YOTTA SAFE | Powered by COMMVAULT

ENDPOINT DATA PROTECTION: A BUYER'S CHECKLIST

ENDPOINT DATA. It 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. To secure your organization's roaming data assets on endpoint systems, safeguard critical company information, and meet your data protection strategy, implementing an endpoint data protection solution provides you with the necessary tools. 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 maintaining user productivity. For optimum protection, consider the following features in this buyer's guide.

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 to ensure the endpoint data protection solution you select is aligned with your business goal

ENHANCE END-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 IT helpdesk support impact, select a modern endpoint data protection solution that will offer users self-service capabilities. Whether users have questions or need support for their business data or even personal data, self-service eliminates taxing the helpdesk. Self-service capabilities may range from access and recovery to content file sharing with internal and external colleagues and partners.

OPTIMIZE RESOURCES

Adding endpoint data protection to your enterprise should not 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 and save valuable storage resources and costs.

AUTOMATE SYSTEM DISCOVERY

Bring your own device (BYOD) programs encompass a wide range of devices, and each employee requires access to different apps, connections, and services. Keeping current with all devices and their applications 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 desktops and laptops while minimizing administrative workloads.

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 you the deployment flexibility you need to implement the solution on-premises, in the cloud, hybrid cloud, or Software-as-a-Service. You want a solution that will not hold you back but provides broad and deep support for the technologies of today and in the future.

SIMPLIFY ADMINISTRATIVE PROCESSES

Minimizing administrative time and cost is a priority for IT operations given limited training, staffing, and budget resources. Select an endpoint data protection solution that integrates your current application and data protection requirements. By protecting and managing desktop, laptop, applications, 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.

SELECTING THE ADVANCED FEATURES YOUR ENDPOINTS REQUIRE

Once you have identified the requirements your organization has for endpoint data protection, consider the key features you will need to satisfy those requirements. The following are several advanced features you may want from your selected solution.

Intelligent scheduling

With devices on the go, it can be challenging 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 network bandwidth consumption and optimize corporate IT 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 unique data blocks to the storage target(s), improving overall performance and lowering storage costs.

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 and reduce the network impact during peak periods.

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, 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. The most advanced solutions enable users to search and restore their backup data through a web console, Windows Explorer plug-in, or even a mobile app and can discover files in seconds.

File sharing

Users are always looking for easy ways to collaborate with others and increase their 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 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 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 an important priority for your organization, consider an endpoint data protection 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. Advanced solutions will also provide integrated legal hold, case management, and workflow features to make discovery processes more efficient.

Endpoint data protection is the key to a comprehensive data management solution to safeguard your critical company information. If you identified many of the advanced features in this buyer's guide as necessary for your organization, consider evaluating Yotta Safe powered by Commvault. As part of the single-platform software solution, Yotta Safe 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.

COMMVAULT®

About Commvault

Commvault is the recognized leader in data backup and recovery. Commvault's converged data management solution redefines what backup means for the progressive enterprise through solutions that protect, manage and use their most critical asset — their data. Commvault software, solutions and services are available from the company and through a global ecosystem of trusted partners. Commvault employs more than 2,600 highly-skilled individuals across markets worldwide, is publicly traded on NASDAQ (CVLT), and is headquartered in Tinton Falls, New Jersey in the United States. To learn more about Commvault visit www.commvault.com.