druva

White Paper

10 Common Pitfalls of Enterprise Endpoint Backup

This guide is written for IT professionals who play a role in data protection and governance within their organizations. The paper provides actionable advice for avoiding common mistakes when selecting a solution to protect enterprise endpoints.

Executive Summary

Backing up and protecting sensitive corporate data is a rising challenge for IT organizations due to several trends: the exponential growth of corporate data, the challenges of Bring Your Own Device (BYOD) – including the steady rise in number and types of endpoints – and the use of cloud-based, SaaS applications. Yet, traditional enterprise backup solutions focus on server backups designed to protect data within the firewall, not taking into account the rapid shift of corporate data to the edge of the enterprise.

Companies today are waking up to the security challenges of endpoint data governance. When considering endpoint backup solutions for an organization, it's important to address issues such as file security, bandwidth constraints and how any endpoint backup solution fits within a larger data governance strategy.

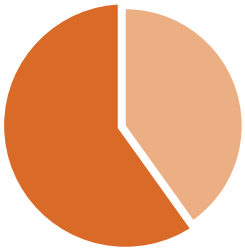
We have identified 10 common, real-world pitfalls that IT professionals need to be aware of before selecting an endpoint backup solution for their organizations.

10 Common Pitfalls of Enterprise Endpoint Backup (and How to Avoid Them)

1 Underestimating the risk of DIY backups

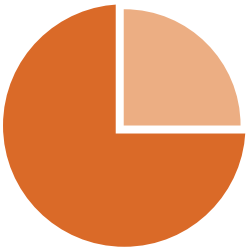
A surprising number of companies do not have a comprehensive approach to data loss in place and instead depend on employees to back up their data. In this environment, it's no surprise that individuals start to get creative in order to accomplish the goal of backing up their files as easily and quickly as possible, and will use the most convenient method available, including external hard drives, USB flash drives, CDs or DVDs, and public cloud applications.

This "do-it-yourself" (DIY) approach brings real risks, including lack of IT visibility into what is being backed up, lack of centralized control when an employee leaves the company, security vulnerabilities in the public cloud, and no way to find data when needed for legal, M&A or IP-based activities — any of which could leave your company at risk for noncompliance and permanent data loss.



40% OF BUSINESSES EXPERIENCED EXPOSURE

of confidential data due to DIY public cloud deployments



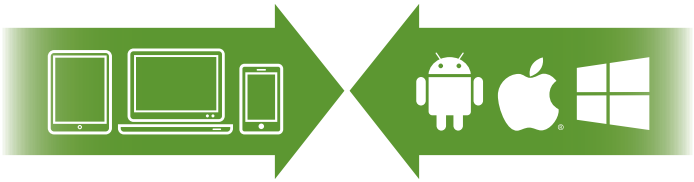
MORE THAN 25%

of businesses faced account takeover issues[1]

Even with IT ownership and oversight, a DIY backup process may not address critical areas such as optimal bandwidth utilization, synchronization of large files (PSTs, for example), and an efficient approach to data deduplication that can avoid backing up entire data sets when only small changes are made to files.

A fully managed approach to enterprise data backup can significantly reduce costs, as well as address compliance issues and ensure Service Level Agreements (SLAs) are in place to guarantee performance, redundancy and fail-safe testing.

1. Symantec Global Survey Reveals Upsurge in Rogue Clouds and Other Hidden Costs



The BYOD trend is accelerating due to the proliferation of devices utilizing multiple operating systems.

2 Underestimating the impact of BYOD

The BYOD trend is still accelerating, as evidenced by the continued proliferation of devices utilizing multiple operating systems and a seemingly endless array of new form factors. With BYOD comes a new set of requirements for backing up data on endpoints, such as heterogeneous OS backup/restore, and keeping corporate data secure in the unpredictable environment outside the company firewall, where bandwidth and worker hours can fluctuate.

25% of IT professionals are not confident that their BYOD policy is compliant with data and privacy protection acts.[2]

Source: ESG Global research

In today's mobile-first enterprise, end users demand anywhere, anytime access to data and file sharing with colleagues and external collaborators to maximize their own productivity. At the same time, IT requires that valuable intellectual property is safely encrypted over public networks while in transit and at rest, and that corporate data stored on these devices is backed up in compliance with policies and can be remotely wiped in the event of theft, loss, or termination of employment – without interfering with personal data.

It is possible to achieve both sets of organizational goals, but not with legacy backup solutions designed for traditional and predictable desktop environments. To fully address the BYOD trend within your organization, gain control of corporate data across a varied mix of devices while embracing end user productivity.

3 Considering a consumer-grade solution for your enterprise backup

It's clear that enterprise backup needs are far more complex than the needs of a home or small business, yet some companies make the mistake of choosing a backup solution designed for consumers.

Asking the right questions of your backup provider will ensure that you are meeting the level of data protection required by today's enterprise. For example, is it compliant with international standards and certifications for cloud infrastructure, operations and control? How does the solution address business continuity (DR, fail-over, data center redundancy)? Does it provide the right policy and visibility tools to manage an enterprise of mobile workers? What about regional support and services needed by a 24/7 global business? These requirements are critically important to enterprise customers, yet they may never cross a consumer's mind. Choose a solution built from the ground up for the very different — and far more rigorous — requirements of enterprise customers: data center certifications and data redundancy, industry-leading data transfer speeds across

2. ESG Report

variable bandwidths, global scalability, and true privacy to ensure secure and high-performance data protection.

Tip: Avoid trying to solve enterprise challenges with a consumer-grade backup solution that can limit your ability to scale.

4 Thinking that legacy server solutions will work for endpoint backup

While you may be tempted to use existing desktop or server backup solutions to solve your endpoint backup needs, take note: legacy server solutions make assumptions about bandwidth, latency and recovery protocols and fixed device location, which do not take endpoint backup requirements into consideration. Solutions originally designed for the highly predictive environments of server backup (secure high-bandwidth LAN, backups on a regular schedule) perform poorly when confronted with endpoint backup environments that are highly unpredictable.

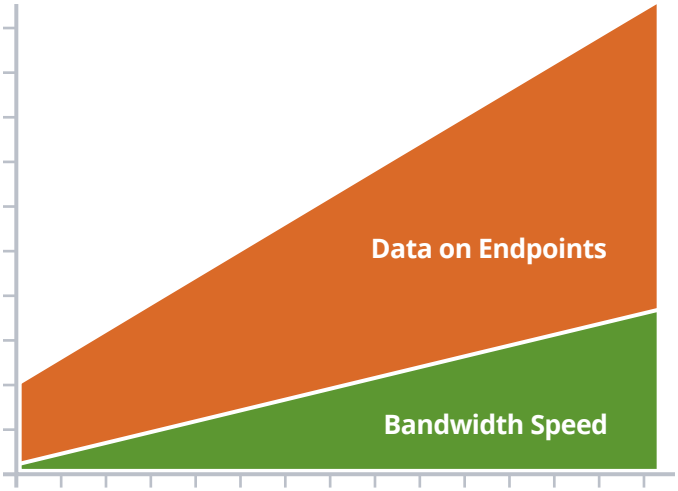
Critical features for endpoint backup — which are not available in legacy server backup solutions — include faster, non-intrusive backups, the ability to work over VPN-less networks, and flexible, opportunistic scheduling.[3] Choose an endpoint backup solution that is architected from the ground up for the mobile workforce to be lightweight, non-intrusive, and powerful enough to offer robust, enterprise-scale data protection.

Tip: Leverage the best of the cloud and mobile encryption technology when evaluating backup solutions.

5 Ignoring the impact on corporate networks

The amount of corporate data on endpoint devices is doubling every 18 months, while bandwidth speeds have only grown 10x over the last 10 years.[4] Not estimating or planning the impact of endpoint backup on your corporate network will impact your end users unless you avoid these common pitfalls:

- Not communicating the needed resources for the application to the other IT infrastructure teams
- Assuming that all users are complying with connectivity policies that could have an impact on client installation or device activation (i.e. VPN connection or logging into domain)
- Not providing adequate internal support resources or inadequately training those resources
- Not critically reviewing your global WAN footprint to plan ahead for distributed deployment



The amount of corporate data on endpoint devices is doubling every 18 months, while bandwidth speeds have only grown 10x over the last 10 years.[4]

3. Gartner: Endpoint User Data Backup Report (ID# G00211731)
4. IDC: Digital Universe report

In order to deal with this large gap between data growth, and bandwidth and computing resource limitations, look for solutions that work on the client side, are able to dedupe objects within files, and eliminate data duplication across all users within the enterprise. Up to 80% of an organization's data is redundant, so enterprise-wide deduplication can provide large bandwidth and storage savings.

6 Not making end user experience a priority

Users frequently disengage backup software when the backup process interferes with their ability to work. In fact, 51% of end users found their current backup solution to be intrusive.[5] An effective backup solution must include bandwidth and CPU throttling capabilities, efficient deduplication, and WAN optimization to provide end users with a non-intrusive experience, resulting in successful backups and protected data.

51% of end users found their current backup solution to be intrusive.

In addition, solutions that allow self-restore not only empower the end user, but also save IT support time and resources. Today, end users have the same expectations of enterprise software as they do for consumer software, so ease of use and zero impact to productivity should be priorities as you shop for an endpoint backup solution.

7 Underestimating security or compliance requirements for your enterprise

While in the past it may have been enough to leave the details of how data were stored to your storage provider, today business leaders need to be able to answer to how their customer data are being maintained, secured and protected, especially with the rise of global business and ever-evolving international data privacy laws. Having the right provider that can help you meet operational compliance by providing SOC1 and ISO-27001 certification, or industry/government specific assurances like HIPAA, ITAR or FIPS, will assure your organization's compliance.

Enterprises evaluating cloud endpoint backup solutions must be confident that their provider satisfies physical data center security requirements and has appropriate third party security certifications. Some leading endpoint backup solutions use sophisticated digital envelope encryption mechanisms that prevent even these solution providers from accessing your data on the servers. This is increasingly important for companies that do business worldwide — and who doesn't today?

8 Not planning for eDiscovery and data governance initiatives

Looking at endpoint backup as simply an efficient way to restore lost data can leave a lot on the table, especially when it comes to leveraging the technology to address trends

5. Ponemon Institute: Quantifying the Benefits of Unified Endpoint Data Management

46% of organizations view eDiscovery as a "high" or "critical" priority over the next year, up sharply from 20% and 18% in 2012 and 2011, respectively.[6]

like eDiscovery. According to Forrester, Q2 2013, 46% of organizations view eDiscovery as a "high" or "critical" priority over the next year — up sharply from 20% and 18% in 2012 and 2011, respectively.[6]

With the right endpoint backup solution in place that includes integrations with eDiscovery analysis platforms, it is possible to gain visibility of data on endpoints and respond to legal holds from your legal teams. Such an approach enables IT to quickly locate information on any device, enforce data usage policies and preserve data. This leads to tremendous cost savings for companies that need to respond to legal requests, freeing up vital IT resources from labor-intensive, costly data collection for other critical IT projects.

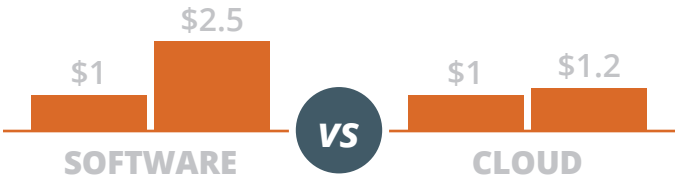
For enterprises subject to industry regulation, it's important to select a service provider that has already has passed the requisite certifications (e.g., HIPAA) for its data centers and operations.

9 Choosing the wrong deployment model and not calculating TCO

Comparing upfront costs alone when evaluating solutions could mean you pay more in the long term. Consider total cost of ownership (TCO): cost of initial setup time, hardware costs, deployment time, and cost of resources to manage the solution. For instance, a solution that has low upfront costs may require weeks of initial setup time and effort which not only increases the time-to-value but also increases TCO from the enormous amount of IT work hours required.

Also, solutions that do not support mass client deployment severely impact both IT and end user productivity, again increasing TCO. Some other features to consider are centralized policy management, automatic client upgrades, on-demand scalability, user self-restore options and optimized storage and bandwidth utilization.

The decision to go with a cloud or on-premise deployment should be based on business factors such as budget, timeline, corporate policies, and external compliance regulations. Define your deployment requirements first or you may be pigeonholed into managing a solution that does not align with your organization's IT strategy. Cloud-based solutions offer you on-demand scalability and allow shifting of capital expenses to operating expenses. On-premise solutions may provide higher performance along with cost advantages from hosting infrastructure behind your corporate firewall.



Evaluate the total cost of ownership (TCO), including costs of hardware, services and deployment time when calculating costs of on-premise cloud deployments.

6. Forrester: Forrester's Forrsights Security Survey, Q2 2013

10 Not understanding the SLAs and quality of cloud infrastructure

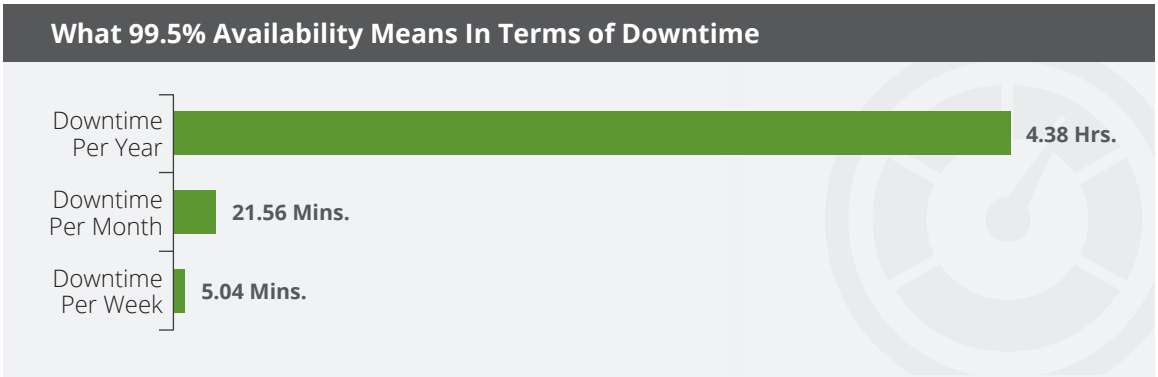
With endpoint backup, ignoring or not fully understanding service-level agreements (SLAs) can mean the difference between recovering quickly from a data loss scenario or suffering significant interruption in business. SLAs should answer: Is there a plan for redundancy in case one method fails? What happens in the event of an emergency and how fast can we recover data?

Any endpoint backup provider needs to provide SLAs to cover data availability, durability, RTO and RPO. Following are examples of some SLAs an enterprise should demand:

- *Service Availability* will define the acceptable uptime for service and access to data, which is recommended to be 99.5%.
- *Recovery Time Objective (RTO)* is the maximum amount of time taken to recover information, and should be less than 5 minutes.
- *Data Durability* sets an agreement on the loss of information, which should be no lower than 99.99999%.
- *Recovery Point Objective (RPO)* designates the granularity for data recovery, which for endpoints is recommended to be less than 10 minutes.

Why are these important? Each of these determines the level of risk and interference in business continuity, which can be significant when it comes to recovering lost sensitive data and addressing compliance issues. Understand the SLAs and quality of cloud infrastructure so that you are able to select a partner that can strengthen — not jeopardize — your security and reliability stance.

Tip: A good rule of thumb to follow for cloud architecture SLAs is that the cloud-based data protection solution has to offer a SLA greater than that being offered by the enterprise. In this way, the corporate SLA is never jeopardized by a cloud provider SLA based on weaker terms.



Source: Wikipedia

Conclusion

When it comes to choosing an enterprise endpoint solution, the biggest mistake you can make is focusing only on cost, backup process or security type. Solving for the smallest problem can only trip you up down the road when you need to scale beyond backup to other governance initiatives. By partnering with your business units and understanding end user trends, you can widen the scope of your endpoint backup initiative and solve larger business challenges – such as readiness for eDiscovery – leading to increased organizational agility.

Here's an easy checklist to use when planning your cloud-based endpoint backup strategy:

10 Steps to Endpoint Backup Success

1. Avoid the data loss risks that come with a DIY approach by solving for data redundancy and disaster recovery.
2. Look for solutions that provide end users with mobile apps to access their data, allow IT to set up profiles limiting access on BYOD devices, and play well with MDM solutions.
3. Demand enterprise-ready features such as industry-leading data transfer speed, across variable bandwidths, global scalability, and true privacy to ensure high-performance data protection.
4. Understand ways that legacy server backup solutions are not designed to protect data on endpoints.
5. Plan for the impact on your corporate network by optimizing dedupe speeds.
6. Make end user experience a top priority; strive for zero impact on productivity.
7. Be aware of and plan for the increasing security or compliance requirements for your enterprise.
8. Choose solutions that integrate features such as eDiscovery enablement, legal hold and federated search, which provide significant savings on cost, time, and effort involved in endpoint data protection and management.
9. Consider TCO: the total cost of initial setup time, hardware costs, deployment time, and cost of resources to manage the solution.
10. Understand the SLAs and quality of cloud infrastructure, and pick a partner that can strengthen — not jeopardize — your security and reliability stance.

About Druva

Druva is the leader in converged data protection, bringing data-center class availability and governance to the mobile and distributed enterprise. With a single dashboard for backup, availability and governance, Druva's award-winning solutions minimize network impact and are transparent to users. As the industry's fastest growing data protection provider, Druva is trusted by over 3,000 global organizations on over 3 million devices. Learn more at **www.druva.com** and join the conversation at **twitter.com/druvainc**.

More Resources

Visit Druva.com/resources for additional resources for learning more about endpoint backup.

- 5 Critical Considerations for Cloud Backup
- The Essential Security Checklist for Enterprise Endpoint Backup
- Request a Trial

For more resources, visit druva.com/resources.

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

Q416-CON-10567