EVault®
A Seagate Company

Datasheet

EVault Endpoint Protection— All the Details: Enterprise Management, Backup and Recovery, and Security

Key Benefits: Overall

- Empower IT with mobile data oversight enabled through central policy controls
- Lock down endpoint data using advanced security features
- Ensure reliable, worry-free remote data backup
- Maximize user productivity; includes self-service recovery
- Customize your hosting environment
  - — EVault/Azure Cloud
  - — EVault Partner Cloud
  - — Your own onsite vault or cloud
  - — Onsite/offsite hybrid
  - — ROBO with local storage

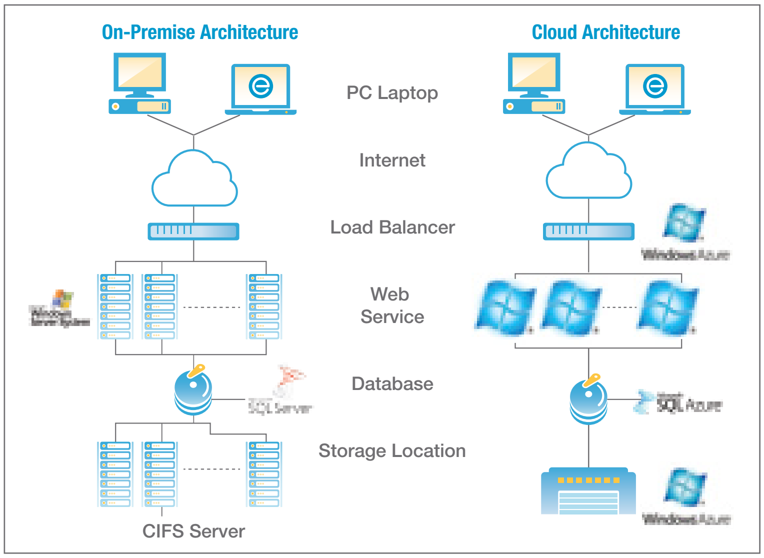
Microsoft Partner
Gold Independent Software Vendor (ISV)
Gold Business Intelligence

Windows Azure

Control mobile data with all-in-one laptop backup, recovery, and data security solution.

EVault® Endpoint Protection offers all-in-one backup, recovery, and data security to help you control data across your enterprisewide mobile workforce. With automated backup to the EVault cloud—or to your own hosted site—granular policy management, and advanced security features, EVault Endpoint Protection makes mobile data protection easy and safe for IT and end users.

In addition to advanced endpoint backup technology, EVault Endpoint Protection offers a full range of integrated policies that can be centrally managed as well as customized for multi-layered offices. Its security suite is designed to minimize data leakage and other risks associated with mobile devices. The solution is easy to implement and deploy, and backed by EVault support that can provide everything from risk assessments and migration help to disaster recovery.



The entire EVault Endpoint Protection application—including storage, databases and application services—can be scaled and deployed either onsite or in the cloud, or as a hybrid of both.

Hosting options include the EVault cloud hosted on the Microsoft Azure infrastructure and managed by the EVault team of experts. These highly resilient, SSAE 16-compliant, and ISO-certified data centers provide geo-redundant storage with a 99.9-percent uptime. Other hosting options include onsite-only or hybrid deployments. Local storage devices can be integrated to increase data transfer flexibility, reduce bandwidth costs, speed time to protection, and ensure faster local recovery.

Key Benefits: Enterprise Management

- Ensure users follow best practices with centralized, customizable policy management
- Achieve a lower TCO with a single all-in-one backup, recovery, and data security solution
- Meet compliance requirements with real-time auditing and reporting functionality
- Optimize network performance and minimize costs through local storage device integration

EVault Endpoint Protection—Global Enterprise Management Efficiencies

Control endpoint data with greater oversight and less overhead.
Control a full range of integrated policies, from a single agent, with a centralized management console that addresses multiple layers of organizations and user groups—that makes it easy on your staff. Global deduplication backs up data blocks only once—that makes it easy on your network. And cloud deployment makes it easy on your infrastructure. The result? Better use of corporate resources and improved management capabilities.

Manage Policy Centrally—Choose from best-practice, out-of-the box policies, or create your own custom policies. Either way, you can maintain oversight of endpoint data, system behaviors, and configuration parameters from one easy-to-manage, central console. Control, configure, report, and audit by user group, user ID, device, or role. Then use the web-based dashboard to manage all backup, recovery, and security policies—including bandwidth throttling, transmission times, the sharing of deduplication pool proxies, encryption, port access controls, e-mail sharing, and remote data deletion. All policies can be delegated to authorized users.

Optimize Performance—Global deduplication ensures that each data block is backed up only once even if the same file resides on multiple PCs. This minimizes bandwidth usage, shrinks backup windows, and reduces your storage footprint. Recoveries are quicker, too, because you restore only changed blocks, not whole files.

Meet Regulatory Compliance—Simplify regulatory reporting and promptly locate security breaches. You'll always be consistent with domestic and global regulations, as well as fully prepared for audits.

Pick Your Deployment Option—Choose from silent, staged rollouts or custom deployments, in bulk or in single configurations. Choose the scalable hosting environment that's right for you: onsite, in one of our partner's clouds, or in the EVault/Azure cloud.

Enjoy Self-Service Automation—Maximize your resources with automated self-service recovery and on-demand search and retrieval via any browser, including Apple iOS, Android, and Windows 8 mobile devices.

Take Advantage of Cloud Architecture—Achieve cost savings and additional protection by utilizing the enhanced performance and scalability of the cloud.

Maximize Local Efficiencies—Integrate local storage devices to enable access to networks only during "off peak" hours, cutting costs when transferring data to central vault.

Lower Your TCO—Create and implement a single backup and security strategy across many solutions: set policy by user groups, accelerate implementation of cloud-connected™ backup and security, and reduce deployment, implementation, and training costs.

Get World-Class Support—Whether you choose to store your data in your own facility, in a partner cloud, or in the EVault/Azure Cloud, our world-class team will support you every step of the way. You can also work with an EVault-authorized managed services provider.

EVault Endpoint Protection: Key Enterprise Management Features

Feature	Details
Multi-layered policy controls	Automate policies to accommodate regional, national, and global organizations; manage multiple policies through one central dashboard
Flexible, automated deployment	Deploy endpoint agents via web-based dashboard
User delegation	Control policies centrally or delegate to end users
Multiple device support	Assign multiple devices and configurations to users
Scalability	Never be constrained by seating or capacity limits
Backup and retentions	Set customizable, flexible retention frequencies according to user and user groups
Flexible hosting	In the EVault/Azure cloud, a partner cloud, onsite, or in a cloud-connected™ hybrid deployment
Expert support	A single point of contact for all your training and support needs; 99-percent customer satisfaction ratings year over year
On-demand support	8:00 a.m.–6:00 p.m. across all U.S. time zones; 24x7x365 emergency support
Corporate branding	EVault Endpoint Protection is available as a custom-branded solution
Public hosting	US and Europe; Patriot Act and EMEA-compliant; multi-tenant platform support for partners

EVault Endpoint Protection—Advanced Backup and Recovery Technology

Safeguard your company's endpoint data with reliable, worry-free backup and recovery.

EVault Endpoint Protection enables you to control a full range of integrated policies all from a single agent; a central console lets you manage multiple organizational layers and user groups. Configure retention frequencies with up-to-the-minute backups, flexible retention versions, and configurable bandwidth controls, either managed by you or delegated to specific users or user groups. Backup data is automatically transferred through optimized processes: bandwidth throttled, compressed, encrypted, and globally deduplicated before going offsite. Advanced security features enable you to wipe and control remote mobile data.

With a global, remote workforce, you need to ensure reliable, smart backups and rapid data recovery while optimizing storage and bandwidth consumption. We help EVault customers recover everything from lost files to downed systems 15,000+ times each month, so you can count on our expertise to help you implement best-practice solutions. Because EVault Endpoint Protection is simple and seamless for the user—it includes quick, self-service recoveries from any browser, without Help Desk support—you can focus on setting policy, not monitoring user compliance. A successful rollout and widespread adoption are virtually ensured.

Key Benefits: Backup and Recovery

- Ensure business continuity with continuous data protection
- Use rules-based, customizable policies to centrally manage the frequency of backup and recovery as well as retention policies for global and remote offices
- Shrink data storage footprints, bandwidth consumption, and backup windows with global deduplication and data compression
- Speed time to protection and recovery with local (LAN-based) storage integration
- Meet even the most demanding RTOs and RPOs
- Enable users to independently search, retrieve, and restore data through any browser

EVault Endpoint Protection: Key Backup and Recovery Features

Feature	Details
IT Department	
Block-level, incremental backups; global deduplication across all users; compression	Use up to 50 percent less bandwidth, get shorter backup windows
Bandwidth throttling	Set and optimize bandwidth and maximize performance
Retention versions/days	Unlimited retention versions are policy-driven and fully customizable; to 180 days in Azure
Comprehensive, fast, flexible restore capabilities	Restore data to any laptop or via any browser
Continuous data protection	Ensure business continuity with up-to-the minute backup frequencies
Geo-redundant replication to second data center	EVault SaaS provides redundancies in Azure Cloud
Local storage cache	Optional integrated local caches for reduced backup and recovery times
Storage capacity notifications	Limit your usage or set additional capacity
Customized error reports	Get notification of backup failures
User	
Non-disruptive, automated backups	No pop-ups, no performance impact, no extra authentication needed
On- and off-line protection in local cache	Backup to local cache provides protection and restore capabilities, even if the device is off-line (uploads cache when device is reconnected); alerts notify you of capacity thresholds
Simple recovery only two clicks away	Select Restore, the Date (to recover from), and Destination (where to save the file)
Fast recovery (measured in seconds)	Restores recently used files from local cache, then from the vault
Device protection	Protects data on multiple personal and corporate devices per user
User-Specific Access, Search, and Retrieval	
Browser-based file retrieval	Accessible from any browser through corporate web portal
Flexible search parameters for file retrieval	Search by date or filename
Mobile-optimized file retrieval	Android, Apple iOS, Windows
Automated, policy-controlled email sharing	Share documents fast with authorized users

EVault®
The best case for
the worst case.™

Key Benefits: Security

- Safeguard data with military-grade 256-bit AES encryption at rest and in transit
- Ensure secure access through policy-managed port access controls
- Wipe PCs clean using remote data deletion
- Track lost or stolen PCs with TCP/IP device tracing
- Get secure cloud storage with Tier 4 data center security

EVault®
The best case for the worst case.™

EVault Endpoint Protection—Advanced Security Features

Lock down your company's endpoint data, no matter where it resides.

If your organization has ever suffered a lost or stolen PC, you understand the liabilities that come with data breach: the damage it can cause your company's reputation and productivity, and the costly fines and legal expenses that can follow, particularly in regulated industries. With its advanced security technologies, a policy engine for managing access across mobile workforces globally, and powerful visibility and audit controls, EVault Endpoint Protection helps you rest easy—even when your data seems out of reach.

Policy Definitions

Security policies—Define which files to protect with backup, at-rest encryption, and proactive data deletion (by file type or directory structure). Also define the amount of storage each user will be permitted and how often, and under what schedule, files will be backed up.

Proactive data deletion and tracing policies—Define whether protected files on a lost or stolen device can be "wiped" or traced, as well as the length of time after which a device will be wiped if it has not connected to the server.

Encryption

End to end—Data is always encrypted: at rest, in transit, even during deduplication. And it never needs to be decrypted.

Military grade—Data is protected with the highest level of encryption: 256-bit AES, 128-bit SSL.

Encryption keys—A patented system encrypts public and private device keys multiple times and stores them in the vault and on the device for extra security.

File- and folder-level encryption—Data encrypts as it is stored on the device, and decrypts when the device opens an application, optimizing mobile performance. Because all data is encrypted on individual hard drives—as well as on the server—data is not accessible if a PC falls into the wrong hands.

Windows Encrypting File System (EFS)—On Windows systems, data is protected by FIPS 140-2 encryption.

Additional Security Features

Port access controls—Manage individual ports, grant read or write access, or lock down ports completely. Security alerts notify you of tampering, while audit trails provide you with the information you need to maintain control.

Remote data deletion*—Wipe lost or stolen mobile devices and laptops clean by permanently "shredding" the data, either on-demand or via time- or policy-based triggers. Your productivity won't take a hit since a full, current backup copy can be recovered easily onto a new device, and users can safely access protected files from any browser.

TCP/IP device tracing*—Track down missing PCs by IP address from the moment they communicate with your backup server. Device tracing effectively deters internal theft and enables law enforcement to detect missing devices as soon as they come online.

Secure EVault cloud hosted in Azure™—Leverage the Microsoft Windows Azure cloud for worldwide accessibility and Tier 4 security.

Controlled access and sharing—A policy module enables administrators to manage document access at the device and user levels, and specify who may email whom by domain.

Operating Systems

- Windows Vista, XP, 7, 8
- Mac OS (Mac OS encryption)

Mobile Access Platforms

- Android, Apple iOS, Windows 8

Languages Supported

- English, French, German and Spanish

Minimum System Requirements

- CPU: Pentium III 1 GHz
- Memory: 1 GB RAM
- Disk space: 1 GB free

Microsoft Azure Certifications and Attestations

Secure, geo-redundant, Tier 4 data centers

- ISO/IEC 27001:2005
- SSAE 16/ISAE 3402
- HIPAA/HITECH
- PCI data security standard
- FISMA
- Various state, federal, and international privacy laws including 95/46/EC (EU data protection directive) and CA SB1386

EVault Endpoint Protection: Key Security Features

Feature	Details
Encryption	256-bit AES, 128-bit SSL
Windows Encryption File System (EFS)	FIPS 140-2 encryption on Windows systems
In-transit encryption	No decryption risks
File- and folder-level encryption	Optimized for mobile performance
Full-disk encryption compatible	Easily layers onto existing whole disk encryption
Multiple encryption keys	
No decryption required on the back end	Eases the burden on back end servers
Global deduplication and encryption	Encrypted data is deduplicated for efficiency and security
No server side decryption	
Domain-controlled email sharing	Determine which email domains are user-authorized
Full machine performance in FIPS mode	No impact to user productivity
Port access controls	Grant read/write access or lock down completely
Remote data deletion	On-demand or via time- or policy-based triggers
Device tracing by TCP/IP address	Deter theft and quickly detect missing devices
Mobile device access control	By user and device
Automatic file deletion	Triggered by password hacking or cold boot attacks
Tampering alerts	Automated alerts triggered by unauthorized port tampering
Tier 4 data centers	SSAE 16/ISAE 3402, HIPAA/HITECH, PCI Data Security Standards, FISMA and ISO/IEC 27001:2005 and 95/46/EC (EU Data Protection Directive) and California SB1386 security standards

Take the Next Step

To learn more about EVault backup and recovery services, call us at 1.877.901.DATA (3282), email us at concierge@evault.com, or visit us at www.evault.com.

For a free 30-day EVault Endpoint Protection trial, visit: www.evault.com/EEP-free-trial.

EVault®
Endpoint Protection