

# Cloud Security Made Easy

With the cloud driving digital transformation, securing cloud environments means securing the potential for growth. As organizations adopt cloud-based services at a record pace, they are also responsible for protecting a larger attack surface that comes with new security and operational challenges.



# 31%

of organizations surveyed in **June 2022** experienced a security incident in the cloud in the last 12 months

Source: Fidelis 2022 AWS Cloud Security Report



# 95%

of security professionals are moderately or extremely **concerned** about the security of public clouds

Source: Fidelis 2022 AWS Cloud Security Report



CrowdStrike and AWS work together to ensure complete protection of your workloads and infrastructure, keeping you secure on your cloud migration journey.



The most common causes of cloud breaches are human errors and omissions introduced during common administrative activities. Organizations tend to grant employees more access and permissions than they need to do their jobs, which increases identity-based threats.

# 83%

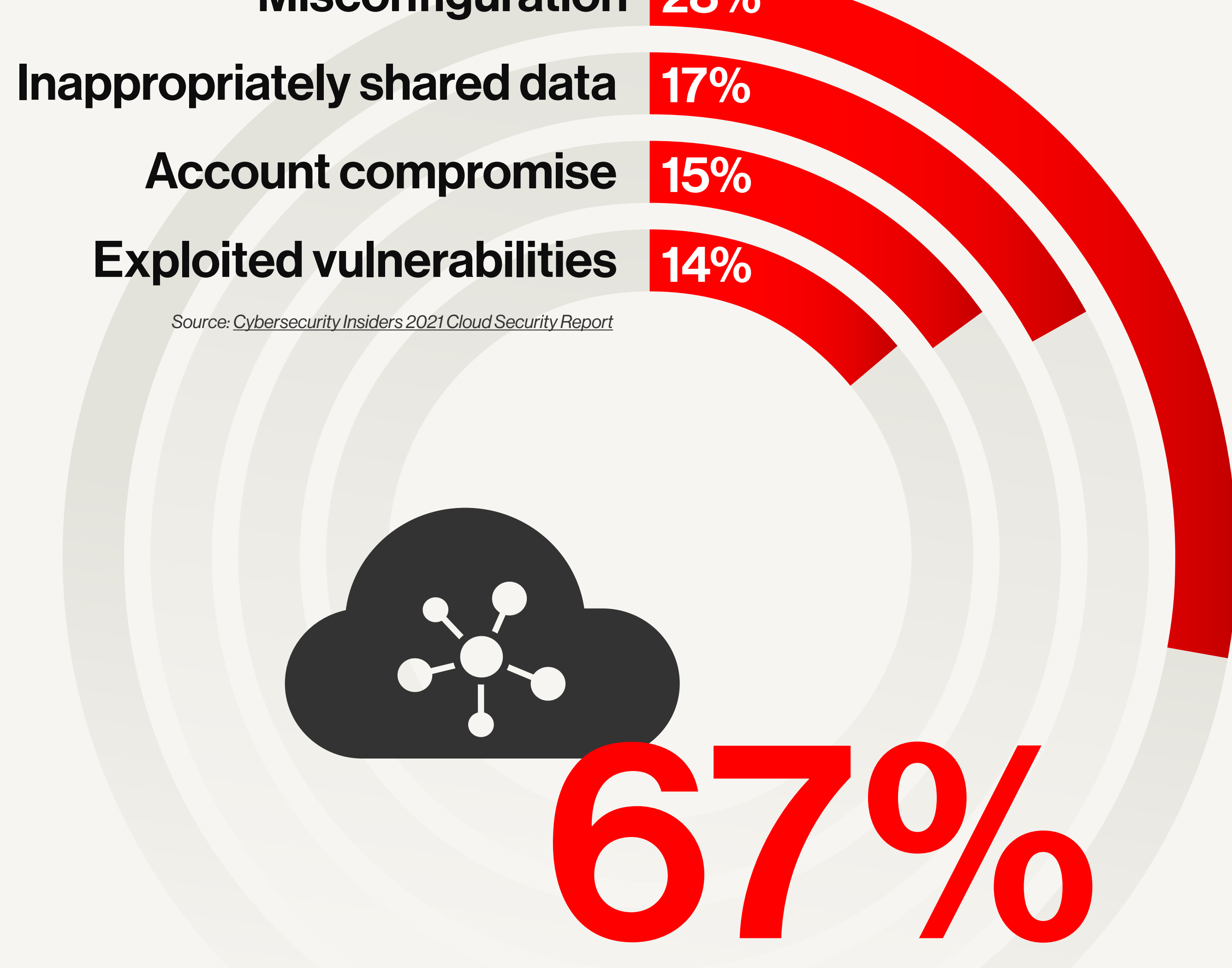


of survey participants said at least one of the **cloud data breaches** they experienced in the past 18 months was related to access

Source: IDC State of Cloud Security 2021

Moving quickly can make applications susceptible to misconfigurations — the #1 vulnerability in cloud environments. Misconfigured access policies often escape security audits and increase the likelihood of breaches.

## Causes of Cloud Incidents



Source: Cybersecurity Insiders 2021 Cloud Security Report

# 67%

of surveyed cybersecurity professionals said that **cloud security misconfiguration** is the biggest cloud security risk

Source: Cybersecurity Insiders 2021 Cloud Security Report

## Protecting Against Cloud Breaches Is a Shared Responsibility

Moving to the cloud without understanding the security and compliance implications increases risk and potentially opens the door to attackers. The shared responsibility model clears up risky gray areas by delineating security obligations for cloud service providers and their customers.

# 8%

of IT executives and cybersecurity professionals surveyed said they fully understand the **shared responsibility** security model across all types of cloud services

Source: Oracle and KPMG Cloud Threat Report 2020

Put simply, the shared responsibility model dictates that the cloud service provider is responsible for securing the cloud itself, while end users are responsible for securing data and other assets they store in the cloud.

CUSTOMER Responsibility for Security "In" the Cloud	Customer Data			
	Platform, Applications, Identity and Access Management			
	Operating System, Network and Firewall Configuration			
	Client-Side Data Encryption and Data Integrity Authentication	Server-Side Encryption (File System and/or Data)	Network Traffic Protection (Encryption, Integrity, Identity)	
AWS Responsibility for Security "Of" the Cloud	Software			
	Compute	Storage	Database	Networking
	Hardware/AWS Global Infrastructure			
	Regions	Availability Zones	Edge Locations	

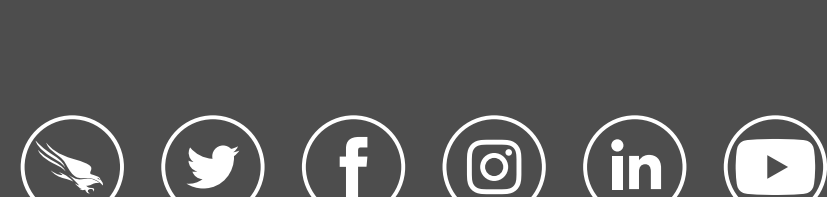


**CrowdStrike Falcon Protects Your Workloads Running on AWS**

**AWS Protects Your Cloud Infrastructure**

When you trust CrowdStrike cloud security solutions to protect your data, you can expect unified cloud security posture management with breach protection for workloads and containers in AWS and hybrid environments. This means you can build safely in the cloud with speed and confidence in complete protection.

Follow us:



© 2022 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are marks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.