iVault Online Backup for Windows®

Enterprise-class data protection for Microsoft Windows® infrastructure

● www.ivault.nl ● info@ivault.nl ● tel: +31 (0)174 443266 ● fax: +31 (0)174 443699

Why iVault Online Backup?

Your data is precious to you. It represents an enormous investment in work and therefore money for your company, or it may have priceless emotional value for you personally. A reliable and secure backup is therefore a necessity. But what constitutes a reliable and secure backup? Are you protected against theft, burglary or fire? Where and how securely is your data kept? Does the solution grow with your company? And when things go wrong, can you rely on immediate and knowledgeable support to get your data?

iVault provides reliable and secure cloud backup solutions for Windows, Macintosh, Linux- and Unix environments, already since 2005, and for hundreds of companies. Realistic solutions that are robust and flexible and actually deliver on their promise, guaranteed and real life proven in harsh daily IT practice, day after day.

Enterprise-class infrastructure

iVault cloud infrastructure utilizes **UNIX®** en **industry-grade hardware** to achieve unparalleled reliability. Our choice for the UNIX operating system was driven by the unparalleled robustness and maturity, resulting from a development history of over 40 years.

To guard your data securely, iVault makes maximum use of enterprise computing features exclusive to UNIX. Among them are the active prevention of silent data corruption (**bit-rot prevention**), instant copy on write **snapshots**, **deduplication** and real-time integrity checking of our entire software stack through **dynamic tracing**.

Datacenters in The Netherlands

With the continuing strengthening of Dutch and European data protection laws and increasing concerns about privacy intrusion, the actual physical location of external data is rapidly gaining importance. iVault data is stored in multiple premium tier data centers, all **exclusively located in the Netherlands**. The exact physical location of your data is always **known** and **guaranteed**.

Partner support

iVault partners are offered a wide range of support:

Primarily our partners have unlimited access to our world-class **technical support**. The quality of our support is historically one of the main reasons to choose for iVault, mainly because, especially in more complex customer cases, you will inevitably end up in situations where you find it indispensable. We have in-depth knowledge of the Windows, Unix, Linux and Mac OS X ecosystems, not only as **system managers** but also as **infrastructure architects** and **software developers**.

Furthermore, our partners have access to **the iVault Self Service Portal**, offering them a simple method of complete maintenance and monitoring for their customers' accounts. For further integration with partner systems, iVault offers various interfacing options through Self Service Portal or backup server APIs.

iVault also offers wide-ranging branding options for White Label partners. The entire backup solution, including client- and server side software, reporting and documentation, is extensively customizable to achieve a customer specific look-and-feel.

iVault Online Backup for Windows

With **Online Backup For Windows** iVault delivers a modern and secure cloud backup solution for your physical and virtualized Windows- and mixed-platform environments, providing a complete and superior replacement for traditional tape backup. Your data is pre-encrypted on-premise before secure transfer to our Dutch datacenters. Our service has many, necessary, reliability, security and operational features. Below the most important ones are described in more detail:

Security

Security and confidentiality of your data is paramount. iVault Onling Backup utilizes **Zero-Knowledge On Premise Encryption/Decryption**. Our client software encrypts your data on your local systems, within the confines of your office, and before transfer, using encryption keys only known to you. Transfer, external storage and eventual retrieval of your data is always handled in encrypted state. At restoration time, decryption only happens at the very last moment, and only locally on your own system. Our encryption utilizes industry-grade algorithms like **Advanced Encryption Standard (AES)** or **TwoFish** with depths of 256bits. All data transfers to our DC servers are handled over secure **SSL/TLSv1**. To further enhance security, the system has an intrinsic **Zero-Knowledge** architecture, without external storage and/or knowledge of encryption keys on our servers. In other words: Neither iVault, nor anyone else, can read your data.

Reliability

Apart from being geographically separated, a reliable backup must be both up to date and verified. To guarantee actuality, iVault Online Backups are executed **automatically on schedule**, preventing them from being forgotten. The backup process continues, independent of your users, also on weekends and holidays. Executed backups are **automatically verified** for correctness and their status is always confirmed by e-mail.

Redundance by replication

Each remote backup is firstly stored on a primary iVault backup server and subsequently replicated to a secondary iVault server. This way your data will not only survive a calamity within your company, but even a calamity at iVault.

Local copy

For some companies, the presence of a physical backup copy on-premise is a hard requirement. iVault Online Backup therefore provides the option to maintain a local copy of the backup, next to and in parallel with the main, remote backup. Since the local copy also retains full history, restores can be executed fully and quickly from this local copy only, if so desired.

Easy access to current and historic data

iVault Online Backup offers simple access to your current data but also to many previous versions of your data, days, weeks, months or even years in the past. All complexities of incremental and differential restorations are handled by the iVault Backup Client and Server. Control of the software is therefore surprisingly simple and can be learned by non-IT staff. Restorations of regular files can realistically be handled by end-users, without further support from IT departments.

Mixed-platform support

Does your company infrastructure comprise other systems than just Windows? iVault Online Backup is a universal solution for all data on all your systems. It does not matter if your data resides on Windows machines, Macs, Linux or Unix servers. Besides Microsoft Windows, iVault Online Backup is available for Mac OS X, Linux, Unix, FreeBSD as well as for hypervisors VMWare and HyperV.

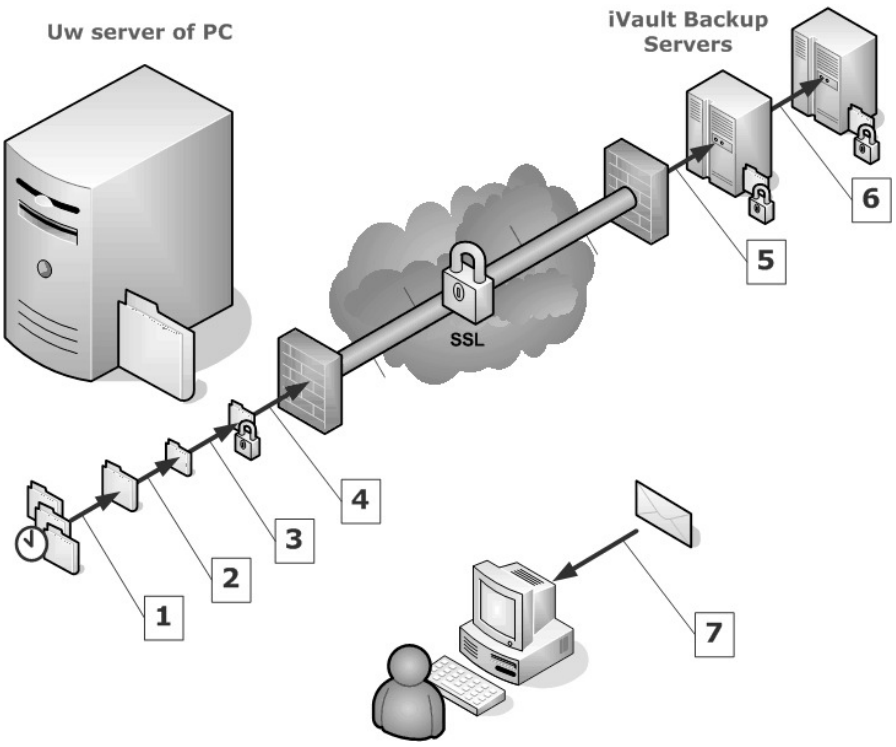
Microsoft Exchange, Microsoft SQL Server and Virtual Machine backup

The complexities of mail-, database- and virtual machine backup are a well-known risk factor in your backup process, since most of these environments require additional pre-processing and quiescence to obtain a reliable backup.
iVault Online Backup contains built-in support for proper backup of the most important Windows layered products, including the relational databases Microsoft SQL Server, Oracle and MySQL, the mail and collaboration solutions Microsoft Exchange and Lotus Notes as well as virtual machine backup support for VMWare and HyperV.

Cost savings

You pay a fixed amount per backed-up system per month. Rates are dependent only on the size of your data and not on the type of system, type of data, or the frequency of your backups. In one sweep you eliminate all purchase and maintenance costs for tape drives, tapes, external storage, transport and tape-backup software. Modules for backup of regular layered products, including Microsoft Exchange, Microsoft SQL Server, Oracle, MySQL and Lotus Notes are included in our standard offering without additional fees. Furthermore you will save significant amounts of time: Changing, transport and maintenance of tapes is a thing of the past and restoration of data is sped up by factors of time since all your backups remain online and instantly accessible. Generally savings of up to 50% are achievable compared to traditional tape backup scenarios.

iVault Online Backup, how does it work?



1. **Selection:** At a preselected time, continuously or at your command, the iVault Backup Client selects new and modified files on your system for backup, according to preset file selections. Backup files for layered products like Exchange and SQL Server, as well as snapshots of Virtual Machines are reliably generated and locally buffered.

2. **Compression:** Backup files are compressed to speed up transfers to the max. After an initial one-time full transfer, iVault Backup Client utilizes In-File-Delta technology to reduce the transfer size to no more than the modified blocks within files. With these methods radical compression rates of 95% and higher are routinely achieved on incremental backups.

3. **Encryption:** Files are encrypted with industry-grade algorithms like **Advanced Encryption Standard (AES)** or **TwoFish** with depths of 256bits. The 256 bits AES encryption is of professional grade and commonly in use by financial institutions and governments. Only you know the key to your data, since our **zero-knowledge** architecture guarantees it is not known anywhere outside your systems. Without it, nobody will be able to decipher your data. Not even iVault staff.

4. **Transfer:** A secure connection over SSL/TLSv1 is opened to iVault Backup Servers over your existing internet connection. Your data, already pre-encrypted, is transfered over this secure connection, essentially doubling encryption. Optionally a local copy of your backup is retained on local storage.

5. **Storage:** Your encrypted data is stored unmodified on the primary iVault Backup Server in one of our data centers. Multiple versions are kept to keep history data accessible. The retention period is user selectable, from days to years if required by your business.

6. **Duplicate storage:** For optimal security and reliability, your backup is replicated to a secondary iVault Backup Server. This makes it available at multiple iVault locations, preventing a safeguard against calamities in iVault's own infrastructure.

7. **Verification and reporting:** During each backup, data is verified through checksum validation procedures. You will also receive an email notification after each backup run. In this way you will know immediately if your backup was correct instead of finding out the hard way only when you need it. You will also receive email reports of every modification made to backup settings as well as on every restauration performed. This will provide you with a secure and complete audit trail.

8. **Restoration:** De iVault Backup Client offers a historic overview of your complete file structure, from today to many months or even years in the past. From this history you select the desired day and file selection for restauration. The backup client will then retrieve the required files from the backup server, all still encrypted. As a final step local decryption, and incremental file merge will reconstruct the required file tree at the user's system.

iVault Online Backup Specifications

Functional specifications

- Multiple backup schemas per backup set. Time based or continuous with adjustable running time.
- Automatic zero-knowledge on-premise encryption.
- All files always fully encrypted off-premise, including on backup servers.
- Incremental and differential backup strategy only sends new and modified files.
- In-File Delta technology only sends modified blocks inside files. Essential for fast backup of large, frequently mutating files like Exchange, databases and virtual machine snapshots.
- Support for full and transaction log backup modes of MS SQL Server 7.0/2000/2005/2008 R2/2012, MS Exchange Server 2000/2003/2010/2013, Oracle v8i and later, MySQL, Lotus Domino/Notes 5.0
- Support for additional Microsoft Exchange features like individual mailbox level backup and Exchange 2010/2013 DAG (Data Availability Group) backup
- Support for virtual machine backup on VMware ESX/ESXi/Server en Microsoft Hyper-V Server.
- Extensive backup reporting via e-mail with detailed reports on new, modified and deleted files and backup status after each backup.
- Secure access to all backup data via standard Internet Browser.
- Extensive reporting of all settings modifications as well as restorations executed providing a full audit trail.
- Backup verification before storage by means of checksum validation with CRC (Cyclic Redundancy Check).
- Retention of previous and deleted file versions. Adjustable up to 999 days. Full restauration of removed files possible with daily granularity.
- Exclusive and inclusive file selection filters.
- Pre- and post commands.
- Supported operating systems: Windows (all major versions), Mac OS X, Linux, Unix, FreeBSD, Netware.
- Automatic update via LiveUpdate.

Security specificaties

- Secure point to point Secure Socket Layer (SSL / TLSv1) communication between backup client and server.
- Support for HTTP/HTTPS Proxy and Socks v4/v5 firewall.
- Maximum strength / default encryption mode: 256 bit Advanced Encryption Standard in Cypher Block Chaining mode (AES 256 CBC mode) / TwoFish 256 bit ECB.
- Supported encryption algorithms: AES, Twofish and Triple DES. Supported encryption modes: Electronic Cook Book (ECB) and Cipher Block Chaining (CBC).
- Zero-knowledge architecture. Encryption key not stored or known anywhere off-premise.
- Automatic generation of random initialization vector, salt and iteration counter for each file during encryption.
- Extensive reporting of all settings modifications as well as restorations executed providing a full audit trail.
- Backup verification before storage by means of checksum validation with CRC (Cyclic Redundancy Check).
- Online access limitation by predefined IP filtering.
- Redundant storage on multiple iVault Backup Servers in secure Dutch data centers.
- Storage architecture: Multiple redundant file systems utilizing Solaris ZFS storage pools. Dynamic tracing for complete storage stack verification.

System requirements

Operating systems	iVault Online Backup voor Windows: • Windows Server 2000/2003/2008/2012 • Windows XP/Vista/7/8 iVault Online Backup other versions: • Mac OS X 10.6, 10.8, 10.9 • Linux, Kernel version 2.2 or later • Solaris version 2.x or later • FreeBSD • NetWare vanaf versie 5.1
Internal memory	• 128 MB minimal, 256 MB recommended
HD storage	• 100 MB
Network protocol	• TCP/IP (HTTP/HTTPS)

From Backup to Business Continuity

Your company grows and so does the size and complexity of your IT infrastructure. You collect more data, more systems and you will inevitably start to experience the need for better data management. Your ever growing group of stakeholders requires a solid business continuity policy. What to do?

It is good to know that iVault solutions will continue to grow with you. From **backup** via **disaster recovery** to complete **business continuity solutions**.

iVault is your partner in development of a pragmatic but solid **Business Continuity Plan** with accompanying organization and fallback infrastructure. We do fully realize that business continuity requires a process of awakening and must become an embedded **mindset** in your company. Our approach therefore entails stepwise but simultaneous realization of both technical and organizational aspects, allowing you to achieve and retain the required level of protection, quickly and affordably.

If you represent a larger organization, opting for a formal approach to your business continuity requirements, iVault can also assist you with following aspects of business continuity planning, in line with industry best practices and relevant ISO/IEC and BS standards:

Business Impact Analysis (BIA): The separation of critical and non-critical functions in your organization and determination of the recovery time- and point objectives (RTO & RPO) and recovery requirements (RR).

Threats- and Risks Analysis (TRA): Analysis and documenting of threats and risks to your organization as well as their impact on it's critical functions.

Recovery Strategy and Business Continuity Plan (RSD/BCP): Drafting of recovery scenarios, composition of recovery teams, planning or fallback locations and systems as well as manual workarounds.

Testing, Training & Excercises (TT&E): Regular testing of and training in scenarios as documented in the Business Continuity Plan (BCP), including Technical Swing Tests and recovery exercises at various levels (table top, medium and complex) .