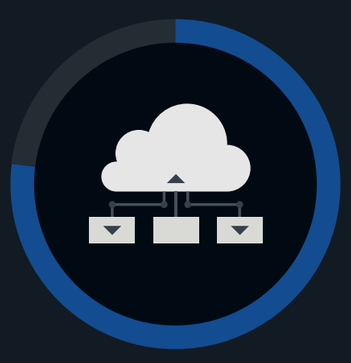
Enterprise Strategy Group™ by TechTarget

THE CLOUD DATA SECURITY IMPERATIVE

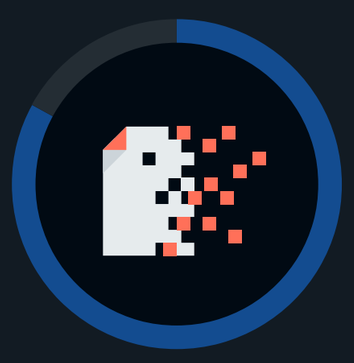
Digital transformation initiatives and remote work have further accelerated the migration of data assets to cloud stores. However, organizations are finding that sensitive data is now distributed across multiple public clouds. The use of disparate controls has led to a lack of consistent visibility and control, putting cloud-resident data at risk of compromise and loss. TechTarget's Enterprise Strategy Group recently surveyed IT, cybersecurity, and DevOps professionals in order to gain insights into these trends.

Notable findings from this study include:

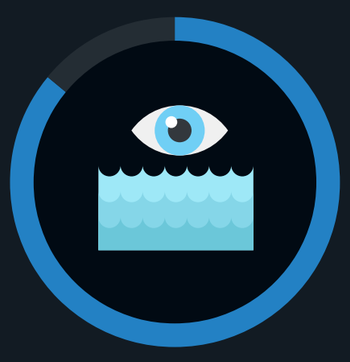
59%
of organizations believe that more than 30% of their sensitive IaaS/PaaS cloud-resident **data is insufficiently secured.**



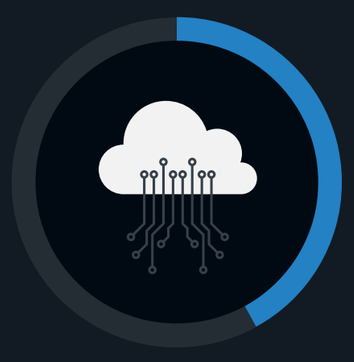
77%
of organizations currently store sensitive data in more than one IaaS/PaaS platform.



83%
of organizations have experienced multiple data loss events involving sensitive cloud-resident data in the past 12 months.



86%
of organizations say they have sensitive data stored in a data lake, data warehouse, or data lakehouse.



42%
of organizations say they have lost cloud-resident sensitive data from SaaS applications.

54%
of organizations believe that on-premises data security is more effective than public cloud infrastructure/application data security.

64%
of organizations use a combination of third-party and CSP-native data security controls.

For more from this Enterprise Strategy Group study, read the full research report, *The Cloud Data Security Imperative.*

LEARN MORE

Source: Enterprise Strategy Group Research Report, *The Cloud Data Security Imperative,* May 2023.