

The Data Dilemma

COVID-19 has forced many organizations to reassess and accelerate their digital transformation strategy in order to adapt to the 'new normal'.

A global study by Trend Micro shows the increase in cloud adoption may leave business data insecure.



2,556
decision makers
28
countries



88%
of organizations surveyed **confirmed** that the pandemic has **accelerated** their cloud migration, yet only **55%** are **adding security** to protect it

Cloud security confidence is high



51%
of decision makers claim the acceleration in cloud migration has **increased their focus on security best practices**



87%
believe they are **in control** of securing their remote work environment



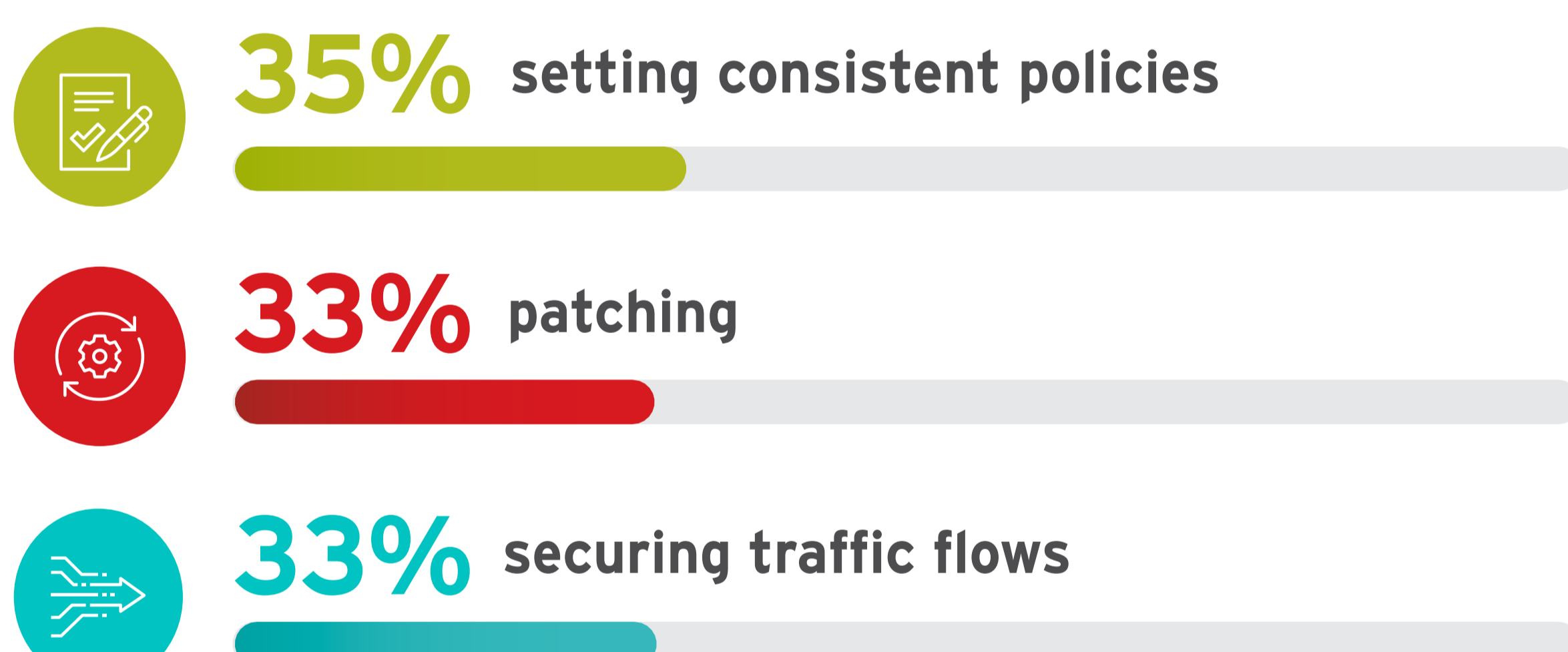
83%
believe they will be **in control** of securing their future hybrid workplace

Confidence may be high, but there are challenges

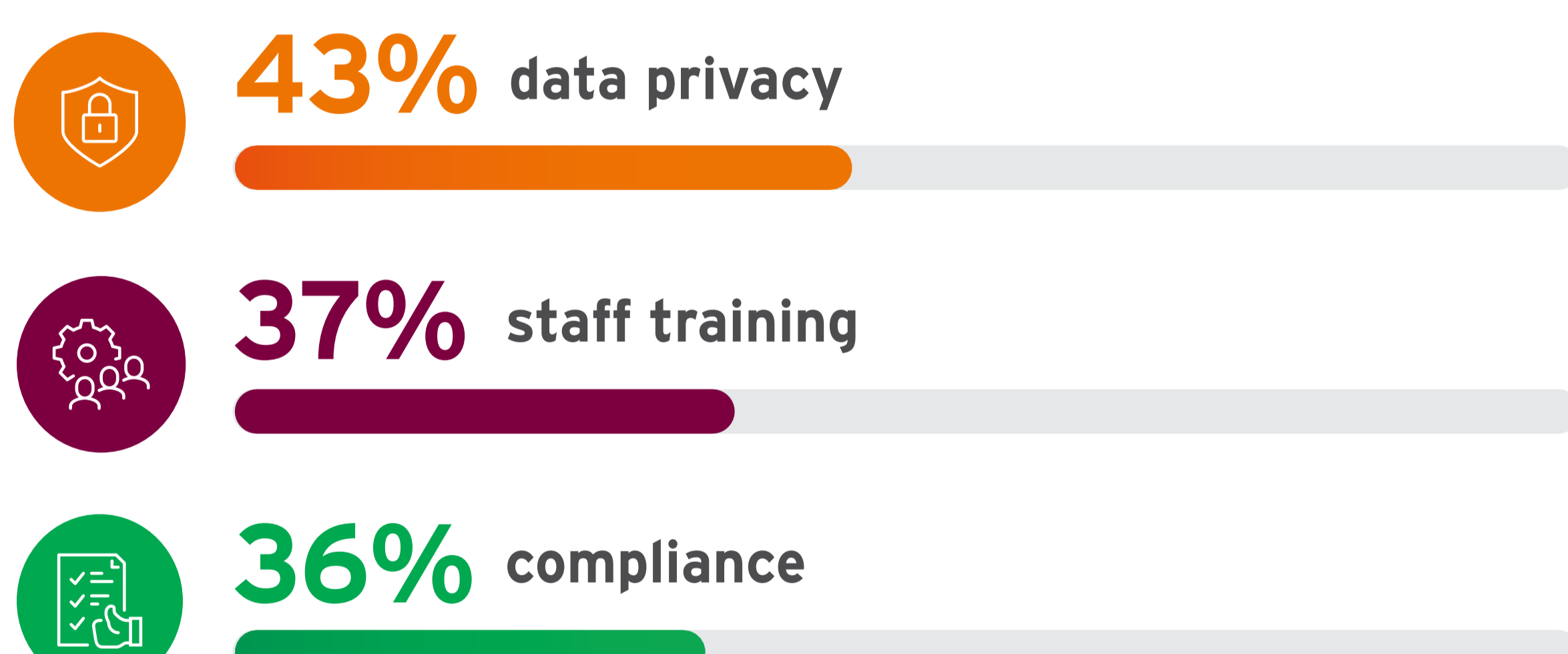


Security remains a significant barrier to cloud adoption for almost half of respondents (**45%**), with concerns that potential coverage gaps might be exploited

The largest day-to-day operational headaches of protecting cloud workloads are:



The most significant barriers in migrating to cloud-based security tools are:



Who is responsible for your security?

Organizations have a misconception that their Cloud Service Provider (CSP) not only protects the cloud infrastructure, but also company data



92%
are **confident** they understand their cloud security responsibility, but **97%** believe their CSP offers sufficient data protection



55%
of respondents **use third-party tools** to secure their cloud environments

While many organisations around the world are embracing and adopting the cloud, there is still a lack of understanding around how to secure it.

Trend Micro's global study highlights the misconceptions that lead to serious security consequences and makes recommendations for best practice security decisions when it comes to cloud and cloud adoption.

