The Changing Face of Data Security

January 29, 2019
Sensitive data is widespread in digital transformation environments
97% of respondents will use sensitive data on digitally transformative technologies.
only 30% of respondents are using encryption within these environments.
The reality of a multi-cloud enterprise
Data environments are increasingly complex, with survey results showing complexity is the most commonly perceived barrier to implementation among respondents.
Number of cloud environments

- **IaaS**:
  - 1
  - 2 or three
  - 4 or more

- **PaaS**:
  - 1
  - 2 or three
  - 4 or more

- **SaaS**:
  - >10
  - 11-50
  - More than 50
This level of multi-cloud usage greatly compounds the difficulties that organizations have to face in protecting their **sensitive data**, as each environment, and often each implementation within the environment, can require a unique data security approach."

44% of respondents rated complexity as a perceived barrier to implementing data security, higher than staff, budget, and organizational buy-in.
Data breach resistance: no one is immune
60%

Say they have been breached at any point in their history, with...

30%

...experiencing a breach within the past year alone.
U.S has reported the most breaches.
Encryption rates are low
Despite recognizing the importance of protecting sensitive data, encryption rates throughout the enterprise are surprisingly low.
“For the most part, these are network and end-point protections, rather than the best solutions that are best for protecting sensitive data, data-at-rest and data-in-motion security tools.”

<30% of enterprises say they use encryption for the vast majority of use cases studied.
Encryption for Big Data, IoT and Containers adoption
Across Big Data, IoT and Containers, encryption is the key driver of adoption and usage.
IoT

42.3%
Containers

47.3%
Big data

45.3%
Data security is hard
But it’s vitally important. Organizations need to take a fresh look at how they provide data security.

Against this backdrop, analysts recommend that security professionals consider the following:
IDC Guidance / Key Takeaways

• Focus on all threat vectors.
• Look for solutions that let you do more with less.
• Prioritize compliance and sovereignty issues.
• Data security, starting with encryption, is an important part of the mix.
• Invest in modern, hybrid and multi-cloud-based data security tools and measures that scale to modern architecture.
Thank you to our Sponsors: