to opt-in. Also, it continues to leave wiggle room in its contracts by using indistinct language such as "we can"/"we may". Leading data protection authorities from EU have made several [recommendations to Google to improve its Privacy Policy](#).

"Using Google became a huge concern. We didn't know where our data was being stored or how it was being observed by Google. It's widely known that Google interrogates your information. We wanted to migrate to a more secure system that would protect the privacy of our email communication and documents."

Damian White, Facilities Manager at Caldera Health Ltd.

Caldera Health Ltd., a medical startup located in New Zealand moved from [Google Apps to Office 365 because of privacy concerns](#). "Using Google became a huge concern," says Damian White, Facilities Manager at Caldera Health Ltd. "We didn't know where our data was being stored or how it was being observed by Google. It's widely known that Google interrogates your information. We wanted to migrate to a more secure system that would protect the privacy of our email communications and documents."

2. How does Office 365 help my organization keep its data secure in the cloud?

In Office 365, we offer core security capabilities built into the service. This means you need not take on additional projects to deploy encrypted email, data leakage, eDiscovery, and rights management capabilities. A recent commissioned study conducted by [Forrester Consulting](#) estimated the savings that large companies might see as a result of this. Office 365 users surveyed in this study saw the following savings on average after moving to the cloud with Office 365:

- 6.8% reduction in compliance costs
- 10.7% reduction in time spent on eDiscovery efforts
- 73% decrease in the number of data breaches
- 32% reduction in the cost of those breaches

As the technology landscape changes and you move to a world of accessing your corporate data on multiple mobile devices, and sharing it not only via email but also via files in team sites and shared drives, we are constantly innovating to keep you secure.

Last month at TechEd we announced a [few upcoming updates](#) to our security capabilities being built right into Office 365. [New mobile device management \(MDM\) capabilities](#), set to roll out in first quarter of 2015, will enable you secured access to corporate data in Office 365 services from a diverse range of smartphones and tablets, including iOS, Android, and Windows Phone devices. The expansion of [Data Loss Prevention \(DLP\) capabilities](#) beyond email to additional Office 365 services and Office clients will help you to protect sensitive content no matter where it is stored and shared within our services. To further minimize the risk of unauthorized access to your content from our service, we are introducing a new and advanced encryption technology called per-file encryption.

In contrast, Google continues to attempt to sell enterprise users an incomplete solution and requires organizations to rely on third-party apps to meet critical needs such as Data Loss Prevention and On-Demand Message Encryption. The third parties offering apps in Google Apps Marketplace have varying levels of expertise in meeting enterprise needs, and might not bring the same rigor to building secure solutions as well-established cloud service providers.

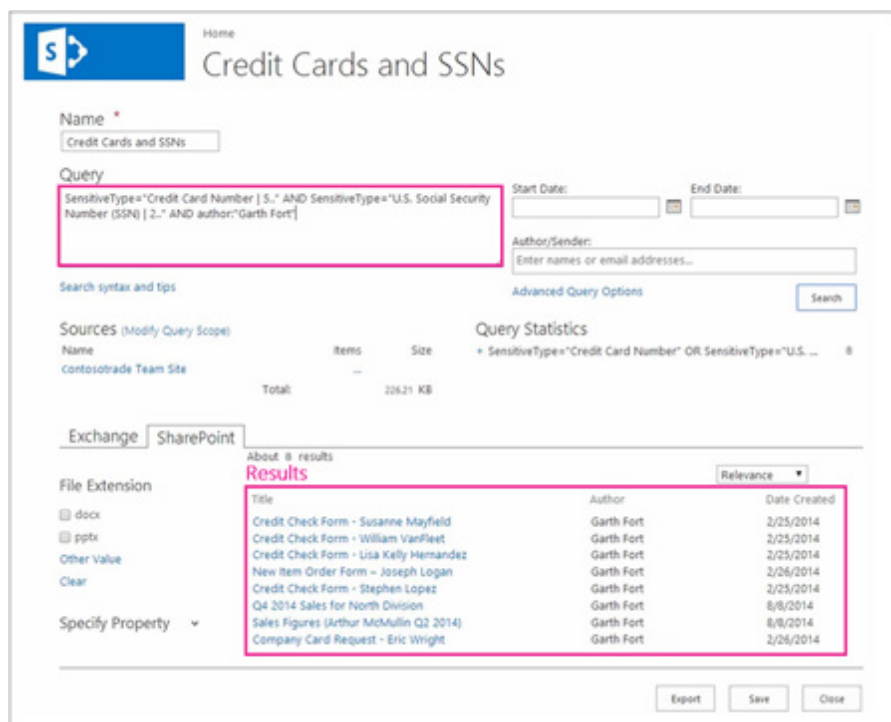


Figure 2 With Office 365, compliance officers can easily find sensitive information stored and shared within the services.

Goodbody, one of the largest wealth management firms in Ireland, Beginning in November 2011, [Goodbody evaluated Google Apps, but found that the messaging and productivity service did not have the security features that the firm needed.](#) “We had to be able to lock down who has access to information and limit where they can access it from. Google didn’t have a good solution for that,” says Stuart Halford, head of Technical Projects and Service Assurance at Goodbody.

3. How does Office 365 help my organization comply with regulatory standards?

At Microsoft, we go to great lengths to not only meet but also exceed your compliance needs. We have built more than 1,000 controls into the Office 365 compliance framework that enable us to stay up to date with ever-evolving industry standards. Our specialist compliance team continuously tracks standards and regulations, and develops common control sets for our product team to build into the service. Currently we are [working to meet ISO 27018](#), an international code of practice that establishes controls to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. As evident from <http://trust.office365.com>, we not only offer you transparency about where your data is stored, who has access to it and when but also offer you meaningful choices in these matters.

In contrast, Google offers minimal support to Google Apps for Work users concerned about compliance. For example, to customers who require compliance with The European Commission’s [Data Protection Directive](#), Google does not offer options to limit the regions in which their personal data will be stored or processed. To customers who require compliance with the FBI’s Criminal Justice Information Systems (CJIS) security requirements, Google does not promise to meet FBI background checks on the personnel that have access to customer content in their Government SKU. Even when Google claims to meet a compliance standard, they meet it in a limited fashion with only enough

Chief Information Officer. “In addition to functionality limitations, Google Mail had legal issues that could not enable us to restrict and store data within the United States, as policy requires us to. We also wanted support for retention and e-discovery policies that enterprise-class solutions often offer but that Google wasn’t even willing to talk to us about.” Instead, GSU chose Microsoft Office 365.

Your people and your data are your most important assets. As you consider moving your productivity solution to the cloud, we want to do our best to answer your questions. [Visit Office 365 Trust Center](#), the place where we share our commitments and information on trust-related topics.

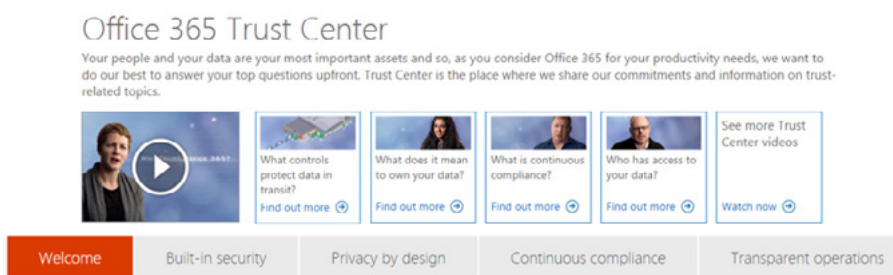


Figure 3 With Office 365 Trust Center, we offer you transparency and meaningful choices.

compliance capability to tick the checkbox on an RFP form. For example, Google’s Health Insurance Portability and Accountability Act (HIPAA) compliance does not cover Google Sites or Hangouts and requires users to disable Additional Services.

Georgia State University (GSU), one of the Southeast’s leading urban research institutions, [chose Office 365 over Google Apps for compliance related reasons](#) too. In late 2010, GSU began evaluating online solutions, including Google Apps for Business and Google Mail in particular. But that option didn’t meet the university’s needs. “There were several problems with Google Mail,” says J.L. Albert, Associate Provost and

“There were several problems with Google Mail. In addition to functionality limitations, Google Mail had legal issues that could not enable us to restrict and store data within the United States, as policy requires us to. We also wanted support for retention and e-discovery policies that enterprise-class solutions often offer but that Google wasn’t even willing to talk to us about.”

J.L. Albert, Associate Provost and Chief Information Officer, Georgia State University