PROTEGRITY

STRATEGIC OVERVIEW

Developing a Cloud Data-Protection Architecture

Businesses are beginning to recognize that most of the doubts they had about shifting workloads to public cloud aren't valid.

Any lingering reservations about cloud security, migration, and other technology challenges have been cast aside by the allure of greater operational flexibility, not to mention the opportunity to tap applications such as AI and analytics, containerization, and automation. Also, the sudden shift, en masse, to remote work caused by the COVID-19 pandemic reminded them even more of the operational value of cloud.

Gartner expects spending on public cloud services to increase 18.4 percent in 2021, to total $304.9 billion–compared with $257.5 billion in 2020–in large part because of the acceleration of digital modernization created by remote employees who conceivably can't work without cloud. But long after the pandemic–whether employees return to their offices or not–cloud will continue to be a conduit to improved collaboration with customers and partners, as well as the route to key insights from data that's analyzed via machine learning.

That's not to suggest cloud is free of the security concerns that had long delayed migration. More than three billion people had their personal data stolen in just two of the top 15 biggest breaches of the 21st century, while the smallest incident since 2000 involved the data of a *mere* 134 million people.

The fact is, data-security threats will only increase in number and complexity as enterprises migrate even more data and workloads into the cloud. Enterprises surveyed by Everest Group said 58 percent of their workloads already are, or soon will be, on a hybrid or private cloud, while 60 percent of organizations place sensitive data in the cloud.

If businesses want to expand their digital footprint in the cloud and grow with nimbleness and authority, they have no choice but to strengthen their data-security efforts–especially with them fast-tracking cloud migration because of the pandemic and that regulations require safeguarding the privacy of certain data. By developing a cloud protection architecture that makes data security a top priority, companies can fully embrace the potential of cloud.

Developing a Cloud-Protection Architecture

The ability to directly control the protection of data as it flows in and out of the cloud is vital. With a cloud architecture centered on data protection, companies can take control of security and focus on cloud-based innovation.

Such an architecture protects data at all points: as it rests, when it's in motion, and when it's in use. This includes the movement of data from legacy data centers and into the cloud. The organization, itself, and not the cloud vendor, can determine the data-security policies that best align with laws regulating the privacy of data. Without control, data security rests with a cloud provider, which typically doesn't offer that level of protection.

Organizations need to think holistically about data and how it flows through cloud and on-premises technologies, and then architect a solution that works with, and not against, these data assets. Cloud technology is only as good as the data behind it, and data is only as valuable as the effort put into its security.

Key Practices of a Cloud-Security Strategy

An effective cloud-security strategy will make good use of several practices:

SEPARATION OF DUTIES AND EXTENSIVE AUDITING

Best practices dictate that administrators do not have access to data, preventing those with privileged access from becoming the targets of cybercriminals. Access to secure assets is instead logged with the user, place, time, and action. This creates an audit trail that supports compliance.

FINE-GRAINED PROTECTION

Protection is ascribed to certain pieces of data or the person trying to access it, different from the loosely applied coarse-grained protection method that prevents data from being used in more than one cloud platform or application without losing its protection. Fine-grained protection is what gives organizations true control of data security, enabling them to craft security policies as they deem appropriate. For instance, they can allow front-line employees to see only the elements of customer information that they should see so they can better serve customers.

CENTRALLY MANAGED SECURITY POLICIES

This is the best way to manage sensitive data elements, data protection, and access privileges.

Centralized management of security policies simplifies enforcement across disparate cloud systems and tools, protecting sensitive data across the large sweep of cloud-based applications and functions that modernize business.

LEGITIMATE CONCERNS FOR CLOUD

CIOs and IT leaders had legitimate concerns in the past about migrating to cloud. In fact, many of those concerns linger:

- How does a cloud provider handle encryption and encrypted data?
- Do our users have exclusive access to their data?
- Does our data get commingled with data from the cloud vendor's other clients?
- Does the cloud provider satisfy all compliance requirements including specific statutory regulations for all jurisdictions or all enterprise policies?
- Is data stored so that it is physically protected as well?
- Does the cloud provider mine the data that it stores for its own purposes?
- Is the cloud provider fully auditable?
- Does the cloud provider provide breach notifications according to our company's privacy policies and statutory requirements?
- Are the cloud provider's overall security capabilities sufficient?
- Does the cloud provider have data-transfer capabilities and sufficient security for the data transfer?

The answers sort themselves out when organizations build a cloud architecture that emphasizes data security.

TRANSPARENT ADMINISTRATION

Data security should be transparent for users, so they can determine what to protect–particularly sensitive data that falls under the scope of regulation. You can't protect data if you don't know it needs special protection.

Build a Cloud Architecture Based on Data Protection

An effective cloud data-protection architecture closes security gaps and simplifies the management of policies because it easily integrates with all transactional systems, distributed architectures, big data and analytical systems–whether they are on-premises or in hybrid-cloud infrastructures. With a unified view of data in all of those places, companies can make singular decisions on how to protect sensitive data.

A PROTECTION ARCHITECTURE ENSURES THAT:

- Data is protected before it migrates to the cloud.
- Data is protected wherever it flows, especially as it moves across complex data ecosystems.
- Data-security policy enforcement is consistent, as policies are centrally managed by data or role.

Companies need a data-centric security strategy that meets their requirements for doing business–instead of constraining them with a one-size-fits-all approach that doesn't scale with the breadth and complexity of today's enterprise environments and instead creates gaps in data security.

To take advantage of different cloud platforms and tools, as well as various on-premises technologies, an organization must have an individualized data-centric security approach that completely protects sensitive data in a way that aligns with corporate policies, stringent government regulations, and exacting customer expectations about uncompromising privacy.

PROTEGRITY

Protegrity USA, Inc.
(Global Headquarters)
1165 E Wilmington Avenue
Suite 200
Salt Lake City, Utah 84106
1.203.326.7200
1.650.431.7000

Protegrity (Europe)
1 St Katherine's Way
London, E1W 1UN
+44 1494 857762

Email: info@protegrity.com