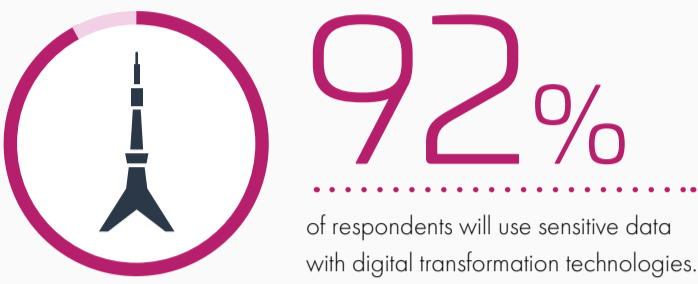# THALES

The Changing Face of Data Security in Japan

2019 Thales Data Threat Report – Japan Edition

Results from the 2019 Thales Data Threat Report - Japan Edition. The report concentrates on the results from 100 respondents in Japan with responsibility for, or influence over, IT and data security from within a total survey set of 1200 respondents around the world. Survey, reporting and analysis conducted by IDC and sponsored by Thales.
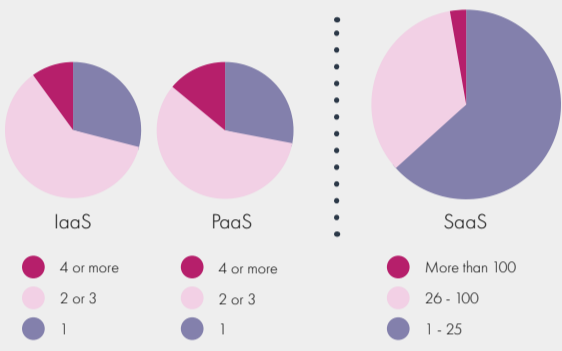
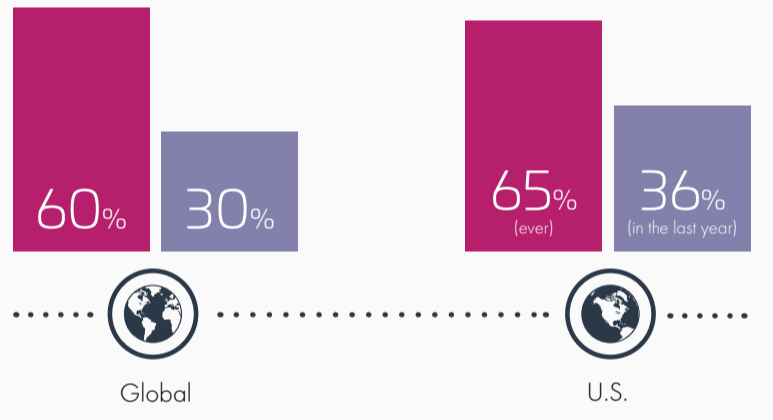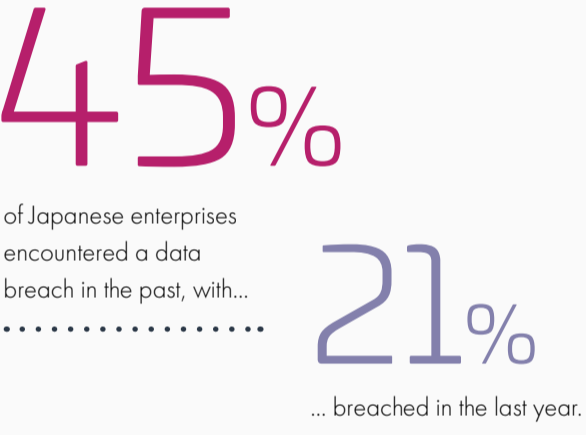## Sensitive data is widespread in digital transformative environments

92%
of respondents will use sensitive data with digital transformation technologies.

33% or less
are using data encryption within these environments today.

The reality of the multi-cloud enterprise

Multi-cloud environments make the task of protecting sensitive data more complex.
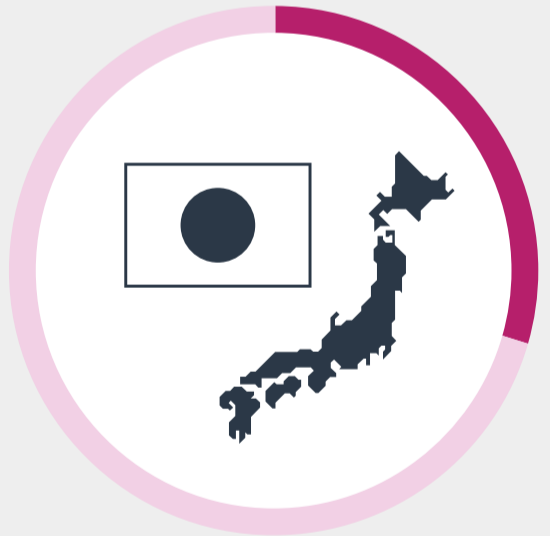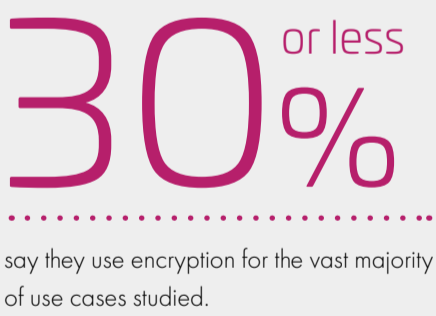
Number of cloud environments

IaaS
- 4 or more
- 2 or 3
- 1

PaaS
- 4 or more
- 2 or 3
- 1

SaaS
- More than 100
- 26 - 100
- 1 - 25

44%
are worried about security breaches and attacks at the cloud provider.

45%
recognise SaaS encryption with enterprise encryption key management as a top solution to SaaS data security problems.

Nearly half of Japanese enterprises encounter a data breach

45%
of Japanese enterprises encountered a data breach in the past, with...

21%
... breached in the last year.

60% **30%**
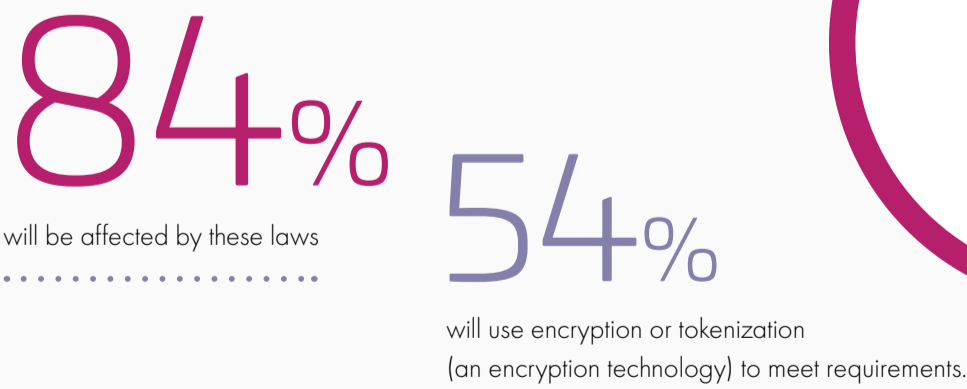Global

65% (ever) **36%** (in the last year)
U.S.

Encryption rates are low

Despite recognizing the importance of protecting sensitive data, encryption rates throughout enterprises are surprisingly low.

30% or less
say they use encryption for the vast majority of use cases studied.

Data privacy and sovereignty regulations

With the impact of APPI and over 100 data privacy regulations already in place around the world:

84%
will be affected by these laws

54%
will use encryption or tokenization (an encryption technology) to meet requirements.

Data Security doesn't have to be hard

Organizations need to take a fresh look at how they provide data security. Visit the Thales website to download the full report, including IDC recommendations.

Follow us on: