

EVault Endpoint Data Protection—Summary

Data Sheet

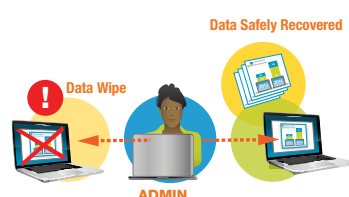
Key Benefits

- **Business visibility and control:** Instantly retrieve and wipe remote data for employee turnover and lost devices.
- **User productivity:** Context-aware, incremental backups adapt to user activity and network connections; run in the background; and protect users, whether they're online or offline.
- **Data protection efficiency:** Location-aware backups with optional onsite caches minimize the impact on bandwidth and provide continuous protection regardless of cloud connectivity.
- **Legal Hold compliance:** Once a litigation notice has been received, administrators can place relevant devices on Legal Hold without notifying or impacting employees.

Laptop backup and recovery for data availability and data loss prevention.

Employees are spending more of their work hours outside the office, and they are frequently on the go. This diminishes corporate visibility into laptop data, makes productivity increasingly dependent on varying mobile network connections, and increases the threat of data loss. EVault® Endpoint Data Protection from Seagate® is the only cloud-based backup-and-recovery solution for laptops that continuously and efficiently protects data and prevents data loss regardless of network connectivity. It can also retrieve and remotely wipe laptop data, simplifying your IT department's handling of lost devices and employee turnover. Users stay productive and protected, and organizations gain complete visibility and control.

Simplify Data Recovery During Employee Turnover



Administrator suspends the device, recovers applicable files, and wipes data remotely—all within minutes. EVault Endpoint Data Protection automatically retains data so you can recover it quickly and efficiently when employees leave your company, and you can remotely wipe data to prevent its loss. Why box up equipment and wait

for devices to be returned when you can recover the data and make it available to management immediately? And don't worry about ex-employees sharing confidential information; simply activate an on-demand or time-triggered data wipe.

Protect User Productivity with Silent Installs and Context-Aware Backups

On-the go workers get continuous, efficient data protection regardless of network connectivity.

Don't unnecessarily interfere with remote workers or slow them down with forced backups. EVault Endpoint Data Protection backs up silently, even when users are offline. Silent installs, multiple bandwidth and policy controls, and context-aware backups that automatically halt and resume in response to network availability enable users to stay productive and help IT meet the tightest recovery point and retention objectives.



Microsoft Partner
Gold Application Development

Microsoft Azure



EVault Endpoint Data Protection—Summary

Comply with Legal Hold Requirements



Once a litigation notice has been received, administrators can place relevant devices on Legal Hold. This ensures that all data backed up by these devices in the past, present and future remains in the EVault vault indefinitely. Users are not notified that their device is on Legal Hold and they are not able to delete any of their data from the vault.

Use Local Caches to Accelerate Backup and Recovery, Increase Efficiency

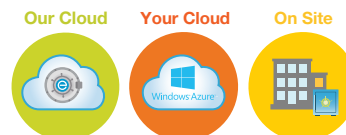
Backups and recoveries are routed over the LAN to local storage and then uploaded to the cloud during off-peak times. EVault Endpoint Data Protection easily accommodates local network storage caches to dramatically reduce your organization's time to protection—implementation time is cut from days to hours—and to speed backup and recovery, often by more than 50 percent. Back up to the LAN and set optimal transmission times over the WAN so that network impact and bandwidth costs go down as well. Easily upgrade user laptops.



EVault Endpoint Data Protection: Key Features

Gain Business Visibility and Control	• Instant remote data retrieval and wipe simplifies the handling of lost devices and employee turnover. • Complete data separation with per-device encryption keys keeps individual and group information separate and confidential. • Batch process restores can be made to file servers, local hard drives, or network-attached storage (NAS) locations. • Data is never decrypted or exposed, even during deduplication.
Enhance User Productivity	• Context-aware, incremental backups adapt to user activity and the network connection (when mobile network connection detected, WAN backups halt but on-device backups continue until standard connection is made). • Silent, automated mass deployment minimizes impact. • On-device cache provides instant access to backup data even when users are offline.
Protect Endpoint Data Reliably and Efficiently with Optional Onsite Caches	• Back up to nearest network cache or the cloud with location-aware employee devices. • Back up and restore data at LAN speed. • Shorten initial backup from days to just hours. • Schedule data uploads to minimize costs and bandwidth limitations.

* Formerly named Windows Azure



Choose the Deployment Option That Works Best for You

Deploy EVault Endpoint Data Protection one of three ways:

In the EVault managed cloud, as SaaS—for any size customer; in your own instance of Microsoft® Azure*—for enterprise-size customers; or on your site, as software—for partners and enterprises requiring multitenancy.

Take the Next Step

To learn more about Seagate hybrid cloud solutions, visit www.seagate.com/cloud-backup.

seagate.com

AMERICAS
ASIA/PACIFIC
EUROPE, MIDDLE EAST AND AFRICA

Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, United States, 408-658-1000
Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
Seagate Technology SAS 16-18, rue du Dôme, 92100 Boulogne-Billancourt, France, 33 1-4186 10 00