Powered By

exate

AN INTRODUCTION TO DATASECOPS

FEBRUARY 2021

Introduction

DATA-DRIVEN COMPANIES ARE 23X MORE LIKELY TO SEE AN INCREASE IN CUSTOMERS AND 6X MORE LIKELY TO RETAIN THEM

Every cybercriminal knows that information is a company's most valuable asset, and by 2022, according to Gartner, "90% of corporate strategies will explicitly mention information as a critical enterprise asset and analytics as an essential competency." Organizations, if they haven't already, will need to take a more data-centric approach when evaluating their value.

"Over the next several years, those in the business of valuing corporate investments, including equity analysts, will be compelled to consider a company's wealth of information in properly valuing the company itself," said Douglas Laney, former vice president and distinguished analyst at Gartner.

Those companies that can unlock and utilize their data will benefit most in the digital transformation. Data-driven companies are 23 times more likely to see an increase in customers and six times more likely to retain them. Better customer engagement leads to higher profits. When a company can digitalize their data in positive, business-oriented ways, it benefits everyone.

But how do you get access to the value-added data in a safe and controlled manner? And how do you ensure security and meet all data privacy compliances? The answer is found in DataSecOps.

DataSecOps is the natural progression of DevOps and DevSecOps principles. It is IT working with data analysts. It is a collaboration between engineers and the admins surrounding how to securely store, analyze, archive and deliver data. DataSecOps offers an automated process to manage both data and security within operations and eliminates silos.

"DataSecOps can protect structured data by integrating security into the migration process," according to reporting by Security Boulevard.

> **"Rather than encrypting the data when it enters the cloud, DataSecOps ensures it is encrypted before it leaves the company's firewall protection. That's the Ops part. The security part is assigning a key to specific columns, allowing permitted access to the database but the overall data is never decrypted."**

The secure encoding and delivery of information is at the forefront of the implementation process. DataSecOps combines and coordinates multiple privacy enhancing technologies within a single intuitive platform, connected to built-in governance and controls. This allows the data to be securely protected with a variety of different methods during the migration process, ensuring greater data protection without compromising accessibility, unlike manual methods or multiple single-point systems.

By allowing data policies to automatically be applied to data, users are able to realize the true value of data once again to provide a strategic and competitive advantage.

Data Privacy and the Worldwide Push to Protect Information

GDPR and other data privacy regulations across the world have forced organizations to change the way they think about data security and privacy. Because of this, there is a push to keep data local as much as possible. This, however, requires having the right infrastructure in place.

The impact of these regulations and the lack of infrastructure is an ability to work with and test production data. Working with production data in a less secure environment is against ISO compliances.

Yet, each development team has its own approach to providing data protections in production, and many don't consider security and privacy elements at all. The same happens when the application and data move to the testing environment; data security is most often ignored, especially among startup companies. The priority is to get the product to market as soon as possible and data privacy goes by the wayside.

The global push for data privacy, as well as industry regulations and consumer insistence, forces companies to put more consideration into protecting data across all stages of the DevOps lifecycle.

Challenges to Protect DATA

It's one thing to make a pledge to protect data in production and testing, but another to actually do it. In all phases of the lifecycle, there are significant challenges to working with data.

In Testing:

- Inability to work with production data
- Multi-chain testing is virtually impossible
- Testing with start-ups is challenging

In Data Localization:

- Requirements to keep data are held locally
- Hinders global digital transformation
- Expensive as companies need to be able to keep up within each jurisdiction in each country with privacy laws wherever business is done

In Meeting Data Regulations:

- Ensuring clients have control over their own data
- Derogations
- Anonymize data, thereby destroying its value

In Data Analytics:

- Have to work with anonymous data sets
- Differential Privacy
- Hyper-personalization experiences where identification is needed in certain situations

How DataSecOps Rises to the Challenge

DATASECOPS PUTS PROTECTING THE DATA FIRST AND FOREMOST

IT and data analyst teams need to collaborate in order to address the concerns surrounding data privacy and security in the DevOps production and testing lifecycle.

Some techniques that are used to protect data in a global environment include different forms of encryption, differential privacy, zero knowledge proof, synthetic data, secure multiparty compute enclaves, transaction execution environment – there is a whole realm of privacy and hardening techniques.

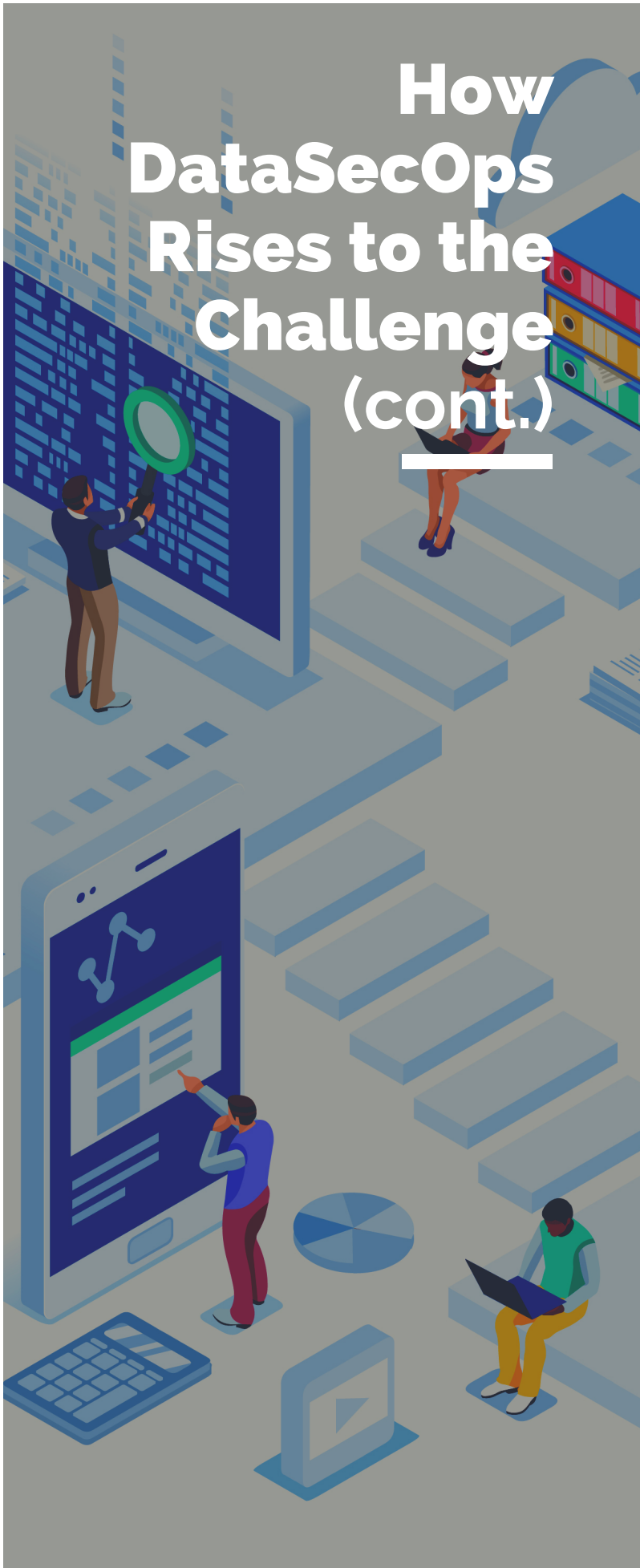
Not only do you have the privacy tools available, there must also be taken into consider the ways data is being accessed – through a database, APIs, the cloud, shared through third parties. Yet there is little policy within organizations on how that data can and should be used.

DataSecOps puts protecting the data first and foremost. This can be done by aggregating all of the different privacy techniques into one hybrid form. That way, if consumers have opted in, you can use consent-driven access or if they've opted out, you can use differential privacy.

This locks down the data while reducing the risk of the data being identified. And because the need for DataSecOps isn't just for production environments, there is the option for synthetic data to be used in development environments.

There are plenty of solutions available that touches on these techniques individually, but that is cumbersome. Instead, the holistic approach is to apply consistent governance and controls of data within development, production and testing environment.

How DataSecOps Rises to the Challenge (cont.)



You can do more by focusing on the metadata rather than on the data itself. This way, if you're working with an API, you will have access to data while ensuring that you're only seeing what you absolutely need to do the job.

This limit to what can be seen and used during the DevOps lifecycle keeps in compliance with the data ethics required by GDPR and other privacy regulations. Data ethics requires permission has been given to use the data and that it is being used within the proper context. It allows for governance over jurisdiction, as well. This offers transparency back to the consumer.

Each development activity has slightly different requirements. DataSecOps needs to be able to work alongside the development pipeline so when you provision data for whichever environment you're using, the right development rules are applied.

The goal of the DataSecOps platform is to automate privacy governance and add cybersecurity controls into the production process. All DataSecOps platforms should include the following five components:

- Metadata
- Governance and Policy (including access management; record retention; and data ethics)
- Privacy Enhancing Technologies (there is no one-size-fits-all model so there's a need for multiple types)
- Data Destruction (including breach management and the right to be forgotten)
- Audit of Use (including anomaly detection and subject access requests)

In the DataSecOps platform, there should be modularity of each of these components, so organizations can plug in their own technologies to provide for control of how the data is used and protected.

Conclusion

Your portfolio of information is going to determine what your valuation of the company is, but providing security and data provisioning is not an easy task. It requires data scientists and data engineers, which is an expensive resource, especially to do the same tasks over and over again. Most of a data scientist's work is working on the provisioning of data.

By adopting DataSecOps you can:

- Automate your data policy to systemically comply with risk and regulation
- Protect your sensitive data with the ability to revoke access on demand
- Unlock your data in order to provide maximum value through analytics and insights, which will drive the personalized experiences that customers demand

Sponsored by eXate

www.exate.com

info@exate.com

+44 (0) 203 745 0713