2019 CLOUD DATA SECURITY REPORT:
HEALTHCARE

netwrix

WHAT TYPES OF SENSITIVE DATA ARE STORED IN THE CLOUD?

32% store **all sensitive data** they have in the cloud

74% store healthcare data

74% store employee data

68% store customer data

WHAT IS THE STATE OF DATA SECURITY IN THE CLOUD?

26% had security incidents in the past 12 months

100% of these organizations never **classified all data** they store in the cloud

ALL these organizations store 100% **of their sensitive information** in the cloud

HOW DO ORGANIZATIONS PLAN TO STRENGTHEN DATA SECURITY IN THE CLOUD?

70% are planning to start **encrypting** data

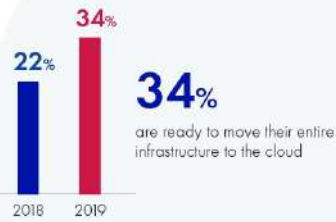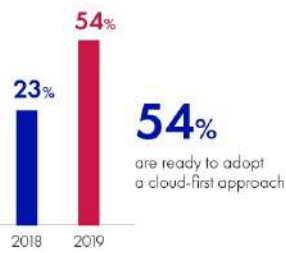**50%** want to start **monitoring activities** around data

44% will be enforcing stricter **security policies**

WHAT ABOUT BUDGET TO SUPPORT CLOUD SECURITY INITIATIVES?

85% did not see an increase in their cloud security budgets in 2019

30% say that they **do not get financial support** for cloud security initiatives from their management

WHAT ARE THE TRENDS IN USING CLOUD SERVICES?

23% 2018
54% 2019

54% are ready to adopt a cloud-first approach

22% 2018
34% 2019

34% are ready to move their entire infrastructure to the cloud

18% of healthcare organizations would consider **moving data back** on premises

TOP 3 REASONS TO UNCLOUD

56% Security concerns

22% Reliability and performance

22% High costs

TOP 3 TYPES OF DATA TO MOVE BACK FIRST

33% Healthcare data

33% Customer data

11% Employee data