

Security and the SaaS BackupGrid

Introduction

Today, more companies than ever recognize the value and convenience of using online backup to protect their server data. Enterprises considering software-as-a-service online backup face these security concerns:

- Could an unauthorized individual gain access to backed-up data?
- Could backed-up data be altered?
- Will necessary data be available when needed?
- Is data safe from fire, floods, and human error?

Utility Backup Solutions offers hosted data storage that enables customers to reduce the costs, risks, and complexity of storing and protecting their business information. With our heightened focus on security, privacy, and cost savings, Utility Backup Solutions goes beyond simple cloud storage to enterprise Storage as a Service.

The SaaS BackupGrid

The SaaS BackupGrid service from Utility Backup Solutions addresses all these concerns with the most secure solution available. For example, the software agent encrypts all data before transferring it from the customer's servers. All data remains encrypted at the secure off-site Data Bunkers and on optional TurboRestore appliances. Only the customer controls the data encryption passwords. To ensure the physical security and availability of stored data, the SaaS BackupGrid service employs a fully redundant vaulting infrastructure at two underground Data Bunkers maintained by Iron Mountain.

Security for Data in Transit

The SaaS BackupGrid service assures that the connection between application servers and the secure off-site Data Bunkers is secure. The SaaS

BackupGrid service uses the best security methods available, including:

- *Automatic, outbound-only connections:* There is no added security risk to the customer's environment. In particular, there are no inbound connections. The software agent on a customer's server communicates only with the SaaS BackupGrid backend infrastructure. The agent initiates all connections from the customer's server (outbound connections) over two ports reserved for the SaaS BackupGrid service, or over port 443 (the SSL port) if those ports are not available. Normally, there is no need to alter the firewall security perimeter. This makes installation particularly simple and secure at remote sites.
- *Public key encryption for mutual authentication:* the SaaS BackupGrid backend infrastructure and the Agent software independently validate certificates each time a connection is made. This authenticates the Agent to the electronic vault, and the vault to the Agent.
- *256-bit Advanced Encryption Standard (AES) encryption of all data before transmission and storage:* your data is encrypted during transmission and remains encrypted at all times while stored at the secure off-site data center. 256-bit Advanced Encryption Standard is the level of encryption that banks and government agencies employ.
- *Customers control encryption key passwords - escrow service available:* Customers may keep their encryption passwords private, so there is no possibility of any Utility Backup Solutions employee accessing customer data. We also offer a free, optional escrow service for encryption passwords, which

enables customers to recover data even if the encryption passwords are not available.

- *Customers can change encryption passwords:* If there is a potential security breach, such as when a trusted individual leaves a customer's company, the customer can simply change the data encryption passwords, which is similar to changing the door locks. Older backed-up data can still be restored, but only with the new password.
- *Digital signatures:* All communication between the Agent and vault uses industry-standard SSL (Secure Sockets Layer). This prevents any accidental or malicious modification, and protects the integrity and confidentiality of all data.

Security for the BackupGrid Web Management Portal

The BackupGrid Web Management Portal is convenient for customers to use because only a Web browser is needed for access from anywhere in the world. Security features of the Web user interface include:

- *Encrypted communication:* Secure Sockets Layer (SSL) encryption protects the BackupGrid Web Management Portal.
- *Data Protection:* The contents of backed-up files are not accessible.
- *Privacy protection:* Because data encryption passwords are not set or accessed with the Web user interface, even if someone steals a user's login and password, they cannot restore any data, except to the specific computer where it originated.
- *Strict password rules are available:* A company can set password specifications for their account, such as minimum password length, reuse policy, expiration period, and requirement for non-alphabetic characters.
- *Limits on insider attacks:* Customers can grant users only the rights and privileges necessary for their specific job duties. For example, a help desk person might have the ability to initiate restores, but not to set or change backup policies or add other users. Similarly, an IT administrator might have some (or limited) responsibilities for servers

and users where they work, but not be able to see or manipulate servers or user accounts at other locations.

Physical Security for Data Stored in Electronic Vaults

Utility Backup Solutions has partnered with Iron Mountain to offer secure off-site storage in Iron Mountain's Data Bunkers that provide high-security, environmentally-controlled storage for media. These Data Bunkers include data centers with redundant infrastructure.

The Data Bunkers include the following security measures:

- Extensive multi-acre underground sites.
- Gated entrances with 7x24 guards.
- Restricted access requiring photo ID and visitor escort.
- Real-time closed circuit TV monitoring.
- Commercial power feeds with generators for full backup power.
- Clean Agent Fire Extinguishing System (CAFES) and on-site firefighting apparatus and personnel.
- Internal and external 24x7 environmental monitoring alarms for temperature, "waterbug" leaks, smoke, fire, and motion detection.
- External accreditation by the Uptime Institute according to their Tier Classification and Performance Standard.

The data centers within the Data Bunkers have achieved SysTrust certification, which satisfies the specific Trust Services Principles and Criteria of the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). SysTrust examination assures that a system is reliable when measured against four essential principles: availability, security, integrity, and maintainability.

SaaS BackupGrid Vaults

SaaS BackupGrid data is stored in electronic vaults in each data center. When customers sign up for the SaaS BackupGrid Service, their data is mirrored between vaults at each site for high availability. The

Service Operations Center (SOC) constantly monitors the Data Bunkers, data centers, and vaults. In the unlikely possibility of a failure, backups are rerouted and continue automatically to the remaining vault. When the failure is repaired, all missing backup data replicates to the repaired or replaced vault. All other elements of the backend infrastructure, such as the Web servers, the backend database, and the command and control systems, are also redundant.

Storage Security

All data stored on SaaS BackupGrid vaults (and on TurboRestore appliances or Media Restore Devices) is encrypted with 256-bit AES encryption. The only time data is decrypted is when the software agent on a customer's server receives encrypted data while processing a restore request.

Secure, Reliable Server Protection

The SaaS BackupGrid is based on Iron Mountain's award-winning LiveVault technology, the same technology platform that world-class service providers including IBM, HP, and LexisNexis have selected to protect their customers' valuable data. Today, over 20,000 servers worldwide and 1.8 petabytes of customer data are under the protection of the LiveVault technology.

Data backed up with the SaaS BackupGrid is automatically off-site and safer than it is in the customer's own facility. Customers rely on Utility Backup Solutions to have their data available when they need it, while protecting the privacy and integrity of the data.

About Utility Backup Solutions

Data is the lifeblood of any company, and data backup in the modern era should be as simple as 'plugging in' to a utility that is always on, always reliable and can actually deliver when you need it.

Utility Backup Solutions offers best-of-breed, one-stop data protection and recovery solutions designed specifically to address the special needs of today's small- and-medium-sized businesses. With our automated solutions for servers, our customers can reduce operational costs, focus staff on new initiatives and improve workforce productivity, adhere to regulatory and compliance concerns and achieve total peace-of-mind.

The SaaS BackupGrid service, based on Iron Mountain's award-winning LiveVault platform, is a comprehensive solution for online protection and recovery of server data for small-and-medium businesses in North America. The SaaS BackupGrid is offered in a utility billing model—that is, the services provided to our customers are consumption-based, pay-as-you-go software-as-a-service subscriptions.

With Utility Backup, you can finally abandon the administrative and financial burden of a legacy magnetic tape backup program, and join the thousands of satisfied customers enjoying the "set-it-and-leave-it" reliability of a modern data protection solution.

We pride ourselves on offering a valuable and effective solution to a real problem for our customers. We believe in transparency, customer satisfaction, and providing true value. If we are successful, we believe we will be rewarded with long customer relationships.

Contact Us

Utility Backup Solutions, LLC
570 El Camino Real #150-501
Redwood City, CA 94063-1262
888-374-3282
www.utilitybackupsolutions.com