druva

White Paper

8 Must-Have Features for Endpoint Backup

Ensure corporate data is secure and protected by choosing an endpoint backup solution with these eight essential features.

druva

White Paper

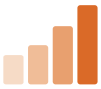
More than 80% of data is duplicated across users.

1. Advanced deduplication

Because more than 80% of data is duplicated across users,[1] choose a solution that compares data across all users in the enterprise (global deduplication) to minimize storage and bandwidth requirements for backup. In addition, checking for duplicate data on the endpoint (client-side deduplication) ensures duplicate data is never transferred to the server, saving large amounts of bandwidth and resulting in faster and smoother backups. Reap additional savings with a solution that understands the on-disk formats of various applications and does not back up duplicate data within files (application-aware deduplication).

2. WAN optimization

Approximately 200 million employees work remotely,[2] which means looking for a solution that guarantees successful and non-intrusive backups on a variety of networks. WAN optimization ensures that backups are fast and effective, even over weak networks, by optimizing packet size based on network noise and latency and using parallel connections. Backups that are interrupted over weak networks resume automatically without interrupting the user, saving user time and productivity.



Smart percentage-based bandwidth caps effectively back up data on networks of varying quality.

3. Resource throttling

Ensure backups are successfully executed in the background without interrupting the user by choosing a solution with resource throttling. If backup processes slow down an employee's computer, he will cancel the backup, leaving his data unsecure.

Adapt backup processes to available bandwidth with smart percentage-based bandwidth caps that effectively back up data on WAN or LAN networks of varying quality. CPU throttling should also be offered to ensure that backups do not interfere with users' high-priority applications by giving them precedence over backup processes.

1. Microsoft Report – "SIS and its effects at Microsoft"
2. Gartner Report #160375–Options for PC Data Backup

Two-factor encryption key management prevents even the solution provider from accessing corporate data.

4. Enterprise-grade security

With 70 million mobile devices lost or stolen each year,[3] enterprise-grade security is imperative to protect critical corporate data on employee devices. Prevent unauthorized access by looking for solutions that encrypt data in transit, on the server, and on the endpoint device. Look for solutions that offer remote wipe and geo-location, allowing the location of a device to be pinpointed and corporate data to be removed.

If considering cloud backup solutions, look for two-factor encryption mechanisms that prevent even the solution-provider from accessing corporate data on the servers. Make sure that cloud backup uses certified cloud infrastructure such as ISAE 3000 and SAS 70.

5. User self-service

Anytime, anywhere access and self-restore via client, web, and/or mobile reduce IT support time and resources. For instance, if an employee loses his laptop on a business trip, he can access his documents on another device such as a smartphone or self-restore his data to a new machine and minimize lost productivity.

6. Centralized management

Choose a product with centralized management to deploy globally without user involvement. A unified console enables easy policy management and reporting for IT administrators. Even as a company scales, management continues through one centralized interface, so adding and managing new users is easy.

3. http://www.readwriteweb.com/mobile/2012/02/infographic-the-cost-of-stolen.php

Manage commingling of corporate and personal data with BYOD backup policies.

7. BYOD enablement

More than 70% of all smartphone-owning professionals use their personal devices to access corporate data,[4] so choosing a solution that helps manage commingling of corporate and personal data with BYOD backup policies is critical. Administrators should be able to configure which folders are to be backed up, as well as the frequency of backups, and define which mobile resources are to be used (e.g., data connection if WiFi is unavailable) so users continue to retain privacy and productivity without compromising protection of corporate data.

Features like remote wipe as mentioned in #4 are useful in the situation where an employee leaves the company, so that IT administrators can remove corporate data from the employee's personal devices. Additional BYOD enablement features should include file sync and sharing, mobile apps for various platforms, and web browser access.

8. Settings backup

Make replacing a user's hardware or migrating to a new OS much simpler by looking for solutions that layer backup of a user's data along with his personal settings. Being able to restore a user's personal settings and data regardless of device model and operating system saves a lot of time for administrators. End users benefit because they can continue working in a familiar work environment without spending time reconfiguring personal settings.

Choosing an endpoint backup solution that includes the eight features above will ensure full data protection, maximize user productivity, and reduce time and maintenance for IT administrators. Be confident that your endpoint backup solution is the right choice.

4. http://www.eweek.com/mobile/byod-programs-pose-security-risk-for-businesses-ovum/

About Druva

Druva provides integrated data protection and governance solutions for enterprise laptops, PCs, smartphones and tablets. Its flagship product, inSync, empowers an enterprise's mobile workforce and IT teams with backup, IT-managed file sharing, data loss prevention and rich analytics. Deployed in public or private cloud scenarios or on-premise, inSync is the only solution built with both IT needs and end user experiences in mind. With offices in the U.S., India and U.K., Druva is privately held and is backed by Nexus Venture Partners, Sequoia Capital and Tenaya Capital. For more information, visit **www.Druva.com.**

druva

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44.(0)20.3150.1722
APJ: +919886120215
sales@druva.com
www.druva.com