CHECKLIST

Commvault

Endpoint data protection: A buyer's checklist

Endpoint data is 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 while it is potentially at the highest risk. Implementing an endpoint data protection solution provides you with the necessary tools to secure your organization's roaming data assets on endpoint systems and keep critical company information safe.

EVALUATING YOUR ENDPOINT DATA PROTECTION REQUIREMENTS

Selecting the best endpoint data protection solution for your environment requires careful evaluation of your goals—both for your IT operations and user productivity. Consider these five requirements:

#1

ENHANCE END-USER PRODUCTIVITY

Today's users desire to have access to all their personal and business anywhere, anytime, and on any device. Supporting these increasing demands can be a costly exercise for IT helpdesks. To free your users to work the way they want without relying on IT helpdesk support, select a solution that offers self-service capabilities ranging from access and recovery to content file sharing with internal and external colleagues and partners.

#2

OPTIMIZE RESOURCES

Adding endpoint data protection to your enterprise should not slow operational or user performance. CPU and power utilization features and bandwidth throttling can help maximize your existing infrastructure resources. For further efficiency, select a solution that offers global deduplication. This can eliminate as much as 90% of redundant data saving valuable storage resources and costs.

#3

AUTOMATE SYSTEM DISCOVERY

Bring your own device (BYOD) programs encompass a wide range of devices, from smartphones to laptops, and each employee requires access to different apps, connections, and services. Staying up to date with all these devices and their applications can be a complex operation. To help, select a solution that will auto-discover new endpoints and automatically install backup agents to guarantee protection for all smartphones and laptops while minimizing administrative workloads.

#4

ENABLE DEPLOYMENT FLEXIBILITY

If your organization is already leveraging the value of the public cloud, or you are planning to in the future, select an endpoint backup solution that offers deployment flexibility to implement the solution on-premises, in the cloud, hybrid cloud, or Software-as-a-Service.

#5

SIMPLIFY ADMINISTRATIVE PROCESSES

Minimizing administrative time and cost is a priority for IT operations given resource and budget constraints. Select a solution that integrates your current application and data protection requirements. Protecting and managing desktop, laptop, applications, and server data in a single solution helps minimize administrative burden and infrastructure complexity.

SELECTING THE ADVANCED FEATURES YOUR ENDPOINTS REQUIRE

Once you have identified your organization's requirements for endpoint data protection, consider the key features you will need to satisfy those requirements.

Intelligent scheduling

With devices on the go, it can be challenging to protect them on a regular schedule, every day. Ensure a consistent end-user experience with automated backup schedules based on multiple variables, such as CPU, power source, and network conditions while the user is connected to the internet, and managing data transfer speeds and bandwidth consumption.

Source-side (Client) deduplication

Reduce network bandwidth consumption and optimize corporate IT disk space usage, with source-side deduplication. This will eliminate redundant data from the client before it is stored, transferring unique data blocks to the storage target(s), improving overall performance and lowering storage costs.

Optimized network management

To further optimize user experience, whether they are working on a high-speed connection or at a public access point, select a solution that will flexibly throttle the amount of bandwidth consumed by backups and reduce the network impact during peak periods.

Data Loss Prevention (DLP)

Minimize the risk of data breach or loss if a laptop is lost or stolen. The ability to encrypt at the file level, remotely 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 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 data center. 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, enabling users to search, view, and recover their own files and folders using a web console, Windows Explorer plug-in, or even a mobile app.

File sharing

Users are always looking for easy ways to collaborate with others and increase 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 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, moved, and shared. To address this challenge, select a solution that enables secure file sharing with role-based permissions and the ability to facilitate collaboration between internal employees as well as with business 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 a priority for your organization, consider a solution that will automatically support your corporate 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. Integrated legal hold, case management, and workflow features make the discovery processes more efficient.

SECURE ENDPOINT PROTECTION WITH COMMVAULT CLOUD

If you identified many of the features in this buyer's guide as necessary for your organization, consider Commvault® Cloud Backup & Recovery. Reduce data risk, increase visibility, and improve employee data access. Commvault Cloud Backup & Recovery runs effortlessly on desktops, laptops, and more in any location, with self-service and automation tools so that files can be retrieved and recovered without IT intervention.

Learn more, visit **commvault.com/endpoint**