Unlocking Innovation Through Data Security

Welcome to a Borderless World

Innovation is more than a buzzword. The ability to leap ahead of the competition and deliver value to customers has become nothing short of critical. Yet, somewhere between infinite possibilities and actual opportunities lies the real world of building and supporting a framework for business innovation. Not surprisingly, data lies at the center of this equation.

Data is the currency for the digital age. It drives decisions, delivers insights, and defines how companies embark on tasks as wide-ranging as research and development, marketing, sales, operations, finance, human resources, and customer support. But, not all data is created equal, and not all data is generated, stored, managed, and consumed the same way. This makes protecting data — and ensuring privacy — a growing challenge.

Within a typical enterprise, data now streams across multiple geographic locations, offices, and business groups. It spans various networks, systems, and applications from legacy software to multi-cloud environments that use multiple vendors and programming languages. It also reaches across supply chains and extends to third parties, including customers, through application programming interfaces (APIs) and connected devices that comprise the rapidly growing Internet of Things (IoT).

This environment points to a need to create a data protection strategy. It requires a more advanced way to accommodate, manage, and control large volumes of data throughout its lifecycle. It requires visibility—preferably through a single pane of glass—that offers deep insight into interfaces, interaction points, and tools required to ensure broad and deep protection that extend beyond conventional borders and boundaries. It also requires sophisticated tools to address increasingly challenging policy enforcement and regulatory compliance issues. **The answer? A best practice approach**.

Data Protection Isn't Optional

The ultimate goal with any enterprise security framework is to establish robust protections without allowing these systems to get in the way of the business. Unfortunately, this goal often proves elusive. Today, a typical security team relies on upwards of 70 tools, often with different controls, interfaces, and functions. Things grow more complicated by the day as tools and interfaces proliferate — especially in the cloud. In many cases, administrators, and security teams must manage all these systems and the difficulties that result when multiple systems attempt to control the same task or technology, such as encryption or application security. Too often, the results are inconsistent policy enforcement, limited data access, limited business growth, and an elevated level of vulnerability.

The problem doesn't stop there, however. Far more complex data ecosystems — and the sheer volume of today's data moving through them — increase data exposure points that can lead to breakdowns, breaches, regulatory penalties, bad press, and other potential problems. While heterogenous data frameworks are ideal for fueling innovation, they aren't designed with data protection as the primary goal. Although firewalls, encryption, authentication, data loss protection (DLP), malware tools ,and other security systems continue to play an important role in enterprise cybersecurity, they don't address the specific problem of managing and securing sensitive data.

Even cloud-centric organizations face steep challenges. Clouds can't replace all legacy systems or remove the need for data warehouses and data centers. They simply add another layer to the enterprise data framework. Likewise, IoT systems add new requirements for handling data and artificial intelligence on the edge of the network, along with data that streams across servers, clouds, and organizations. As if all of this isn't enough, there's onerous regulatory compliance issues to grapple with. This includes PCI, HIPAA, the European Union's (EU) General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA), to name a few. Unfortunately, there are significant penalties for noncompliance.

Take Data Security to a Higher Level

It's no secret that data security is only as strong as its weakest link. As data migrations and multi-cloud environments become the new normal, it's critically important to simplify the vast array of processes, oversight, and controls through a centralized view and comprehensive controls. There are four critical factors involved in creating a best practice data protection strategy:

> **Think Strategy.** A best practice approach to data security requires a clear strategy and the right technology. It demands a vendor-neutral, enterprise-wide security policy with a solution that extends across different technologies, databases, clouds providers, and tools. While clouds won't kill the datacenter, an enterprise must be equipped to handle the challenges of managing and moving data in and out of clouds, including through serverless functions and container platforms. Ideally, a solution is available as a container so that it can be easily deployed, moved, and adapted as needed.

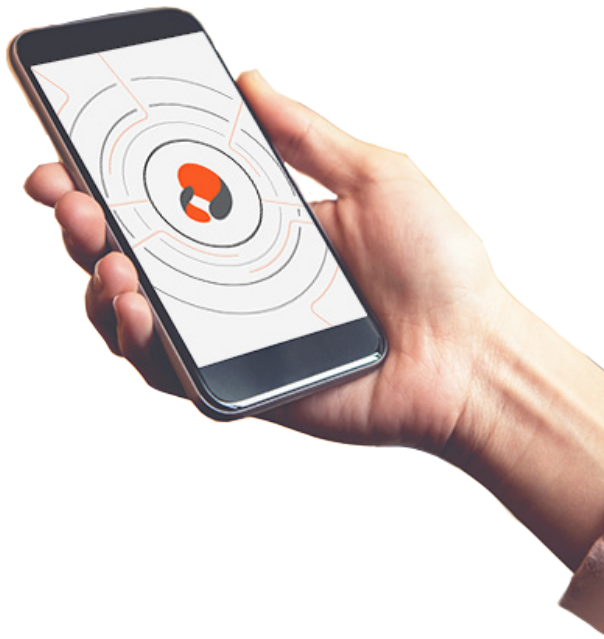
> **Focus on Data Classification and Authorizations.** A starting point for this journey is ensuring that your organization's data is classified correctly and that access matches roles and risks. It's vital to understand how internal teams use data, what data they require, and what data is dispensable. Traditionally, organizations protect data at the system level. But this model is no longer suited to today's data frameworks. So, roles, authorizations, and access must revolve around concepts such as least privilege, zero trust, and separation of duties. It's important that authorized users can see data in the clear and others who are restricted do not.

A historical landmark decision from the EU's highest court illustrates the extent of the challenege. In July 2020, it ruled that a Privacy Shield Agreement between the U.S. and EU was invalid. The current framework doesn't adequately protect European citizens the way that GDPR had intended, the judges noted. This ultimately places a greater burden on businesses to develop better data-level safeguards and protections. On a practical level, this means an organization must track where every piece of data comes from, where it resides, and understand how it is used. Consulting firm Gartner Inc. estimates that by 2024, 75% of the global population will have its personal data covered under modern privacy regulations, up 10% from 2021.

In this environment, businesses must adopt a data management framework that's built for digital transactions and interactions. Among other things, this involves de-identifying data but also being able to re-identify it for key business purposes. Unfortunately, many data security products simply make copies of sensitive data and use basic masking techniques to hide credit card numbers, account numbers, National Insurance Numbers, birthdates, and other personal identifiers. In the end, they don't fully anonymize and protect sensitive data. So, without a single pane of glass and comprehensive controls, vulnerabilities emerge, risks grow, and privacy safeguards remain elusive.

Dial Into Discovery. With this strategic foundation in place, an organization can deploy robust data discovery tools to better understand the nature of sensitive data, where it resides, how it travels inside, and outside the organization, and how it is used by different groups — including in different situations and circumstances. Effective data discovery not only allows organizations to more effectively link data with roles, it also aids in streamlining auditing, simplifying compliance, and delivering essential protections.

Harness the Power of Tokenization. A tokenization framework is valuable because it eliminates the need to replicate data, and incur costs and risks associated with multiple versions of data floating around an enterprise. The best lightweight tokenization technology can run on commodity hardware and requires no modification to existing processes and systems, thus further magnifying cost savings, agility, and scalability. If cybercrooks breach a system or gain access to a database, the tokens represent valueless information. This technology makes it possible for a business to maintain data formats, character lengths, and other essential features. It also introduces more transparent and flexible protection models.



The goal is a data protection framework that delivers robust end-to-end controls. A business should have the ability to de-identify a vast array of data types dynamically and effectively — without compromising business processes, performance, and innovation. With advanced security tools such as encryption, tokenization, and masking it's possible to ensure that the integrity of transactions is preserved.

In the end, data repositories are more fully protected and more easily accessible for legitimate business purposes. This approach ensures that an organization maximizes the value of data while minimizing risks. It's a data management and security model designed for the digital age.

A Global Retailer Takes Aim at Data Protection

Overseeing sensitive employee data, including Social Security and National Insurance Numbers, is a critical function for human resources departments. At one global retailer, the task was particularly complicated. The company had multiple data repositories and data management systems in place around the world. This included Teradata EDW, as well as Pivotal HD, and SQL Server. Adding to the challenge, it had to enable secure analytical and operational processes according to the US Food & Drug Administration (FDA) reporting requirements.

Addressing this framework wasn't easy. Data character preservation had to take place across the entire data flow — FTP, Hadoop (Hive), DataStage, Teradata, and various user applications. The data management system also had to handle scripts and coding alignment between production and development test environments.

The company ultimately selected a holistic Protegrity solution that delivered data tokenization as well as advanced built-in auditing and reporting. The result was an ability to protect data and maintain a high level of agility and flexibility for the business. Moreover, the data was "future proofed" through support for European character sets and new data sources that could emerge. The approach helped the retailer improve performance and trim costs — with a maximum level of data security.

Putting Innovation to Work

A best practice framework leads to maximum data protection, strong regulatory compliance, high performance, and scalability. It also simplifies inherently difficult security tasks, such as masking data while ensuring its usability. As organizations migrate to a framework that revolves around agility, flexibility, DevOps, and rapid innovation — typically through multi-cloud environments and a growing array of IoT data — this approach delivers highly automated controls over data from top to bottom and across an enterprise. It also extends outward across business partners and customers, while tackling key regulatory and compliance concerns.

With a single pane of glass in place, it's possible to gain full visibility and control over the array of clouds, legacy databases, data lakes, and other data sources. An enterprise can establish unified controls that span vendors, hardware systems, products, and data formats. This environment supports ongoing changes to an IT framework without disrupting data flow and, ultimately, innovation.

In the end, a privacy by design framework delivers the flexibility to add or change clouds, add IoT devices, harness APIs, and migrate data, containers, and other elements quickly — without introducing gaps and exposure points. It's a platform designed and built for today's demanding digital business requirements, but it's also equipped for future growth and ongoing changes, in whatever form they take. Privacy-by-design is a model for today's borderless business world. It puts innovation and disruption in the spotlight.

How You Can Get Started

These methods can help you ensure that your organization's data framework is up to speed and ready for digital business.

1. Devote the necessary time to understanding and defining **roles and responsibilities.** This serves as the foundation for any data management framework.
2. Focus on **data discovery.** It's critical to classify data and gain a granular view of data types so that a data management system can do what it is supposed to do — manage and protect data. The right solution can greatly simplify this process.
3. Establish clear **policies** and **access controls** that match roles and responsibilities. Access control should incorporate multi-factor authentication, which greatly reduces the risk of unauthorized use of an account.
4. Make sure that the data management and protection solution integrates seamlessly with an **identity management system,** such as Microsoft Active Directory or Okta.
5. Deploy end-to-end controls and reporting capabilities for **protecting** and **auditing** data in order to ensure a system is working effectively and correctly.
6. Use a **central dashboard** that delivers a centralized view and consolidated controls over data. This single pane of glass greatly simplifies control over disparate applications, devices, networks, and systems, including multi-cloud frameworks and IoT data. Best-in-class applications provide this level of oversight.
7. Use scalable, low latency, lightweight fine-grained **tokenization,** such as Vaultless Tokenization that Protegrity offers. It handles data de-identification and re-identification seamlessly, ensuring that an enterprise is using the most advanced and secure data protection methods possible.

FOR MORE INFORMATION ABOUT HOW PROTEGRITY CAN HELP SECURE DATA IN THE CLOUD AND BUILD A MORE ROBUST DATA-CENTRIC ENTERPRISE, VISIT PROTEGRITY.COM.

[1]Gartner Inc. https://www.technologydecisions.com.au/content/it-management/news/data-privacy-regulations-to-protect-63-of-the-world-by-2023-82212200
[2]IBM. https://www.ibm.com/downloads/cas/QMRQER0B

Protegrity USA, Inc.
1.203.326.7200