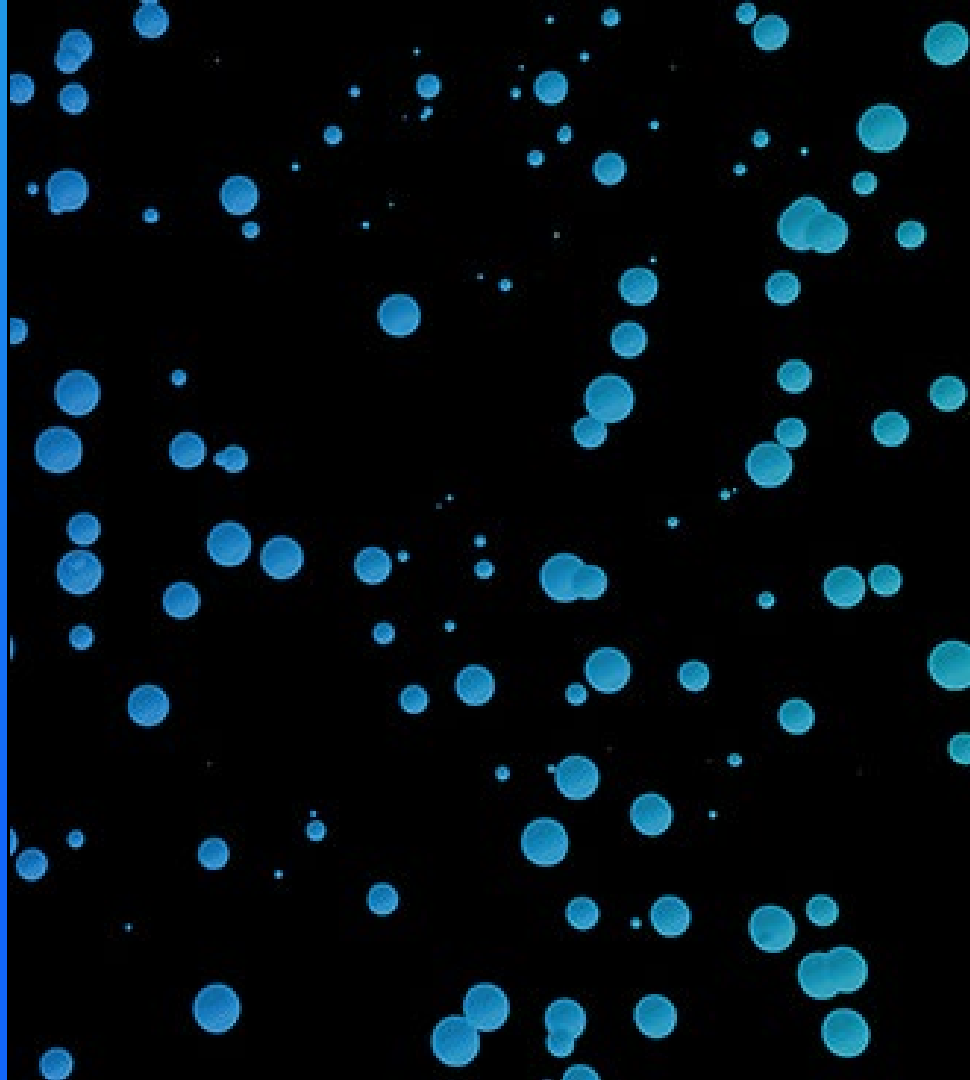
Security **For**, **From** and **In** the Cloud:

Tales from the Front Lines

Cyber Implications in Cloud Migrations

Bob Kalka, CRISC
Vice President, IBM Security
bkalka@us.ibm.com
Austin, Texas

IBM



Cyber Implications in Cloud Migrations

Cloud Security:

For?

From?

or **In?**

- Current State
- Macro Dynamics: A Risk-Based View
  - Organizational
  - Technological
- Micro Dynamics: The Shared Responsibility Model
  - Controls
  - Threat Management
  - Digital Trust

Current state of cloud migration

51%

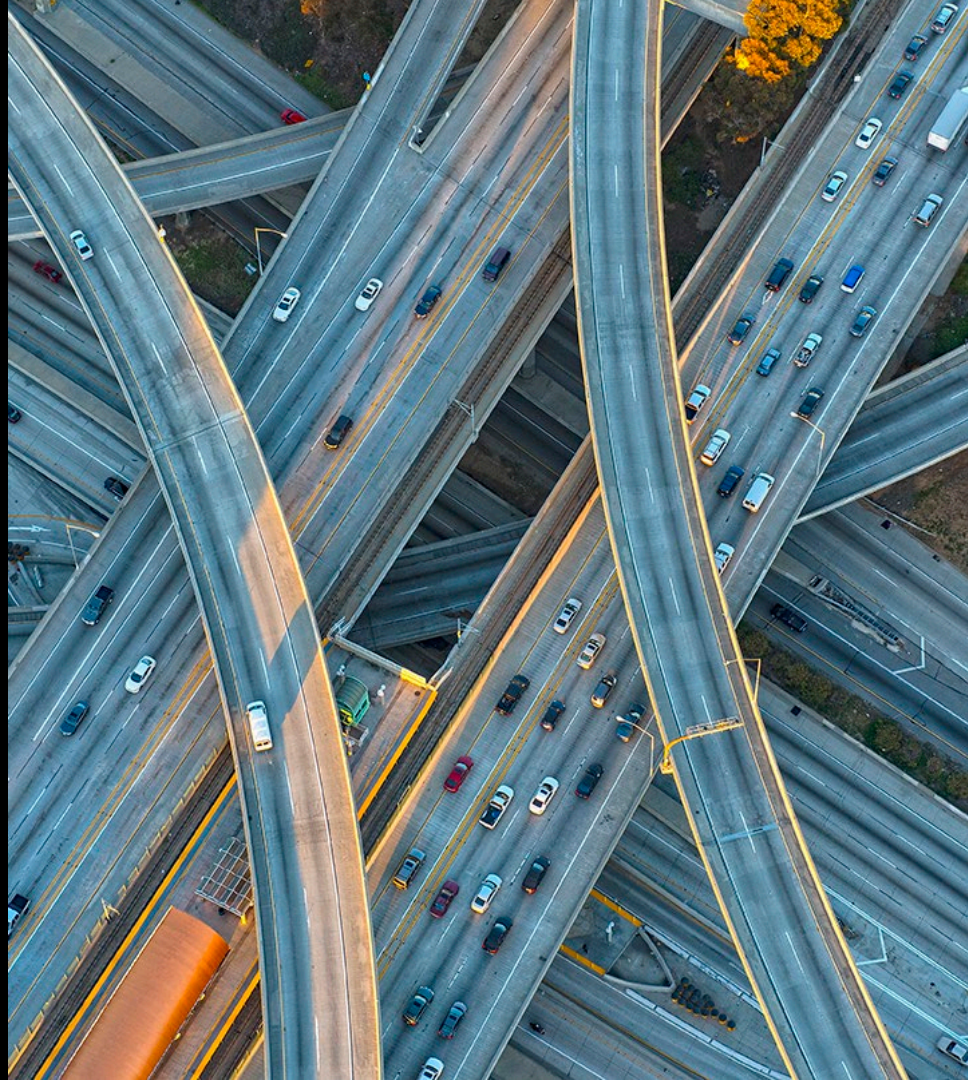
have publicly exposed at least one cloud storage service

Only 7%

have good visibility of all critical data

49%

of databases are not encrypted



Current state of cloud migration

73%

have not implemented a privileged account solution for DevOps

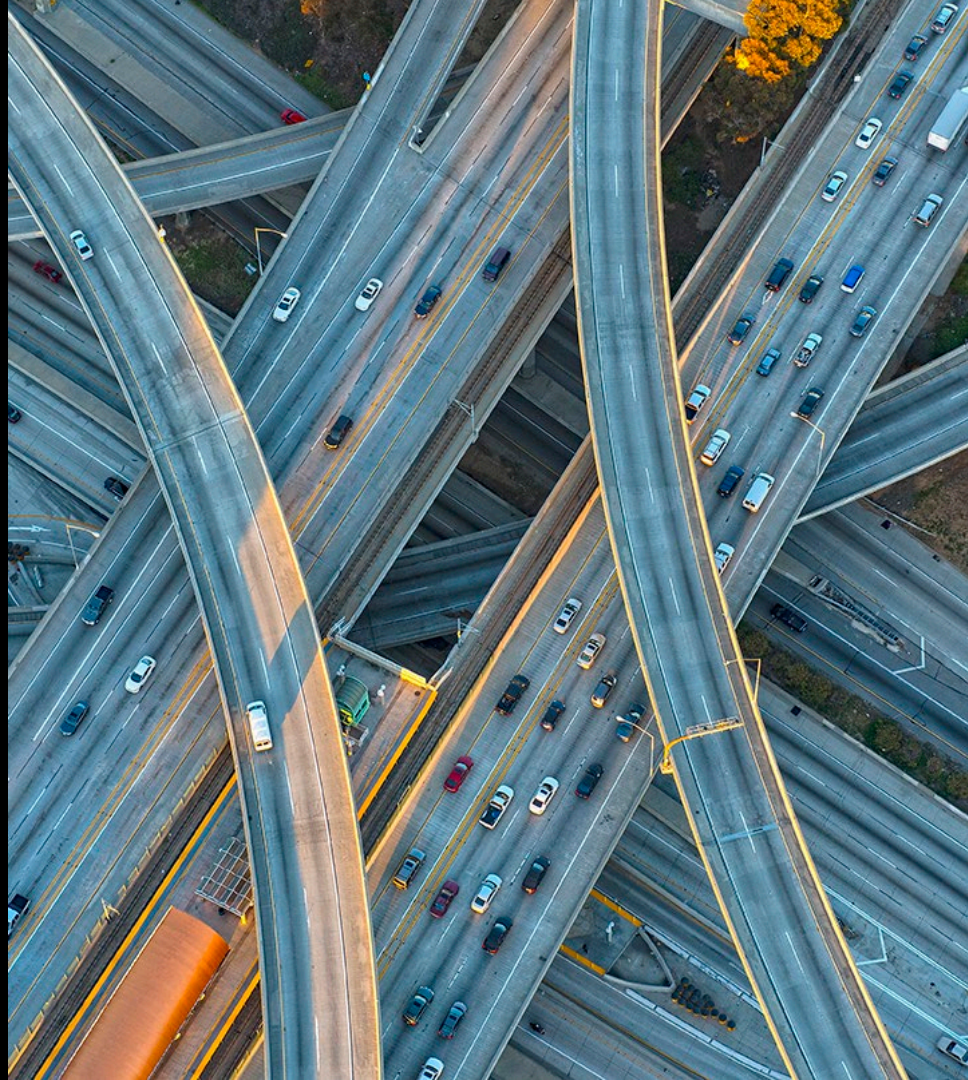
80%

of security breaches involved privileged credentials

Current state of cloud migration

24%

have hosts missing high-severity patches in the cloud



Current state of cloud migration

95%

of cloud security failures are predicted to be the customer’s fault, through 2022 (Gartner)

Taking a risk-based view of secure cloud migration

- Organizational
  - Proactive Cyber Involvement

    vs. “we shift – they will secure”
  - Employee training

Taking a risk-based view of secure cloud migration

- Technological
  - Workloads
    - Phase by level of risk (mission-critical)
    - Evaluate cost of migration (apps et al)
    - Limiting access between services
    - Sprawl (especially migrating from private cloud)
    - Provider Lock-in

Taking a risk-based view of secure cloud migration

- Technological
  - Data
    - Identify and locate ‘crown jewels’ data
      - the new perimeter…
      - including pre-existing dispersion
    - Evaluate latency issues with access to some data
    - Increased complexity for staff, e.g. encryption and key management
    - Multi-tenancy

The shared responsibility model

- Controls
  - Default cyber policies, configuration and monitoring
  - SLAs: frequency and depth
  - Compliance -> Risk Management

The shared responsibility model

- Threat Management
  - Find, Confirm, Fix…and Federate

- Digital Trust
  - Right User, Access, Data and Reason

② THREAT MANAGEMENT

CP4S

Find

[redacted]

Confirm

[redacted]

CONNECT

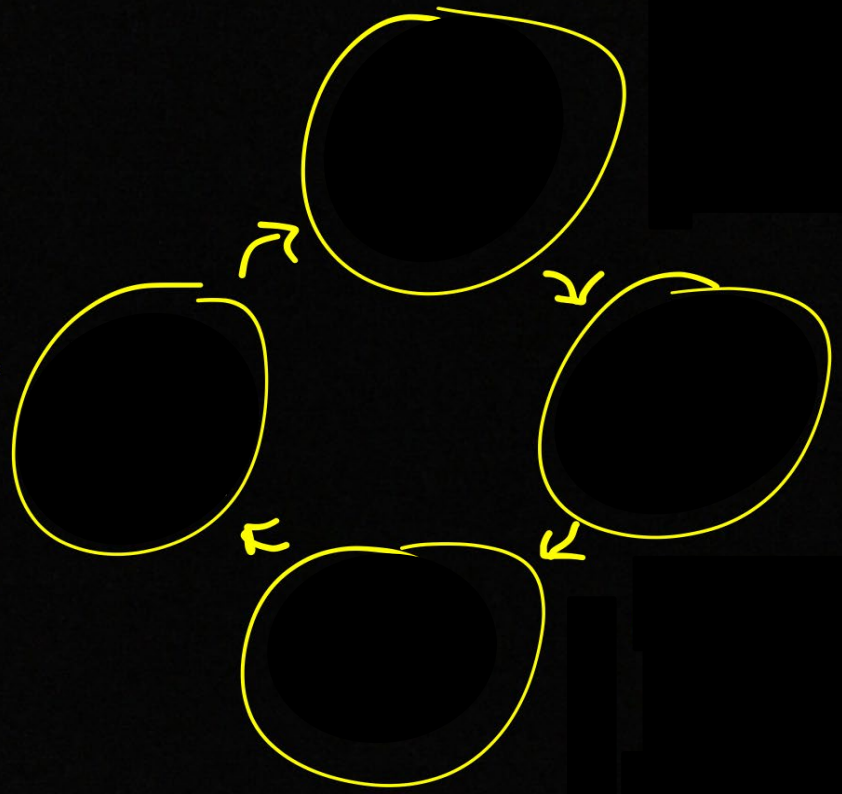
Fed Search

Fix

[redacted]

Ⓐ

3 DIGITAL TRUST



Thank you