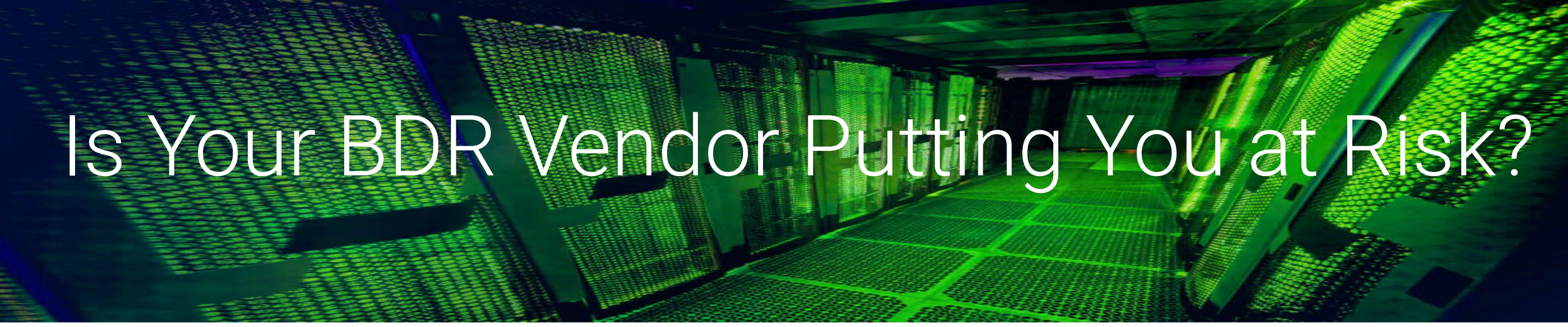

Is Your BDR Vendor Putting You at Risk?

The fear of significant data loss haunts businesses of all sizes. From enterprise organizations suffering a major breach to small or midsize businesses plunged into downtime, the repercussions can be so drastic that investing in backup and disaster recovery (BDR) solutions is almost universal.

Most teams have the same goals when using a BDR solution. They want to spend less time managing backups, want simpler and automated workflows, and they want to recover faster. They want transparent pricing and reliable support. But most of all, they want to know their data and organization is secure.

That's not always the case, though. With some BDR vendors still relying on outdated technology and practices, some vendors can actually hurt your team and sabotage your recovery.

8 Ways BDR Vendors Put You at Risk

The platform requires too much manual management. Do you really want to pay highly skilled IT staff to babysit backups? Or would you rather have them focusing on high-value projects that drive the business forward? Solutions that demand intensive hand-holding only waste the team's expertise and experience. The loss here: productivity and innovation.

The solution limits your ability to scale. If your backup solution can't grow along with your organization — think expanding storage, new servers — you'll either need to say no to new business or pay up when you hit a certain amount of VMs. Make sure your yearly growth is covered in case you grow from 10 terabytes this year to 15 terabytes next year — and doubly make sure the vendor isn't trying to push you into a small solution to force you to pay for a bigger one two years from now.

The solution is insecure. Encryption — for data at rest and in motion — is key here. If your vendor is not encrypting your backups, your breaches could be that much worse. You'll also want to ensure that data migration, datacenters and cloud backups are protected with proper controls — and that your vendor has taken the time to learn your specific risks and needs, so they can tailor your security program rather than give you a one-size-fits-all prescription.

You can't recover fast enough. This is an enormous liability when it comes to a ransomware attack, but long downtime windows hurt you in other ways. Lost sales and productivity, brand damage and irate customers can all deal a severe blow to the organization. If failing over is a complex process or recovery takes more than an hour, you're going through needless delays.

You're lost in multi-vendor chaos and weak support. When problems hit, you need to have a conversation with the people who can solve the problem. But when your solution contains a variety of vendors, you often contact a multitude of support teams who keep passing the buck. These disputes can go on for months while you're stuck with a malfunctioning system. The best way to avoid this is a unified solution that lets you talk to the same people who built it, rather than third-party support.

The SLA doesn't protect you. Your service level agreement (SLA) is a critical part of keeping your apps, servers and data protected. Your SLA should spell out the agreed upon Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), cover the number of backup copies available, file level recovery ability, the speed of the replica environment and other factors. If not, your budget and your recovery will be on the line.

The BDR solution isn't compliant. If you're dealing with PCI, HIPAA, SOX or other compliance requirements, you'll need to ensure your solution meets those regulations. Ask your vendor to spell out exactly which controls are meeting which requirements when it comes to the storage and transfer of data; any failed audits or fines will fall on your shoulders, not theirs.

You can only achieve partial recovery.

Tiered recovery, where critical data and systems are prioritized, is a smart strategy. But when numerous servers go down, a system capable of recovering only some systems is going to force you to decide between the file server and exchange server and make other tough decisions. In the age of unlimited uptime, you need a vendor that can keep everything going without impacting performance.

A final word: just because one of the above is an issue with your current BDR vendor, it doesn't mean you need to cut the cord. Find out the options first for adjusting your arrangement. But if your vendor is limiting your recovery or putting you at risk in numerous ways, it's probably time to look for a more modern solution.