THE EXPLAINER

DYNAMIC DATA MASKING AND MONITORING

01

DYNAMIC DATA MASKING CLOAKS DATA

As the name implies, dynamic data masking actually masks data. Just as protective masks have obscured people's smiles (and frowns) during the pandemic, this data protection method covers sensitive data. People who shouldn't see the data won't see it.

02

IT DOESN'T ALTER DATA; IT SIMPLY PROTECTS IT

Also known by its shorter acronym DDM, dynamic data masking doesn't alter, in any way, the sensitive data that's in need of protection. The data is still there. Unlike, say, tokenization, another form of data protection, DDM doesn't substitute the data with a non-sensitive token. It simply masks the sensitive data. The data remains in its original form.

03

IT'S NOT THE BEST PROTECTION METHOD BUT IT'S EFFECTIVE

Although not as comprehensive or as strong as tokenization or other data-protection methods, DDM still does the job. It's effective when nothing more than low-level protection is needed, like masking the street addresses of individuals in a column of a larger dataset. Organizations might want to conceal the addresses only with DDM because it's quick to apply and that information, when in a bigger dataset, won't reveal any identifying details about people.

04

DDM CAN BE COUPLED WITH MONITORING

Data monitoring is yet another data protection method, and it's ideal to apply in tandem with DDM. Like data masking, monitoring can safeguard less sensitive data, such as the city and state of a person's address — data that does not map to a specific person but when pieced together with other unprotected data, could allow for a hacker to identify individuals. When organizations monitor data, they're usually performing transactional auditing to provide context as to who is accessing data, which data they're accessing, and how it is being accessed.

05

DDM IS JUST ONE TOOL IN A BIG PROTECTION TOOLBOX

Dynamic data masking and data monitoring alone will not help organizations safeguard sensitive data and preserve the privacy of customers, partners, and employees. But when businesses use a ***data protection platform*** that offers DDM and monitoring along with a robust array of data protection methods — tokenization, encryption, anonymization — they are demonstrating they understand the complexity of data protection. They're proving to customers that they're effectively aligning a protection method with the level of data sensitivity. For example, a business can choose to mask a customer's street, monitor city and state, and tokenize the name and Social Security Number (SSN)/National Identification Number (NIN). This allows less sensitive data such as city and state to be available for analytics, without the need to de-tokenize before use, while the highly sensitive name and SSN/NIN data elements are replaced by tokens and therefore remain useless to bad actors. Data is simultaneously protected and available to provide valuable business insights.

PROTEGRITY

For more information, visit **www.protegrity.com**