US SIGNAL®

Backup-as-a-Service

US Signal's Backup-as-a-Service is powered by the Acronis Backup Cloud Engine to provide you with deep agent compatibility, offsite storage, easy to use management portal, and simple recovery operations.

At a Glance

- Agent-based backup solution providing a hosted management portal and offsite storage
- Supports hypervisor integration with on-premises deployments
- Supports full image level, individual file/folder, and application specific restorations
- Deep agent compatibility across operating systems, applications, and virtualization platforms
- Solution can be managed by US Signal to offload daily management and troubleshooting
- Built-in data compression to reduce the amount of data transmitted over the network
- Ability to throttle bandwidth and CPU on a per machine basis to ensure continued performance objectives

Technical Overview

The US Signal Backup-as-a-Service platform is an agent-based backup and recovery solution that can store backup files either on-site or on US Signal hosted cloud storage. Individual servers can be protected by installing the backup agent directly inside any supported operating system and will even provide application protection and recovery for supported applications. Agents can also be installed on any server with network visibility to your hypervisor, to provide a backup and recovery solution for VMware vSphere or Microsoft Hyper-V.

Backup-as-a-Service can be managed by you, unless you want to US Signal to fully manage the solution end-to-end. Our US Signal professional services engineers can be engaged to install agents on your protected workloads, create and maintain backup jobs, fully monitor the solution, and recover your files or servers back to the source environment.

Backup Operation and Features

- Customizable levels of source data compression
- Bandwidth throttling
- Agent activity CPU throttling
- Schedule backup jobs and retention from the web management portal
- Optional AES-256 encryption
- Local (on-premises) backups and / or cloud copies

Security

All traffic sent from the client machine to US Signal cloud storage is transmitted over SSL encryption. Create your own key to enable AES-256 key encryption within the backup plan settings. In doing so, the backup data will be encrypted before transmission from the source server; providing end-to-end encryption from the source and destination storage environment. Any restoration of AES-256 encryption backup data requires input of the key before a recovery can be executed.

Serviceability

The Backup-as-a-Service management and storage servers are publicly accessible endpoints, thus you can protect any source environment including servers or applications hosted in your own datacenter, US Signal Resource Pool servers, or US Signal Hosted Private Cloud workloads. The only connectivity requirements are access to the Internet and allowing specific outgoing TCP ports utilized for backup operations.

Supported Operating Systems and Applications

Operating Systems

- Microsoft Client Operating Systems XP and above
- Microsoft Server Operating Systems 2003 and above
- Mac OS X
- Red Hat Enterprise Linux 4.x and above
- Ubuntu 9.10 and above
- Fedora 11 and above
- SUSE Linux Enterprise Server 10 and above
- Debian 4 and above
- CentOS 5.x and above
- Oracle Linux 5.x and above

Applications

- Microsoft SQL
- Microsoft Exchange
- Microsoft SharePoint
- Active Directory
- Office 365 Mailboxes

Hypervisors

- VMware vSphere
- Microsoft Hyper-V

Backup Types

Disk/Volume – Contains an entire copy of the selected disks or volumes and can provide recovery for entire disks, volumes, and individual files and folders.

File/Folder – Protect user-defined individual files and folders on the source machine.

System State – Only available for servers running the Windows operating system and protects the following system files:

- Task scheduler configuration
- VSS Metadata Store
- Performance counter configuration information
- MSSearch Service
- Background Intelligent Transfer Service (BITS)
- The registry
- Windows Management Instrumentation (WMI)
- Component Services Class registration database

Applications – Protect and provide granular level restores for application specific data from supported applications.

Office 365 Mailboxes – Protect Office 365 mailboxes and provides granular restores for individual items or entire mailboxes.

Recovery Methods

File – Individual files or folders can be directly restored to any machine with an installed agent or downloaded from the management portal.

Image – Restore entire physical servers or virtual machines using the included boot media.

Backup Locations

Cloud – Backups can be stored in US Signal's cloud storage environments in any one of the following markets:

Grand Rapids, MI
Detroit, MI

Network Share – Store backups on SMB/CIFS/DFS network shares accessible by the source machine.

Local – Store a copy of the backup files on the source machine performing the backup.

Hybrid - Leverage Cloud, Network, or local locations to provide backup resiliency.

Service Level Agreements

Storage infrastructure availability of 100%

Managed Backup – Support response of 2 hours from the time a request is received.

Managed Backup (Optional)

US Signal will manage the following aspects of the Backup-as-a-Service platform on your behalf:

- Agent installation and upgrades
- Backup job creation or modifications
- Restoration of images and files/folders to source
- Monitoring of backup plan success and failure activity

FastPath (Optional)

Additional add-on for US Signal cloud customers to offload backup traffic from their Internet access port, by providing private network routes to management components and storage infrastructure, so the Internet port is not consumed by backup traffic.

Compliance

US Signal's BaaS solution is built using HIPAA and PCI security standards helping you achieve your compliance requirements.