



Protect your multi-cloud data with a backup and recovery service that's purpose-built for the cloud

With Veritas CloudPoint, organizations can manage multiple cloud service providers from a centralized dashboard

Many organizations are turning to multi-cloud environments to save money, avoid vendor lock-in, and increase flexibility. But the cost savings of the multi-cloud can fly out the window if organizations lack a robust data protection strategy: According to a recent study of over 400 companies, the average data breach costs \$3.62 million USD.¹ A cloud backup and recovery service can help organizations reap the benefits of the multi-cloud while protecting their cloud-based data and applications.

We researched publicly available materials to find the information about Veritas™ CloudPoint™ that we present in this report. As a data backup and recovery service built for the cloud, Veritas CloudPoint aims to provide a simple interface that helps administrators manage multiple cloud service providers from a single console. In addition to its unified interface, CloudPoint offers features like application-consistent and agentless snapshots, auto-discovery, and granular search and recovery. With Veritas CloudPoint, IT administrators can use unified management tools and essential backup and recovery features to protect their organizations' data.

¹ Ponemon Institute, "2017 Cost of Data Breach Study," accessed June 13, 2018, https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_COdB_Report_Final.pdf

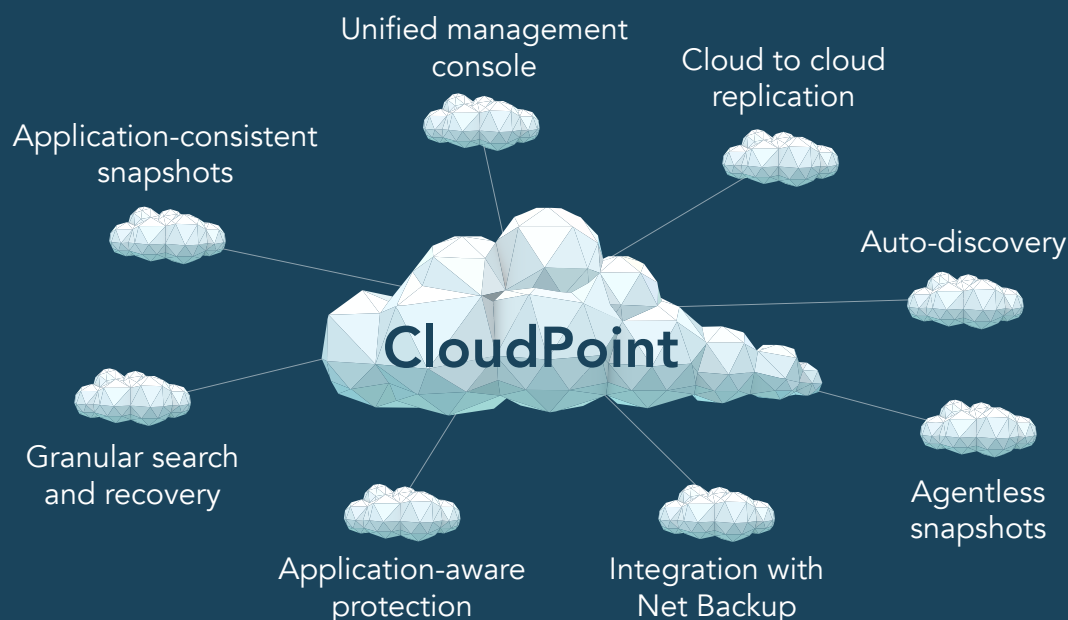
The challenges of protecting data in a multi-cloud environment

As the public cloud market continues to grow,² many companies are turning to a multi-cloud approach—in fact, 81 percent of enterprises now have a multi-cloud strategy.³ But multi-cloud environments present two big challenges.

- 1. Security risks:** The rise of cyber and ransomware attacks has increased the chance that companies' valuable data will be compromised.⁴ Even as 74 percent of organizations reported storing some or all of their sensitive data in public clouds, 22 percent experienced data loss or breaches with cloud service providers (CSPs) in 2016 alone.⁵ Whether they're facing the consequences of human error or a malicious attack, companies need a solution that can back up and recover their data quickly and easily.
- 2. Incompatible management tools:** Backing up and recovering data from every single CSP can cause hassle for IT staff and lost time and revenue for a company—especially if those backup and recovery systems weren't built for the cloud to begin with. With cyber and ransomware attacks already taking an average of 23 days to resolve, companies can't afford to lose time on clunky backup and recovery tools that aren't optimized for the cloud (*2017 Cost Of Cyber Crime Study*, 9).

Veritas CloudPoint aims to combat these challenges with a data protection service that's purpose-built for the cloud. CloudPoint uses a centralized dashboard to help users manage data backup and recovery in Microsoft® Azure™, Amazon Web Services™ (AWS), Google Cloud™, and more. CloudPoint is cloud-native; according to Veritas, this "makes it simple to deploy, easy to scale, and very cost-effective to run."⁶

-
- 2 Gartner, "Gartner Forecasts Worldwide Public Cloud Services Revenue to Reach \$260 Billion in 2017," accessed June 7, 2018, <https://www.gartner.com/newsroom/id/3815165>
 - 3 RightScale, "RightScale 2018 State of the Cloud Report," accessed June 7, 2018, <https://assets.rightscale.com/uploads/pdfs/RightScale-2018-State-of-the-Cloud-Report.pdf>
 - 4 Accenture, "2017 Cost Of Cyber Crime Study," accessed June 7, 2018, https://www.accenture.com/t20170926T072837Z_w_/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
 - 5 Intel Security, "Building Trust in a Cloudy Sky," accessed June 7, 2018, <http://usdatavault.com/library/Building-Trust-in-a-Cloudy-Sky.pdf>
 - 6 Veritas Technologies, "Veritas CloudPoint," accessed June 7, 2018, https://www.veritas.com/content/dam/Veritas/docs/data-sheets/V0469_GA_ENT_DS_CloudPoint2.0.pdf



How Veritas CloudPoint works

We gathered publicly available information to gain a clearer image of how CloudPoint works. Let's imagine you're an administrator deploying CloudPoint from Microsoft Azure. You can deploy CloudPoint directly from the Azure marketplace—saving time for your company.⁷ You then attach CloudPoint to your other CSPs, like Amazon Web Services and Google Cloud. CloudPoint unites your CSPs in a unified platform, giving you a broad overview of your VMs on a single interface.⁸

CloudPoint uses cloud service providers' publicly accessible APIs to take snapshots and index them in object storage.⁹ CloudPoint also offers application-aware protection (which helps the program taking application-consistent snapshots better protect applications that need it) as well as auto-discovery and agentless snapshots. These features automatically scan VM virtual disks for data and track it in a database, reducing management workloads for IT administrators (*Veritas CloudPoint 2.0.2 Administrator's Guide*, 67).

CloudPoint also enables you to take a variety of approaches when it comes to managing your backups and recovery. With CloudPoint, you could choose to:

- Deploy agents on mission-critical VMs like those running customer databases. These agents supplement the crash-consistent snapshots taken by CSPs (which only back up files) with application-consistent snapshots, which capture in-system memory so you don't have to do file recovery when you bring up a VM that has crashed (*Veritas CloudPoint 2.0.2 Administrator's Guide*, 50).
- Protect sensitive information by wiping snapshots with personally identifiable information. CloudPoint can automatically search snapshots for this information and then either flag or delete it, ensuring it can't be misused (*Veritas CloudPoint 2.0.2 Administrator's Guide*, 132). This feature helps companies meet General Data Protection Regulation requirements around the protection of personal information.¹⁰
- Integrate CloudPoint with an existing NetBackup™ infrastructure so that companies already used to the NetBackup experience can use the same interface.¹¹
- Use role-based access control to make sure that only trusted administrators can perform specific roles. Administrators can also apply policies across multiple clouds at once, potentially saving time and effort (*Veritas CloudPoint 2.0.2 Administrator's Guide*, 79).
- Find deleted files with granular search and recovery. This feature pulls out individual files to wherever an administrator wants, such as the user's desktop (*Veritas CloudPoint 2.0.2 Administrator's Guide*, 121).
- Use cloud to cloud replication to take a snapshot in one region and restore the snapshot to a different region, allowing you to more quickly replicate data between regions (*Veritas CloudPoint 2.0.2 Administrator's Guide*, 106).

For more information on the features offered by CloudPoint, see the Veritas datasheet: https://www.veritas.com/content/dam/Veritas/docs/data-sheets/V0469_GA_ENT_DS_CloudPoint2.0.pdf

7 Microsoft Azure, "Veritas CloudPoint," accessed July 19, 2018, <https://azuremarketplace.microsoft.com/en-us/marketplace/apps/veritas.cloudpoint-2-0-0?tab=Overview>

8 Veritas Technologies, "Veritas CloudPoint," accessed July 19, 2018, https://www.veritas.com/content/dam/Veritas/docs/data-sheets/V0469_GA_ENT_DS_CloudPoint2.0.pdf

9 Veritas Technologies, "Veritas CloudPoint 2.0.2 Administrator's Guide," 130, accessed July 19, 2018, https://www.veritas.com/content/support/en_US/doc/127987807-127987811-1

10 Michael Nadeau, "General Data Protection Regulation (GDPR): What you need to know to stay compliant," accessed July 17, 2018, <https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html>

11 Veritas, "Veritas NetBackup Snapshot Client Administrator's Guide," accessed July 19, 2018, https://www.veritas.com/support/en_US/doc/23946785-130532244-0/v130162731-130532244

Conclusion

Whether they're dealing with data breaches or simple human error, organizations storing their data in a multi-cloud environment need to make sure they can back up and swiftly recover their data. A data protection plan like Veritas CloudPoint can help organizations do just that. According to the publicly available materials we found, CloudPoint is purpose-built for the cloud, has essential backup and recovery features, and helps IT administrators manage their backups from one convenient interface.



This project was commissioned by Veritas.



Facts matter.®

Principled Technologies is a registered trademark of Principled Technologies, Inc.
All other product names are the trademarks of their respective owners.

DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY:

Principled Technologies, Inc. has made reasonable efforts to ensure the accuracy and validity of its testing, however, Principled Technologies, Inc. specifically disclaims any warranty, expressed or implied, relating to the test results and analysis, their accuracy, completeness or quality, including any implied warranty of fitness for any particular purpose. All persons or entities relying on the results of any testing do so at their own risk, and agree that Principled Technologies, Inc., its employees and its subcontractors shall have no liability whatsoever from any claim of loss or damage on account of any alleged error or defect in any testing procedure or result.

In no event shall Principled Technologies, Inc. be liable for indirect, special, incidental, or consequential damages in connection with its testing, even if advised of the possibility of such damages. In no event shall Principled Technologies, Inc.'s liability, including for direct damages, exceed the amounts paid in connection with Principled Technologies, Inc.'s testing. Customer's sole and exclusive remedies are as set forth herein.