COMMVAULT®

Endpoint Data Protection: A Buyer's Checklist

ENDPOINT DATA. It's often one of the most forgotten aspects of an enterprise data protection strategy. Yet, content on laptops, desktops and mobile devices is among a company's most valuable data even while it's potentially at the greatest risk. According to IDC there will be some 1.3 billion mobile workers by 2015.[1] However, only half of enterprises today are using some type of endpoint backup.[2] That means that the volume of endpoint data that is in jeopardy is nothing short of significant.

Selecting the best endpoint data protection solution for your environment requires careful evaluation of the goals you are looking to achieve – both for your IT operations and user productivity.

1 Worldwide Mobile Worker Population 2011 – 2015 Forecast, IDC
2 Market Overview: Enterprise Endpoint Backup and Recovery Solutions, Forrester Research

With an increasingly mobile workforce creating more critical information outside IT's traditional domain, mounting demands for anywhere, anytime access to information and the potential cost and risk of compliance and eDiscovery requirements, the need for endpoint data protection is clear and at a dangerous tipping point. Why?

Because, compounding these drivers is the increasing fear of security as workers turn to unsecure consumer-grade file sharing solutions to achieve their mobile data access and collaboration needs. In fact, more than four out of five IT professionals report security problems caused by consumer file sharing and sync services used for company business.[3]

To secure the roaming data assets on endpoint systems, and safeguard critical company information, organizations should implement a comprehensive endpoint data protection strategy. For optimum protection while enhancing user productivity, consider the following features in this buyer's guide.

EVALUATING YOUR REQUIREMENTS

Selecting the best endpoint data protection solution for your environment requires careful evaluation of the goals you are looking to achieve – both for your IT operations and user productivity. Consider these five requirements and how you may rank them to ensure that the endpoint data protection solution you select is aligned with your business goals.

ONE: Enhance User Productivity. Today's users desire to have anywhere, anytime and any device access to all of their personal and business data. Supporting these increasing user demands can be a costly exercise for IT helpdesks. To free your users to work the way they want without costly support impact, select a modern endpoint data protection solution that will offer users self-service capabilities for their business data, without taxing the helpdesk. Capabilities may range from the ability for self-service access and recovery to file sharing of content with internal and external colleagues and partners.

TWO: Optimize Resources. Adding endpoint backup to your enterprise shouldn't slow operational or user performance. Select a solution that offers CPU and power utilization features and bandwidth throttling to make the most of your existing infrastructure resources. For further efficiency, select a product that offers global deduplication. This can eliminate as much as 90% of redundant data.

THREE: Automate System Discovery. Today's mobile workers may use as many as three or more devices.[4] Keeping up with each of these devices can be a complex operation. To help, select an endpoint data protection solution that will auto- discover new desktops and laptops and perform an automatic installation of backup agents to guarantee protection for all PCs while minimizing administrative workloads.

FOUR: Enable Deployment Flexibility. If your organization is already leveraging the storage and infrastructure value of the public cloud, or you're planning to in the future, select an endpoint backup solution that offers you the deployment flexibility you need to implement the solution on-premises, in the cloud or a hybrid of the two.

FIVE: Simplify Administrative Processes. If minimizing administrative time and cost is a priority for your IT operation, select an endpoint data protection solution that also serves your server data protection requirements. By protecting and managing desktop, laptop and server data in a single solution you can minimize administrative burden and infrastructure complexity without the use of separate point solutions and multiple management consoles.

3 Harnessing the Tyranny of Autonomy: The Dropbox Problem and the Manager's Dilemma, GigaOm

4 Market Trends: Secure Files Sharing and Collaboration in the Enterprise Q1 2014, Forrester Research

SELECTING THE ADVANCED FEATURES YOUR ENDPOINTS NEED

Once you have prioritized the requirements your organization has for endpoint data protection, consider the key features you'll need to satisfy those requirements. Following are some of the advanced features you may want to demand from your selected solution.

INTELLIGENT SCHEDULING.

With devices on the go, it can be difficult to protect them on a regular schedule, every day. Select a solution that offers scheduling intelligence that won't impact the user. Solutions that offer this will evaluate available resources including CPU utilization, power source and network conditions while the user is connected to the internet and run or resume backup operations in the background without user intervention.

SOURCE-SIDE (CLIENT) DEDUPLICATION.

To reduce the bandwidth consumption and optimize disk space usage select an endpoint data protection solution that delivers deduplication on the source, or client. This will eliminate redundant data from the client before it is stored, transferring only unique blocks of data to storage targets, improving overall performance and lowering storage costs.

Is Your Data Secure?

Bring Your Own Device in the enterprise is here to stay, creating new data security challenges. Here are 9 data points to consider as you further develop and refine your BYOD strategy.

READ NOW

commvau.lt/1iVlH1Y

OPTIMIZED NETWORK MANAGEMENT.

To further optimize user experience, regardless of whether they are working on a high speed connection or at a public access point, select an endpoint protection solution that will flexibly throttle the amount of bandwidth consumed by backups.

DATA LOSS PREVENTION (DLP).

To add a layer of security at the file or folder level and minimize the risk of data breach or loss if a laptop is lost or stolen, select a solution that offers DLP features. The ability to encrypt at the file level, remote wipe entire systems or select data, and find systems using geo-location data can help prevent data from getting into the wrong hands.

ENCRYPTION.

As data moves around from device to data center, it can be at risk. Select an endpoint data protection solution that will encrypt data at the endpoint, in transit and in the datacenter. This client-level encryption will ensure that data is protected regardless of where it is moving or contained. Look for solutions that comply with industry and government regulations and standards such as FIPS 140-2. For the best protection, use encryption with other security features such as two-factor authentication (2FA) and role-based access controls.

ADMINISTRATIVE AUTOMATION.

To support efficient scalability while reducing administrative workloads, choose an endpoint data protection solution that offers policy and workflow customization. This will enable you to deploy multiple endpoints from a single console and will even auto-discover new desktops and laptops for the automatic installation of backup agents.

USER SELF-SERVICE.

Improve user productivity and reduce helpdesk costs with a solution that supports end-user self-service to content. The most advanced solutions that offer this feature enable users to search and restore their own backup data through a web console, Windows Explorer plug-in or even a mobile app and can find files in seconds.

MOBILE ACCESS.

For organizations with an on-the-go workforce, mobile access to protected data can dramatically improve user productivity. Advanced solutions will allow users to not only view, but also edit and protect data from mobile devices such as tablets and smartphones. In effect, an endpoint data protection's central repository can act like a personal data cloud for users that want to access their content with any of their devices.

FILE SHARING.

Users are constantly looking for easy ways to collaborate with others and increase their personal productivity. Keeping their most current content available on any device and finding ways to share information with others can be a challenge, driving them to use unauthorized consumer file sharing solutions or port files on rogue external storage devices. These workarounds are risky since IT often lacks visibility and control over the data being stored and shared. To help, select an endpoint data protection solution that enables secure file sharing with role-based permissions and the ability to facilitate collaboration between internal employees as well as with partners and customers.

SEARCH AND EDISCOVERY.

The search and discovery of information for corporate litigation, internal investigations, public information, audit and compliance requests can be costly and time consuming. If eDiscovery is an important priority for your organization, consider an endpoint data protection solution that will automatically support your search and discovery requirements. By integrating endpoints into your overall content repository, the most advanced solutions will enable you to deliver enterprise-wide search and discovery for all information. Advanced solutions will also deliver integrated legal hold, case management and workflow features to make discovery processes more efficient.

Endpoint data protection is the key to a comprehensive solution to safeguard your critical company information. If you identified many of the advanced features in this buyer's guide as important for your organization, consider evaluating Commvault software. As part of the single-platform software solution, Commvault Endpoint Data Protection technology delivers efficient, centralized endpoint data protection and management. It simplifies operations to reduce cost and risk, while increasing productivity across the enterprise through groundbreaking self-service capabilities.

To learn more about the full benefits of Commvault Endpoint Data Protection software and the importance of endpoint data protection and access, visit commvault.com/solutions/endpoint-data-protection.

COMMVAULT

PROTECT. ACCESS. COMPLY. SHARE.

COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM