the Explainer: Five Ways to Stop Ransomware

1. KNOW WHAT KIND OF SENSITIVE DATA YOU HAVE AND WHERE IT IS

Data is kinetic; it's everywhere and never stops coming. It's often created through new business processes and applications in the cloud and on-premises systems that can go unnoticed in larger data-discovery efforts. You can't protect what you don't know you have. That's why it's critical to rely on a data-protection platform that corrals all your data so you can determine what's sensitive. When data is properly categorized as sensitive or non-sensitive, then you can decide which data-protection method best aligns with the level of sensitivity, which is often shaped by regulations governing data privacy.

2. DECIDE WHO NEEDS TO SEE WHICH DATA

Data access can get out of whack when your organization freely grants access because it is concerned business functions will otherwise slow. Imbalance also happens when your organization grants hardly any access–a measure that does slow business progress. A data-protection platform can help you achieve a healthy balance. But not just any platform. It must be one that keeps your organization compliant with current regulations and prepares you to handle future regulations. When evergreen compliance weaves privacy into the fabric of your organization, secured sensitive data will always fuel innovation.

3. TOKENIZE YOUR DATA

There are other data-protection methods, including encryption, anonymization and dynamic data masking. But tokenization is often chosen by businesses that want to protect data while also preserving its format and length, so that it can be easily used in analytics. Tokenization converts cleartext data into a random string of characters. Cybercriminals can do nothing with random characters, and, if anything, businesspeople that they are, they'll realize they've just wasted time freezing data that's worthless in their hands.

4. EMPOWER YOUR BUSINESS WITH PROTECTED DATA ANALYSIS

This goes back to achieving a proper balance. When your organization can consistently and effectively classify, discover, and safeguard data, authorized employees can freely access and share it because the sensitive elements are protected. When data-protection methods work in concert with policies that are centrally administered and enforced, data is compliant, secure, and can be shared, without hesitation, for data analytics and other business purposes.

5. DON'T WORRY ABOUT PAYING RANSOMWARE

You won't have to divert money into a rainy-day ransomware fund when your kinetic data is protected. Seize the moment and be an organization that won't make the news as the latest ransomware victim. When you always know which kind of data you have, where it resides, and which kind of data-protection method will best protect sensitive data elements, you will benefit from data insights–and cybercriminals will gain nothing. Let them have the worthless characters, while you let your kinetic data run free through AI-driven analytics and other business applications.

PROTEGRITY

For more information, visit www.protegrity.com