SAFEGUARDING DATA IN A HYBRID MULTICLOUD WORLD

Throughout the last decade of public cloud migration, the top-of-mind question has been “Can I really trust this vendor to keep my data safe?” In 2019, we can confidently say that this paradigm has shifted. Cloud providers such as AWS, Azure, and Google Cloud have responded to the concerns of the past decade and collaborated with enterprise customers to ensure that cloud workloads are as secure and resilient against external threats as those in on-premises data centers.

But that doesn’t automatically make data "safe" in the public cloud.

Although data in public clouds is secure from external threats, true safety—knowing that all your data is in compliance with regulations, stored correctly to ensure business continuity, and secured against access from unapproved internal users—now comes down to what you’re doing to see and control where data is going across your entire infrastructure. The onus has shifted from the cloud back to the organization itself.

NetApp has long been in a unique position to watch how this paradigm has shifted. Our partnerships with the world’s biggest clouds, and our traditional leadership in storage and investment in a data fabric strategy, give us a window into the new questions that are being asked—and answered—about securing and protecting data in a world where hybrid multicloud has become the de facto IT architecture.

The question is no longer “Can I trust this cloud with my data?” but instead “Can I trust that my organization knows who is touching the data and where they are putting it?”

This evolution has been a long time coming, driven by both long-term and emerging industry trends. The most significant, albeit obvious, trend has been the rapid rise to dominance of the public cloud. Ten years ago organizations were slow to migrate; now everyone we talk to is using at least one public cloud. The advent of cloud has changed everything, and public clouds have established a new standard for IT experiences that all vendors must live up to.

Consider how public clouds have addressed the security concerns of the past decade, landing in the spotlight for hackers. They’ve espoused the shared responsibility model so that providers and customers can ensure a complete and consistent security posture. On their hardware and infrastructure responsibility, they’ve defended themselves admirably, hardening their systems to continually protect against new attacks, optimizing systems each time. Yet their biggest advantage is scale—the immense budgets that hyperscalers have access to help them attract the best security talent in the industry, and they upgrade their data centers at incredible rates.

To drive home how secure public cloud environments are, consider our partner Microsoft Azure. Following our Azure NetApp® Files collaboration, we’re working closely with Microsoft to make the service available in Azure Government to meet the demands of the organizations that control the world’s most sensitive information, and to ensure the most secure and compliant environment possible with FedRAMP certification for Azure NetApp Files in both Azure Government and the other dozen Azure regions that are available.
In addition to deepening our relationship with Azure with the efforts on Azure NetApp Files for Azure Government and FedRAMP certification, we have added new security features such as external key management and FIPS 140-2 compliance to our NetApp HCI and SolidFire® solutions, further showcasing our commitment to meeting the most stringent data requirements in highly regulated industries such as government, finance, and healthcare.

Public clouds have become extremely secure, but other trends have emerged that make safeguarding data as challenging as ever. IT environments today are incredibly complex and difficult to monitor—and they’re only getting more so with the constant integration of new platforms and the resulting data silos. At the same time, more people in more places are trying to access data for disparate uses, resulting in well-documented cases of shadow IT and rogue DevOps where processes that prioritize speed to business value rather than security and compliance are the norm.

This is where NetApp Cloud Insights comes in. Our multivendor, multicloud monitoring and optimization service now extends to security and compliance, applying analytics and machine learning to the patterns of who is accessing files and data. Suspicious activity that might indicate an external hacker or data breach can be flagged, and it’s also very important to look at insider threats, whether intentional or unintentional, that might violate internal rules or policy, across the hybrid cloud.

All this adds up to one truth: **Today it’s far easier to accidently put data where it’s not supposed to go than it is for a hacker to crack a cloud and access your data.** Organizations must focus first and foremost on putting controls in place to manage and monitor their data at all times.

That’s why NetApp has announced another new service, NetApp Cloud Compliance, which monitors native cloud storage in the public cloud. Designed to integrate with Cloud Volumes ONTAP®, which provides data management and data protection for AWS, Azure, and Google Cloud block and object storage, Cloud Compliance applies artificial intelligence to identify and classify sensitive data such as payment card information (PCI), personal health information (PHI) like patient data, and personally identifiable information (PII) and to make sure that it is being stored and used only in the clouds that were intended. Cloud Compliance can help ensure that only the appropriate on-premises and cloud environments are storing data and that they are in compliance with industry regulations and the increasing number of governmental privacy mandates such as GDPR in Europe and CCPA in California.

If you can see your data, you can trust that it is secure, regardless of the environment you are operating in. If you have well-defined policies in place that specify what data can live where and who can touch it, and you have the tools in place to monitor that, you won’t need to ask whether your data is secure in the cloud. You’ll know that it is.

This new paradigm for securing and protecting data in a hybrid multicloud world requires a new approach. The industry must embrace a centralized, automated, real-time model that empowers IT leaders to be the single source of truth when it comes to data. IT teams must further be equipped with AI-driven insights to simplify situations that require immediate action, and be given the flexibility to immediately access their data and enrich it for threat detection and forensics.

With NetApp, organizations can trust that they’ve implemented a best-in-class set of solutions to meet the new mandate for data visibility and control, which is central to an effective overall security approach.

We’ve been preparing for the reality of hybrid multicloud. Our vision at NetApp INSIGHT® 2019 is to help organizations build their data fabrics, simplify how they manage IT systems, how they consume IT resources, and how they power real-time, always-on data visibility across any hybrid multicloud environment.

At NetApp INSIGHT 2019, we’re doubling down on that vision and acknowledging the “new normal” for data security and protection for a hybrid multicloud world. We are introducing new and updated tools to build and safeguard your data fabric across the most demanding industries and regulations.

NetApp is the only provider of a complete set of solutions to monitor any mix of IT environments and automate threat detection and to monitor user behavior in real time. NetApp provides the safety net that organizations need to stop unauthorized data access or movement as it is happening.

In 2019, you can trust your public cloud—if you can trust yourself. This is a challenge for IT leaders, and also an opportunity. Safeguarding data necessitates achieving central control and a deeper understanding of how data moves through an enterprise. The visionaries who can make this happen are poised to determine their organizations’ relationship with data for years to come.