smartsimple

www.smartsimple.com | 866.239.0991

How safe is your data in the cloud?

Do you know what precautions your cloud solution vendor has in place?

Strong security practices must be the number one priority for any cloud solution vendor you choose. Without that commitment, your data will be at risk.

But how do you know who has the right security protocols to protect your valuable information? This checklist highlights key security features that all cloud software vendors should provide. Use this list as a guide when evaluating how effectively vendors will meet their security obligations to you.

Security Feature	Description	SmartSimple	Vendor A	Vendor B
Penetration Testing	Regular, white hat hacking to make sure that a real hacker cannot access all your data, hijack other user accounts or redirect your users to bogus sites, even if the hacker has a legitimate user name and password. Vendor willing to share the latest results of this testing with you.	✓		
Vulnerability Testing	Regular testing that their servers are secured from known software vulnerabilities. Vendor willing to share the latest results of this testing with you.	✓		
Availability of Single Tenant Hosting Options	Clients have the option for dedicated hardware and their own fully segmented system.	✓		
Disaster Recovery Process (DRP)	All data is duplicated nightly and stored in a back-up location. A hot site is always available to ensure continuity, even in the event of a major disaster.	✓		
Authentication Policies	The system's security standards match your own corporate authentication policies.	✓		
Back End Management	Vendor and client share this responsibility. Vendor provides security for the application, client data, operating components and hosting.	✓		
Data Security	All data is encrypted on the server hard disk and during data transfer from the server to the client's local hard disk. For endpoint security, the vendor encrypts local hard disks and ensures data cannot be copied to removable media.	✓		

SmartSimple checks all the boxes when it comes to system security:

- ✓ SmartSimple scans for vulnerabilities weekly through our security partner, NetCraft.
- ✓ Reputable third party testing partners scrutinise our systems on an ongoing basis to ensure no one can hack your data.
- ✓ All SmartSimple hard disks are encrypted with AES 256, an industry standard algorithm.
- ✓ Data in motion is encrypted using HTTPS (Hyper Text Transfer Protocol Secure) transfer protocols combined with TLS (Transport Layer Security) ciphers to ensure the highest security when transferring data.
- ✓ Thanks to our standing as an Amazon Web Services (AWS) Advanced Technology Partner, organizations with an existing AWS relationship save money on a dedicated server option.
- ✓ Our backups are stored in secondary locations at least 400 km from our main data locations for extra security in the case of natural disasters.
- ✓ SmartSimple can meet any client security policies - no matter how rigorous.

SmartSimple is SOC 1 and SOC 2 Compliant

We subscribe to a high level of testing, training and compliance that ensures we meet very stringent standards, set by unbiased outside auditors. These professional auditors independently verify and certify that we are following regulated guidelines and are meeting our commitments. We are Service Organization Control (SOC 1 and SOC 2) compliant.

AICPA Service Organization Control Reports℠ AICPA SOC aicpa.org/soc Formerly SAS 70 Reports

AICPA Service Organization Control Reports℠ AICPA SOC 2 Formerly SAS 70 Reports

Contact us for the full details on how SmartSimple manages and protects your data.

www.smartsimple.com | Toll Free: 866.239.0991 | sales@smartsimple.com