REPORT REPRINT

Data obfuscation rises in importance due to the growing desire for self-service data

MARCH 26 2021

By Henry Baltazar

As an increasing number of organizations look to accelerate their DevOps and developers' access to production data, the need to integrate techniques such as data masking into these self-service data operations will rise. In a recent study, we found that more organizations were aiming to implement data obfuscation methods to protect their data.

451 Research

S&P Global
Market Intelligence

Introduction

As an increasing number of organizations look to accelerate their DevOps and developers' access to production data, the need to integrate techniques such as data masking into these self-service data operations will rise to prevent the exposure of compliance- or personally sensitive data. In 451 Research's Voice of the Enterprise (VotE): Storage, Transformation 2020 study, we found that a growing number of organizations were looking to implement data obfuscation methods to protect their data.

451 TAKE

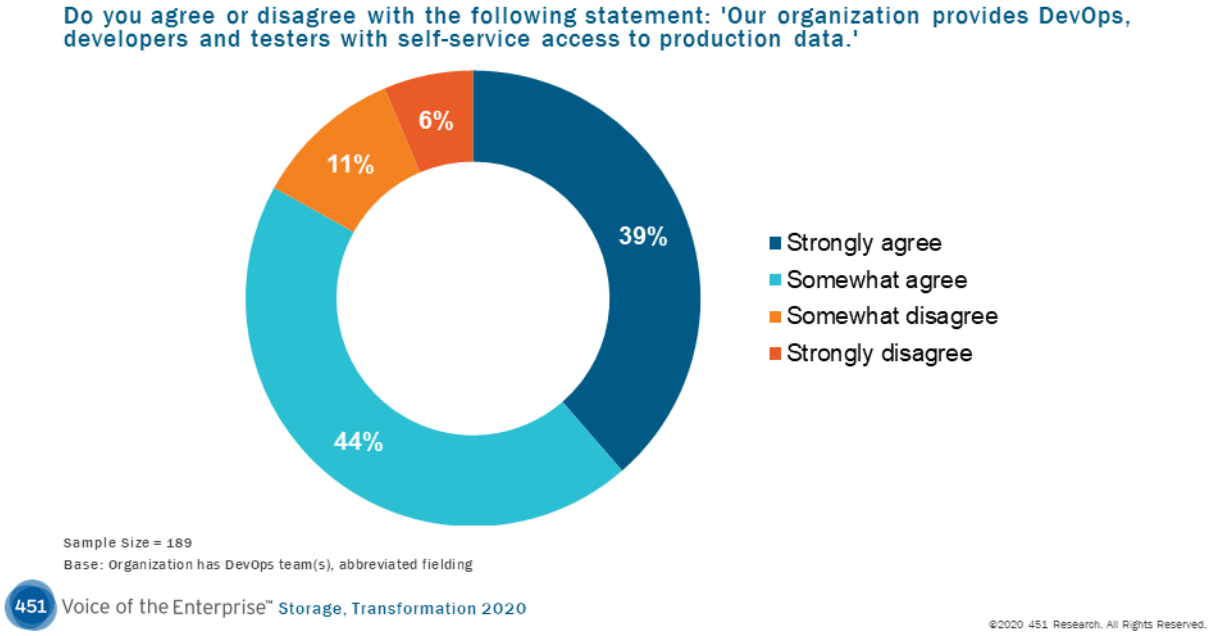
The desire to satiate the ever-increasing hunger for data cannot come at the expense of exposing sensitive data. In our VotE: Storage, Transformation study, 31% of respondents reported that their organization was deemed responsible for releasing compliance- or personally sensitive data within the past three years. While most respondents in the study claimed that their organization was monitoring and preventing unauthorized access to compliance- and privacy-sensitive production data, there is clearly room for improvement. There is no shortage of tools available to provide data obfuscation using data masking, encryption and tokenization techniques, and we expect more tools will emerge – such as Amazon's S3 Object Lambda – to automatically redact data when its is retrieved from cloud storage.

Self-service access to production data is on the rise

In our VotE: Storage, Transformation study, 83% of respondents agreed with the statement that their organization was providing DevOps, developers and testers with self-service access to production data, with 39% strongly agreeing and 44% somewhat agreeing. Only 6% of respondents strongly disagreed, with an additional 11% somewhat disagreeing. In the study, larger organizations were less enthusiastic about providing self-service access to production data, with only 28% of organizations with over 1,000 employees strongly agreeing in contrast to 48% for those with headcounts under 1,000.

Figure 1: Most Are Looking to Provide Self-Service Access to Production Data

Source: 451 Research's Voice of the Enterprise: Storage, Transformation 2020



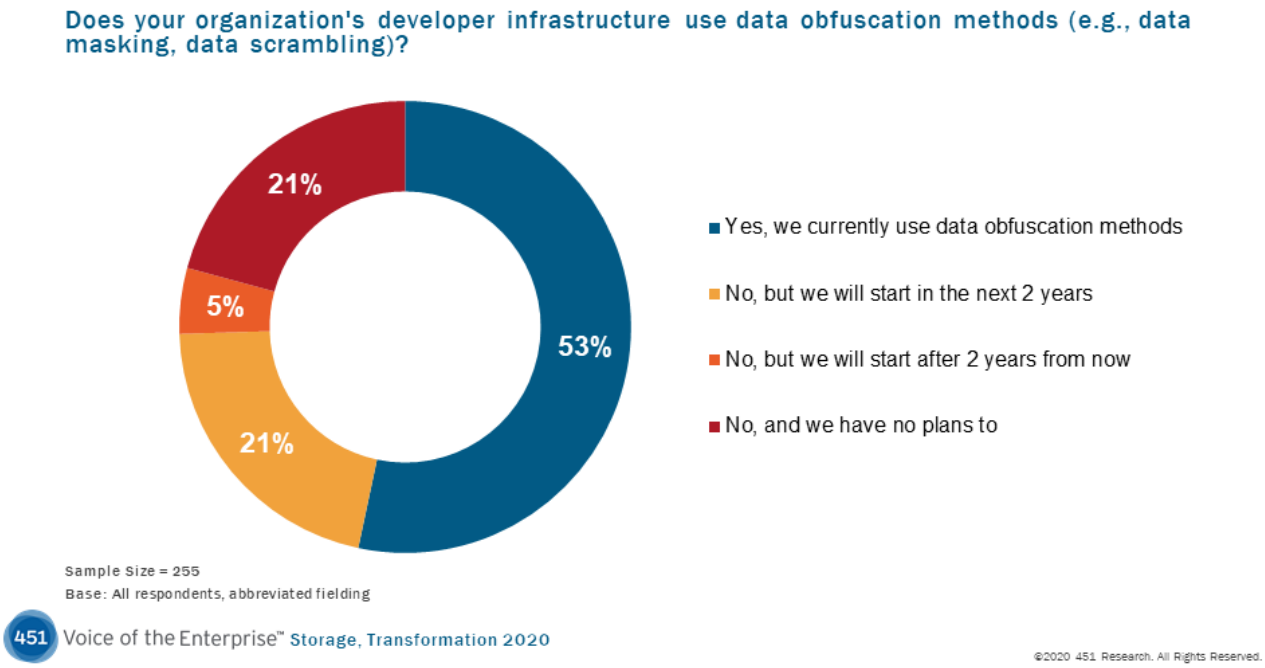
When asked about the monitoring and prevention of unauthorized access of compliance- and privacy-sensitive data for DevOps, developers and testers, 70% of respondents reported that they were currently protecting sensitive production data, with only 9% saying they had no plans to do so in the future (see Figure 1). Given that nearly one-third of respondents claimed to have been responsible for releasing compliance- or personally sensitive data in the past three years, there is clearly room for improvement.

Only half of respondents are using data obfuscation methods

In the study, 53% of respondents reported that they were currently employing data obfuscation methods to protect their organization's developer infrastructure, with an additional 21% planning to do so within the next two years (see Figure 2). Meanwhile, 21% of respondents in the study noted that they had no plans to use data obfuscation methods to protect their developer infrastructure. B2B software, IT and computer services had the highest percentage of respondents with data obfuscation methods in deployment at 76%, which was well ahead of respondents from finance (48%) and manufacturing (45%).

Figure 2: Adoption of Data Obfuscation Methods Is Rising

Source: 451 Research's Voice of the Enterprise: Storage, Transformation 2020



There are several methods for data obfuscation on the market today, including data masking, encryption and tokenization. Innovation continues to take place in this segment – for instance, startup ShardSecure is looking to disrupt by using its technology to split sensitive data into tiny pieces and distribute them across multiple locations so that the individual pieces are meaningless in the wrong hands, a process known as 'sharding.' ShardSecure is a potential alternative to data masking and data obfuscation offerings like BizDataX, IRI FieldShield, Privacy Analytics (IQVIA) and Solix, as well as larger firms with masking capabilities such as Broadcom (CA Technologies), Dataguise, Delphix, HPE, IBM, Imperva (Camouflage Software), Informatica, Microsoft (Blue Talon) Oracle and Protegrity.

In the recent announcement of Amazon's S3 Object Lambda, the vendor suggested that customers could leverage this capability to present multiple views from the same dataset, using Lambda functions to redact data based on the authentication rules created to control data access. Given that compliance remains a key concern for companies that are not willing to put their data in public clouds, the advent of capabilities such as S3 Object Lambda could allow these customers to integrate data obfuscation functionality into their cloud computing environments.