druva

White paper

10 common pitfalls of enterprise endpoint backup

Q121-20131

Introduction

Backing up and protecting sensitive corporate data is a rising challenge for IT organizations due to several trends. Here are just a few that are top-of-mind for today's businesses:

- Growth of remote workforces worldwide
- Elevation of data risks associated with employee departures
- Rise of ransomware and the need for a stronger defense
- Increase in compliance requirements
- Security obstacles of endpoint data governance

As these changes take place in the corporate environment, it's important to recognize that your endpoint backup solution might not be fit to solve for the challenges of today and what's to come. Traditional enterprise backup solutions mainly focus on server backups that are designed to protect data within the firewall — but these legacy approaches have limits. Organizations must adopt a modern endpoint backup approach in order to sustain the growth of enterprise data and adapt to current trends.

To help you and your organization, we've identified ten common, real-world pitfalls of endpoint backup — and how the right endpoint backup solution can help.

1) Underestimating risks of employee departures

When employees leave your organization, does business-critical data leave with them? Do you know if critical or sensitive data has been deleted or tampered with? What about important data left on the devices of your remote workers dispersed around the world? Once remote workers leave the organization, do you have control over data stored on their laptops and mobile devices?

It is not uncommon that departing employees may delete, hide, or tamper with important data.

It is not uncommon that departing employees may delete, hide, or tamper with important data. In many cases, the risks of employee departures are often overlooked, especially for remote working instances. As it turns out, these corrupt activities could have started months prior to departure — and without a proper backup solution, there is no way to provide comprehensive data protection or conduct thorough data investigations.

With proper endpoint backup in place, you can:

- Backup files frequently (a comprehensive backup solution will back up data as often as every few minutes).
- Accomplish large-scale device refreshes and OS migrations across endpoint devices.
- Gain complete data loss prevention (i.e. data encryption on endpoint devices, geo-tracking of devices, remote wipe on laptops and mobile devices, and restore of user data, preferences, and system settings).

2) Overlooking data protection best practices for remote workforces

Due to unforeseen situations and challenges like the 2020 pandemic, organizations world-wide are shifting to a remote workforce. More employees are working from home and using new platforms without understanding remote working best practices around data protection. Data is also being dispersed across multiple geographies and locations, and companies are struggling to protect business-sensitive data, specifically across endpoints like laptops and mobile devices.

The right endpoint backup solution protects and secures data no matter where it goes.

Employees can accidentally download ransomware on their laptops and unknowingly infect the entire organization (chances are higher for remote employees due distractions within their personal working environment). Employees can also accidentally expose confidential enterprise or customer data. In addition, if an employee's device is lost, stolen or becomes damaged, your organization needs a way to recover the data while keeping productivity on the move.

As your organization switches to remote working, it's important to stick to the data protection best practices and empower your organization with an endpoint backup solution. The right endpoint backup solution protects and secures data no matter where it goes, even if your employees are working from home and in different locations around the globe.

3) Miscalculating the impact of ransomware

Ransomware attacks are getting more sophisticated by the minute, and endpoints are particularly at risk, with hackers constantly employing new social engineering strategies and turning this form of intrusion into its own mature industry.

> It's important to start thinking about incorporating ransomware recovery into your endpoint backup strategy.

Damage costs from ransomware continue to skyrocket and many organizations underestimate this massive impact. According to CyberSecurity Ventures, global damage costs from ransomware are estimated to be more than $20 billion in 2021, up from $11.5 billion in 2019. By the end of 2021, they expect there to be a ransomware attack every 11 seconds, up from every 14 seconds in 2019. [1]

Ransomware now affects all organizations and industries — including all of your employee devices (across multiple locations) that are left vulnerable without proper endpoint backup. To fully prepare for ransomware, it's important to start thinking about incorporating ransomware recovery into your endpoint backup strategy. By selecting the right endpoint backup solution, you can ensure that your organization has a solid defense plan in place to reduce the impact of ransomware for a variety of endpoints.

4) Misunderstanding the risk of DIY backups

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

This "do-it-yourself" (DIY) approach brings real risks. IT lacks visibility into what is being backed up, there's less centralized control when an employee leaves the company, and it's much harder 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.

Even with IT ownership and oversight, a DIY backup process may not address critical areas such as optimal bandwidth utilization, synchronization of large files like PSTs, and 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 that service level agreements (SLAs) are in place to guarantee performance, redundancy, and failsafe testing.

Nearly 2,000 IT DivvyCloud survey respondents:[2]

74%
Moderately or highly-concerned about public cloud security

57%
Data breaches are their highest concern

[1] Cybersecurity Ventures, "2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics," Morgan, Steve
[2] DivvyCloud, State of Enterprise Cloud and Container Adoption and Security, 2019

5) Using cloud-syncing services as your "only" backup tool

Many organizations think that cloud-syncing services provide "good enough" endpoint backup and restore capabilities for their enterprise data. But it's a risky misconception. Relying on cloud-syncing services alone for endpoint backup exposes your organization to multiple risks like ransomware, device loss, data corruption, insider threats, and liability exposure of not meeting legal hold, eDiscovery, and compliance requirements.

Relying on cloud-syncing services alone for endpoint backup exposes your organization to multiple risks.

In the instance of a ransomware attack, UK's National Cyber Security Centre (NCSC) warns that, "...cloud-syncing services (like Dropbox, OneDrive and SharePoint, or Google Drive) should not be used as the only backup, in case they automatically synchronise immediately after files have been 'ransomwared', at which point the synchronised copies are lost as well." [3]

Rethinking your endpoint backup approach is a good place to start. Rather than relying on cloud-syncing services alone, consider partnering with a third-party endpoint backup solution. With comprehensive endpoint backup, your organization can protect against any type of risk or corrupt activity, no matter where your employees are working around the world.

6) 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, recovery protocols, and fixed device locations which do not take mobile endpoint device requirements into consideration.

Solutions originally designed for the highly predictive environments of server backup (secure high-bandwidth LAN, regular backup schedules) perform poorly when confronted with endpoint backup environments that are highly unpredictable.

Choose an endpoint backup solution that is architected for the mobile workforce.

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

7) Undervaluing security or compliance requirements for your enterprise

In the past, you may have been able to overlook the details of how enterprise data was stored. Today, however, you have to know exactly how customer data is maintained, secured, and protected, especially with the rise of global business and ever-evolving international data privacy laws such as GDPR. Chances are, you also have to deal with SOC1 and ISO-27001 certifications or industry/government-specific requirements like HIPAA, ITAR, or FIPS to 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?

[3] ZDNet, "Ransomware victims thought their backups were safe," 2020

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 eDiscovery.

With the right endpoint backup solution in place that includes native 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 passed requisite certifications such as HIPAA for its data centers and operations.

According to an Exterro survey of 260 federal judges:[4]

48%
Felt attorneys neglected to comply with "complete and correct" discovery rules

47%
Have taken action to remedy eDiscovery problems 3+ times in the last year

38%
Consider email the most frequently spoliated data type

9) Choosing the wrong deployment model and not calculating TCO

Comparing upfront costs alone when evaluating solutions could mean that you'll pay more in the long term. Consider total cost of ownership (TCO): the costs of initial setup time, hardware, deployment time, and resources to manage endpoint backups. For instance, a solution that has low upfront costs may require weeks of initial setup time and effort.

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. These are critical issues when supporting remote workforces.

The decision how to implement a cloud, on-premises, or hybrid 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 stuck with managing a solution that does not align with your organization's IT strategy. It's also important to keep in mind that cloud-based solutions offer you on-demand scalability and allow shifting capital expenses to operating expenses.

Consider total cost of ownership (TCO): the costs of initial setup time, hardware, deployment time, and resources to manage endpoint backups.

[4] Exterro, Judges Survey of Judicial E-Discovery Perspectives and Practices, 2019

10) Not understanding SLAs and the 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 a significant business interruption. SLAs should answer: Is there a plan for redundancy in case one method fails? What happens to remote workforces 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, recovery time objective (RTO), and recovery point objective (RPO).

Any endpoint backup provider needs to provide SLAs to cover data availability, durability, recovery time objective (RTO), and recovery point objective (RPO). The following are examples of SLAs an enterprise should demand:

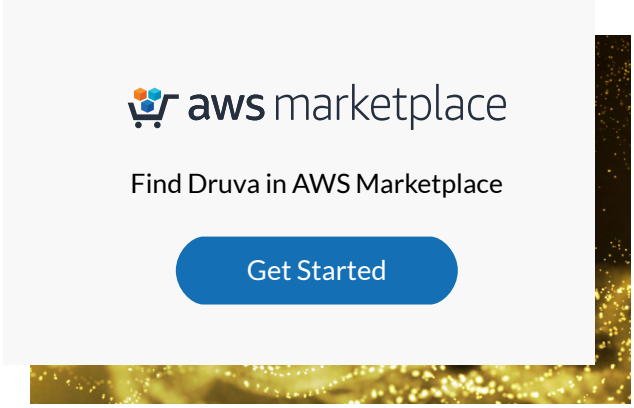
- **Service Availability —** will define the acceptable uptime for service and access to data, which is recommended to be 99.5%.
- **RTO —** the maximum amount of time taken to recover information, should be less than five minutes.
- **Data Durability —** sets an agreement on the loss of information and should be no lower than 99.99999%.
- **RPO —** detailing the granularity for endpoint data recovery should be less than ten 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.

Conclusion

When it comes to choosing an enterprise endpoint backup solution, the biggest mistake you can make is focusing only on cost, backup process, or security type. Solving for the smallest problem can only prevent your organization from scaling beyond backup to satisfy larger business initiatives. That's why it's important to fully understand the top trends, challenges, common pitfalls and how to overcome them, like remote workforce adoption, rise of ransomware, employee departure threats, and growing compliance requirements. By doing so, you'll widen the scope of your endpoint backup initiatives and solve larger business challenges — such as readiness for eDiscovery and data governance — which will ultimately lead to increased organizational agility and efficiency.

Your journey to endpoint backup success starts now
druva.com/products/endpoints



druva

Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital, Viking Global Investors, and Nexus Partners. Visit Druva and follow us @druvainc.