OwnBackup Security Controls

Introduction

OwnBackup was designed from the ground up with security in mind. The architecture implements multiple security tiers designed to address different security concerns.

OwnBackup utilizes Amazon Web Services (AWS) for all its computing and storage needs. AWS is a top-tier facility with the following accreditations: SOC1 - SSAE-16, SOC2, PCI DSS Level 1, ISO 27001, HIPAA, etc.

OwnBackup implements the following controls in accordance with security best practices.

Security Controls

Web-application security controls:

- Access to the application is only via HTTPS.
- An OwnBackup account admin can provision & deprovision additional OwnBackup user access as necessary.
- All the user activities are audited (together with user, timestamp and source IP Address) & audits logs can be viewed by an OwnBackup Admin when logged into OwnBackup.com.
- Access to the OwnBackup account can be IP restricted (via the OwnBackup admin from the 'Account' tab).
- oAuth is used to obviate the need to store admin credentials wherever possible.

Encryption:

- At rest: OwnBackup uses AES256bit encryption on Amazon EBS volumes (via LUKS: Linux Unified Key Setup Package) for storing the users' backed-up data.
- In transit, always over HTTPS:
    - Salesforce->OwnBackup (backup agent): API access always over HTTPS.
    - OwnBackup->Customer: Always over HTTPS (TLS only).
- For internal DR purposes, OwnBackup takes twice-daily snapshots of the encrypted volumes onto Amazon S3.

Firewall:

- OwnBackup utilizes Amazon's Security-groups to limit network access.

Monitoring and auditing:

- OwnBackup collects application, network and OS events to a central syslog server. These logs are analyzed and reviewed to detect suspicious activity, and prevent threats. Any anomalies are escalated as necessary.
- OwnBackup's Incident Response team (available 24x7) monitors security@ownbackup.com and works according to our Incident Response Plan (IRP) when necessary.

Isolation between accounts:

- OwnBackup uses extreme Linux Sandboxes to isolate OwnBackup accounts' data. This ensures that any anomaly, either due to security issues, or an internal software bug, will always be confined to a single OwnBackup account.

Vulnerability management & security updates:

- OwnBackup undergoes periodic penetration testing and vulnerability scanning to maintain the security of our application. In addition to scans conducted by our team, we undergo external security evaluations (most recently in June 2014 by Salesforce, as part of their yearly security evaluation).
- Puppet is used to maintain configuration across OwnBackups' instances such that security updates can be efficiently deployed.