opentext™ | Cybersecurity

WHITE PAPER

Server Backup for greater security and control

Server Backup offers multiple layers of data protection and resilience across a scalable, secure infrastructure

OpenText Cybersecurity provides partners with a powerful and easy-to-manage cloud backup solution, Server Backup. It includes features for configuring, managing and supporting server backup activities. Through an easy-to-use agent installer, users can register their servers and use the centralized portal to create backup jobs to meet their protection needs. Backup options and configurations include:

- File/folder backup
- Application backup (SQL, Exchange, Oracle)
- System state backup
- Image-level backup
- UNC path backup
- On-premises backup
- Cloud backup
- Hybrid backup (cloud and on-premises)

Backing up to multiple locations provides different options for recovering data and preventing data loss. Server Backup delivers both robust protection and straightforward recovery processes.

Security

Server Backup offers the control and visibility features IT administrators need to ensure logical segregation of duties between customers, partners and OpenText operations teams. Behind the scenes is a proven, secure and sophisticated infrastructure built to protect data during transit and in storage.

Control and Visibility

With critical tools available in a multi-tenant portal, OpenText Cybersecurity empowers administrators to customize the configuration of Server Backup to meet business requirements. Key features include:

- Discrete "child site" hierarchy to support autonomous administration of individual customers
- Role-based access for administrators
- An intuitive portal able to group backup assets logically
- Discrete encryption per backup job for extended privacy
- Logically separated data vaults (and credentials) designated per customer
- Aggregated, historical reporting

The multi-tenant hierarchy of Server Backup ensures logical separation of both administrative and data management duties, ensuring data remains private and under the control of the customer.

Access Control

Access to the backup agent and the backup portal – for scoping and scheduling administration (job configuration) or initiating backups and restores (data transfer) – is strictly controlled. The robust username and password requirements can (and should be) further enhanced with two-factor authentication (2FA).

Two-Factor Authentication

When configured, two-factor account authentication provides an extra layer of security when logging in to the Server Backup portal. Users can set up two-factor account authentication anytime by entering a phone number in their profile settings. Users with two-factor account authentication configured will be prompted to enter a code periodically (every 30 days) when they sign into the portal, when they want to reset their passwords and when they sign into the portal from a new web browser. Users have the option to receive authentication codes via text (SMS) messages or automated voice calls.

Agent Registration

Each backup agent deployed to protect source servers requires portal registration. This process requires administration access to the server and authentication via a set of portal credentials, which are managed in the portal administrator account.

Detection

Ransomware is the bane of every business. Potential ransomware detection for Windows and VMware vSphere environments automatically flags anomalies and provides multi-level alerting capabilities like dashboard warnings, threat views and automatic email notifications. If confirmed, uncompromised data can be quickly restored and recovered.

Encryption

Central to the data security model is data encryption. Server Backup uses AES-256 bit private key encryption for all jobs, with an encryption key being created for each job as follows:

- The customer provides an encryption password, which is stored encrypted on the agent in the customer's environment.
- The encryption password provided by the customer is used to generate the key for the AES-256 encryption.
  - This password is not stored in the user interface (UI) system or read from the agent when the UI loads the job settings from an agent.
- The data is encrypted on the customer's system using the customer-provided encryption password prior to being sent to the vault.
- The data is transmitted over a separately encrypted channel.
- When restoring, the data is returned encrypted from the vault and decrypted on the customer's system.
  - The encryption key is not stored in the vault or transmitted to OpenText.

OpenText recommends customers always carefully choose strong random encryption passwords. Also, to prevent and detect malware from accessing the agent, we recommend you install reliable endpoint protection software.

IMPORTANT: The encryption password is required for restoring data. Store it safely. If the password is forgotten, restores will not be possible. If the administrator changes this encryption password for an existing job, it will force a new full backup (i.e., a reseed). Older recovery points will require the previous password. It is imperative to maintain the password history and date of any change.

Transport Layer Encryption

The second implementation of AES protects packets sent between the source server agent and the data vault. In this case, the full packet is encrypted and sent to the server where it is processed. The agent initiates the connection with the server on a pre-determined TCP/ IP port. This port may be customized to suit individual network settings and preferences. Upon connection between the agent and the server, there is an initial handshake to ensure the connection is authorized.

Vulnerability Remediation

OpenText uses regular vulnerability scans, including code-level scans and application-level scans. All results are regularly reviewed, and any security issue is triaged and remediated quickly. Further details are available in our SOC 2 Type 2 report, available upon request when customers sign a non-disclosure agreement (NDA).

Architecture

Server Backup is designed with multiple layers of protection, including secure data transfer, encryption, network configuration and application-level controls distributed across a scalable, secure infrastructure. The system itself is comprised of modular components (portal, data vault and agents) isolated from each other to promote service availability and robustness.

Infrastructure Resilience

Server Backup is built on over 20 years of system hardened software reliability. Our data centers are designed and built to industry standards with multiple layers of fault-tolerance at the component and systems level:

- N+1 redundant compute and storage components
- Redundant server configurations and rack installations
- Multiple, uninterruptible power supplies with battery backup to ensure clean and stable power
- Emergency power generators, which are automatically activated in the event of a power disruption
- Diversely routed networks supplied through multiple providers
- Physical protection measures, including but not limited to:
  - Redundant independent cooling units
  - Temperature and humidity control
  - Chillers feeding CRAC units
  - Early smoke detection system
  - Gas-based fire suppression

- Disaster recovery plans for critical components of the infrastructure, for example:
  - Vault databases backed up locally, twice per day
  - Local vault database backups, which are copied offsite at least every eight hours
  - Offsite copies backed up once per day
- OpenText takes various steps to protect data:
  - Multiple copies of each byte, which protects against drive or node failures
  - Daily snapshots of data are stored for four days
  - Physical access restrictions at all OpenText facilities
  - Access is controlled via on-site security personnel and all access is recorded
  - Facility monitoring includes all perimeter doors, security alarms and digital surveillance and video cameras that monitor and record entry and exit to prevent unauthorized activity

Data Reliability/Durability

Critical to any backup service is data integrity. Server Backup has robust data reliability features present within the service to ensure data reliability over remote connections.

Quick File Scanning (QFS)

Server Backup uses a proprietary, patented technology called Quick File Scanning to examine the metadata of a file and determine if it has changed since the last backup. This ability to quickly scan large data sets and only find files with changes is critical to the efficiency of the solution and for reducing the impact of backup workloads over the network.

DeltaProTM – Delta Processing

Beyond leveraging QFS to identify changed files, our proprietary and patented DeltaProTM data processing allows us to find block-level changes within the changed files. The combination of both QFS and DeltaProTM technologies enables high optimization of data processing to help businesses shrink the window for potential data loss while reducing the impact on the network.

Backup/Restore Transfer Protocol (BRTP)

In addition to DeltaProTM, the Server Backup agent performs remote backups and restores by first making a secure connection with the data vault using TCP/IP. It then implements the proprietary Backup/Restore Transfer Protocol (BRTP) to pass control information and the actual data back and forth with the data vault. This helps ensure accurate write-order sequencing, even over intermittent connections.

Data Availability

Server Backup is a fully hosted solution operated by an experienced operations team. Operations and support teams work on a follow-the-sun basis and are on call 24×7.

Occasionally, the service may become unavailable due to upgrades and other maintenance procedures. These events are planned, and notification as well as a maintenance window are communicated in advance.

- **Scheduled maintenance**. OpenText conducts scheduled maintenance quarterly and monthly to apply operating system and security patches. Partners and customers are given a seven-day notice.
- **Unscheduled maintenance**. OpenText may conduct unscheduled maintenance to address certain new vulnerabilities or applications and infrastructure changes that may be required in the immediate future. Partners and customers are given a one- to six-day notice.
- **Emergency maintenance**. OpenText may conduct emergency maintenance to address issues that may critically impact the service and require immediate remediation. There is no advance notice for emergency maintenance.

Partners and customers may check the service status by visiting the Server Backup section of our status page at https://status.carbonite.com.

Compliance

OpenText engages annually with an independent third-party audit firm to provide attestation of compliance with SOC 2 Type 2 requirements. OpenText operates a control framework based on adherence to several industry standard regulations including:

- Health Insurance Portability and Accountability Act (HIPAA)
- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)

Additionally, Server Backup is ISO 27001 certified and adheres to PCI-compliant processes for customer payment transactions.

System and Organization Controls (SOC)

Partners and customers may request the current SOC attestation report via their account representative (current NDA required). The validated SOC controls in place for all Server Backup services cover the industry best practice for cloud services as outlined by the Cloud Security Alliance (CSA). These include but are not limited to:

- Application & Interface Security
- Encryption & Key Management
- Interoperability & Portability
- Audit Assurance & Compliance
- Governance & Risk Management
- Mobile Security
- Business Continuity Management & Operational Resilience
- Human Resources
- Security Incident Management, E-Discovery & Cloud Forensics

- Change Control & Configuration Management
- Identity & Access Management
- Supply Chain Management, Transparency & Accountability
- Data Security & Information Lifecycle Management
- Infrastructure & Virtualization Security
- Threat & Vulnerability Management
- Data Centre Security

Health Insurance Portability and Accountability Act

The U.S. federal Health Insurance Portability and Accountability Act (HIPAA) specifies how healthcare organizations should handle protected health information (PHI). It's not just healthcare organizations that are affected by federal healthcare legislation. Any business that handles protected health information must comply with federal requirements for securing electronic medical records (EMR). This includes legal and accounting firms, and web hosting businesses, to name a few.

Under the regulation, OpenText regards itself as performing the functions of a business associate and has enhanced its compliance program to facilitate the ability to maintain a HIPAA-compliant infrastructure. Wherever necessary, OpenText will enter into a Business Associate Agreement, providing contractual assurances that we will comply with HIPAA with respect to PHI. In addition, OpenText uses vendors that are willing to enter into HIPAA-compliant agreements, assuring the same stringent standards. OpenText has designed solutions that comply with the more than 40 privacy and security safeguards required under HIPAA.

Data Sovereignty

For customers operating in regulated industries or in countries with data protection laws, it's important to know the geographic location of their data. OpenText offerings within the Server Backup portfolio include the following geographic-specific facilities for organizations that must keep and handle data within a specific region due to a regulatory framework:

- U.S. x2
- Canada
- United Kingdom
- Holland

General Data Protection Act (GDPR)

Server Backup includes technology solutions for keeping personal data secure, ensuring data residency and restricting access for unauthorized users. Server Backup helps support General Data Protection Regulation (GDPR) compliance for EU organizations including the following:

Rectification

Server Backup is designed to automatically capture any and all changes made to source data. So, if there's a need to correct or supplement data in production, those changes will be reflected automatically in the next periodic backup without any additional manual intervention necessary.

Erasure

Data retention periods are easily configurable to delete old datasets after a predetermined period. For example, if the retention period is set for 30 days, and the number of datasets that are retained is configured at 30, any old backups in excess of the 30 datasets specified would be deleted at the end of that period.

Privacy

Server Backup uses AES-256 bit private key encryption for all jobs and data, with an encryption key being created for each job. The customer provides an encryption password, which is stored encrypted on the agent in the customer's environment. The encryption password provided by the customer is used to generate the key for the AES-256 encryption. The encryption password is not stored in the UI system or transmitted to OpenText. This further limits access to data. Data is transmitted to OpenText over a separately encrypted channel.

OpenText recommends customers always carefully choose strong, random encryption passwords. Also, to prevent and detect malware from accessing the agent, we recommend you install reliable endpoint protection software.

Records of Processing

To assist with data processing record-keeping requirements, OpenText offers various reports that can be scheduled and emailed to users. For example:

- **Daily status report** This report includes backup status information for the previous 24 hours, including missed backups and running jobs for computers running the latest agents.
- **Backup details report** This report provides detailed information about each time a backup job ran during a specified time period, including the amount of data backed up, the amount of data changed since the last backup and whether the backup was successful or not.
- **Activity details report** This report provides information about activities in a site during a specified time period, including backups and restores.
- **Usage summary reports** and more.

For more information on GDPR and how it can affect a business, please visit:
https://www.carbonite.com/what-is-carbonite/gdpr

Privacy

When governments or law enforcement make a lawful request for customer data from OpenText, we are committed to transparency and limit what we disclose. We believe customers should control their own data. The organization will not disclose data hosted in any cloud service to a government or law enforcement agency except as directed by customers or where required by law. When a government or law enforcement request for customer data is received, we always attempt to redirect the third-party to obtain the requested data from our customers.

OpenText does not have direct access to customer data. Without the job encryption password provided by the customer, or access to the agent system (controlled by the customer), we cannot decrypt backup data.

For more information please consult:
https://www.carbonite.com/terms-of-use/privacy-policy

Next Steps

OpenText Cybersecurity brings together best-in-class solutions to help your business remain cyber resilient. We can help you prevent and protect against threats from happening in the first place, minimize impact by quickly detecting and responding, recovering data seamlessly to reduce the impact and help you adapt and comply with changing regulations. Server Backup offers businesses a straightforward and reliable backup and recovery solution that securely preserves data confidentiality, integrity and availability while minimizing downtime for your day-to-day operations.

For more information, contact your Account Manager or the sales department. Visit carbonite.com for additional information.

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk. WP_031323