State of Cloud Security

Presented by- Nielet D'mello

SONOMA STATE UNIVERSITY

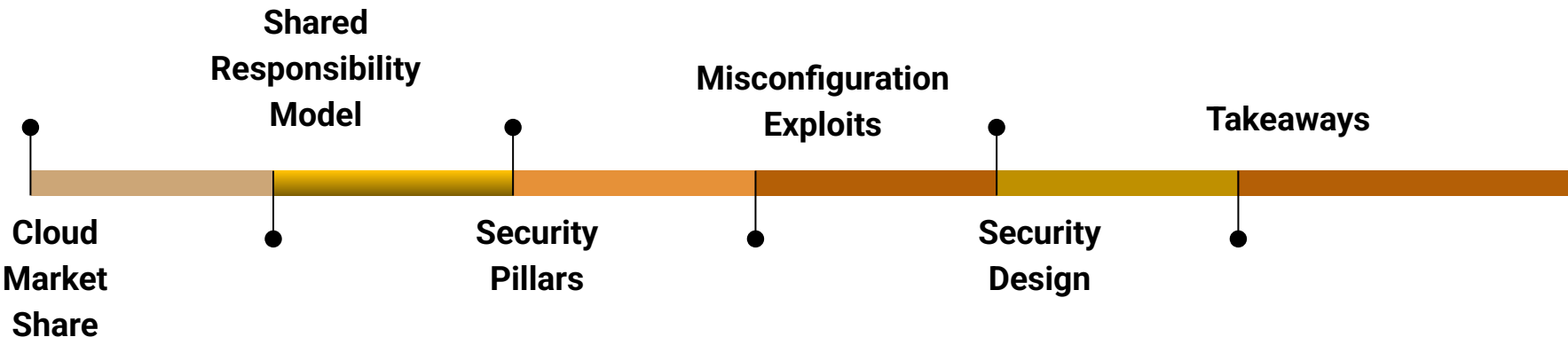
Legal Disclaimer

“All views, thoughts, and opinions expressed in the presentation belong solely to the speaker, and not necessarily to their employers, organizations, committees or other groups or individuals. ”

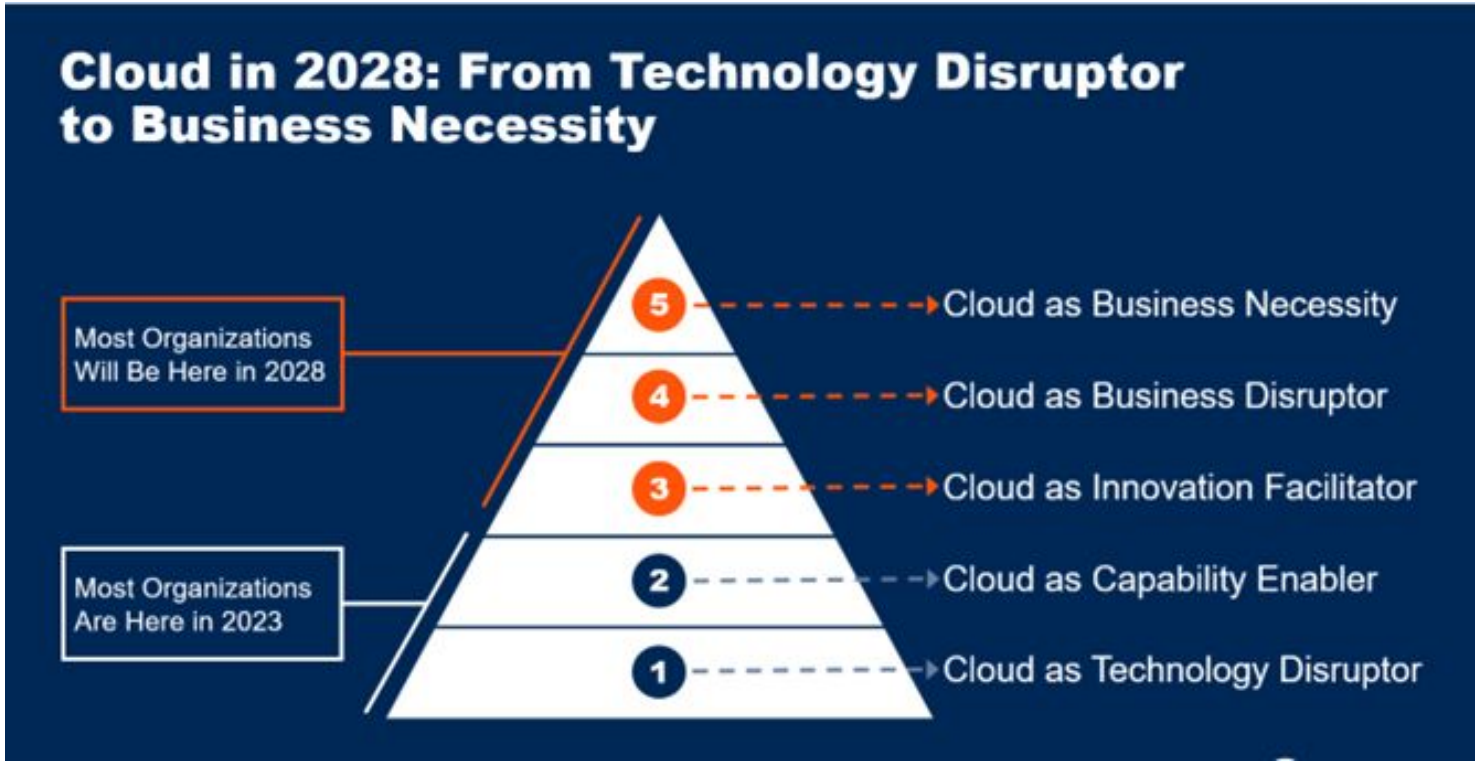
$ cat about_me

- Product & Application Security Engineer @ Datadog
- Previously:
  - Platforms & Infrastructure engineering @ Intel
  - Software engineer @ McAfee
  - Lecturer @ Polytechnic College
- Bachelor in Computer Engg/ Master of Science- Software Engg
- Passionate about Writing
  - The Pragmatic Engineer
  - O'Reilly- 97 Things Every Application Security Professional Should Know
  - Dark Reading
- STEM mentor @ SJSU
- Speaker @ national and international Cybersecurity conferences
  - OWASP AppSec Global USA 2023
  - DEFCON 31 AppSec Village
  - Day of Shecurity

Agenda


Cloud Market Share
Shared Responsibility Model
Security Pillars
Misconfiguration Exploits
Security Design
Takeaways

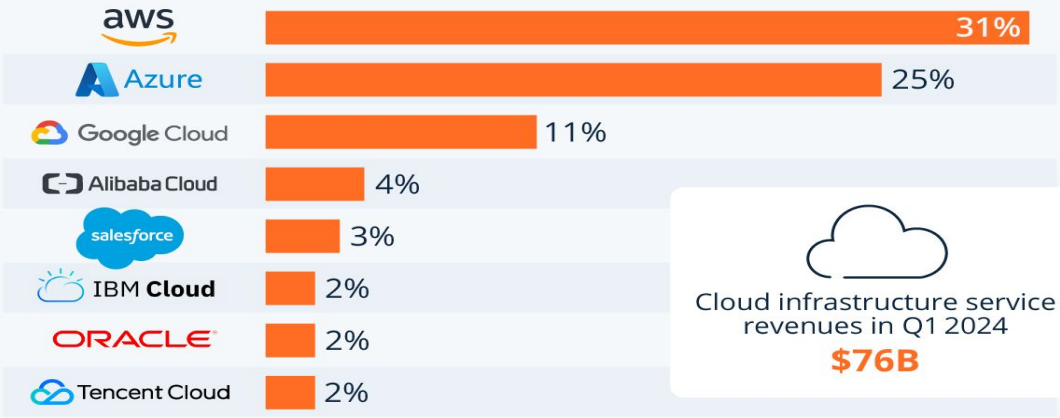
Cloud Market Share



Source: Gartner

Amazon Maintains Cloud Lead as Microsoft Edges Closer

Worldwide market share of leading cloud infrastructure service providers in Q1 2024*



Cloud infrastructure service revenues in Q1 2024

$76B

* Includes platform as a service (PaaS) and infrastructure as a service (IaaS) as well as hosted private cloud services

Source: Synergy Research Group

Security Breach Landscape - Not so uncommon

DARKReading

NEWSLETTER

The Edge | DR Tech | Sections | Events | Resources

Attacks/Breaches | 5 MIN READ | NEWS

Uber Breached, Again, After Attackers Compromise Third-Party Cloud

Threat actors leak employee email addresses, corporate reports, and IT asset information on a hacker forum after an attack on an Uber technology partner.

Security

CircleCI says hackers stole encryption keys and customers' secrets

Security

Reddit says hackers accessed employee data following phishing attack

BLEEPINGCOMPUTER

Home > News > Security

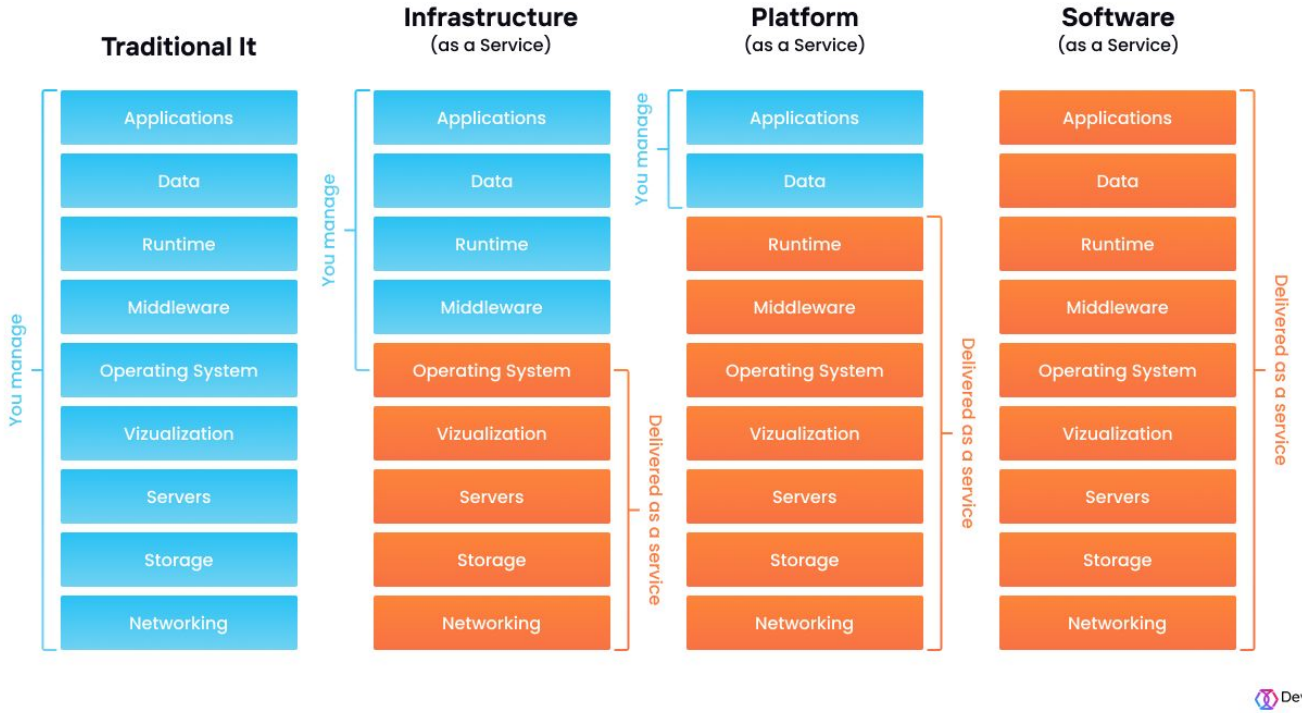
> T-Mobile hacked to steal data of 37 million accounts in API data breach

T-Mobile hacked to steal data of 37 million accounts in API data breach

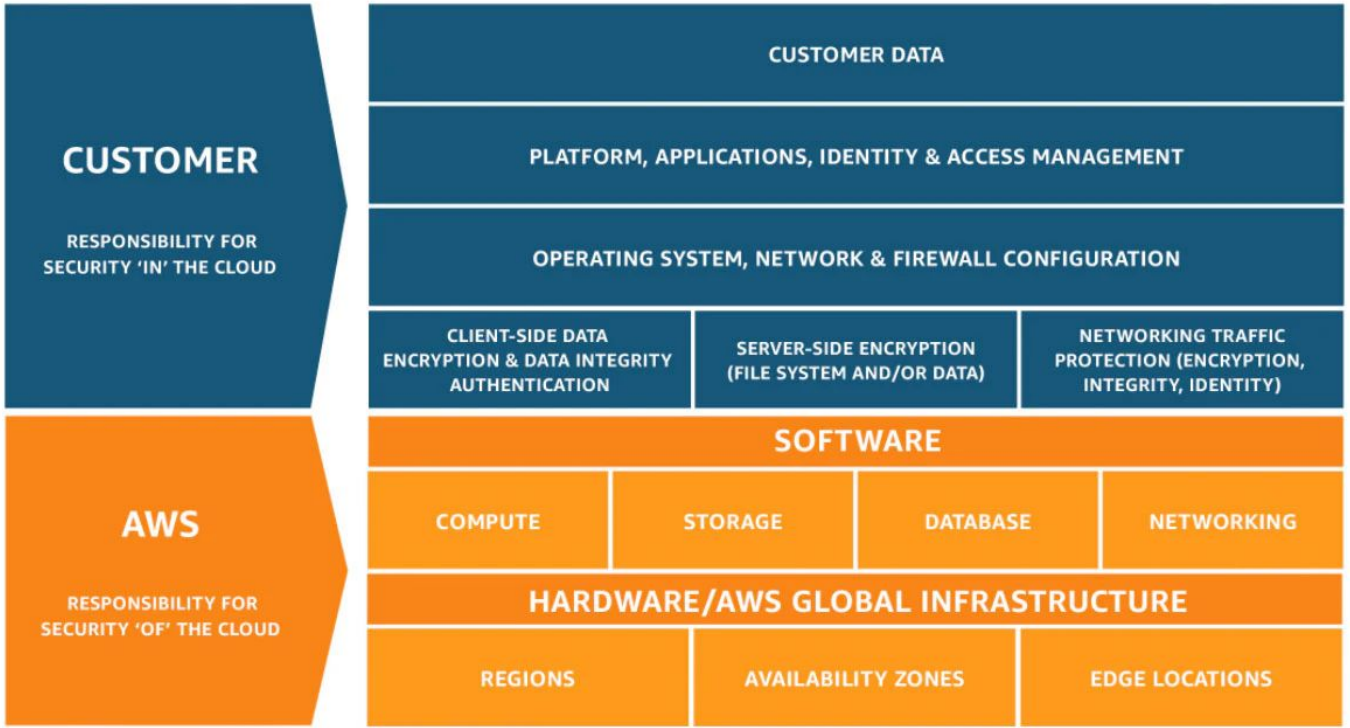
Shared Responsibility Model


WHAT IF I TOLD YOU
THE CLOUD IS JUST SOMEONE ELSE'S COMPUTER

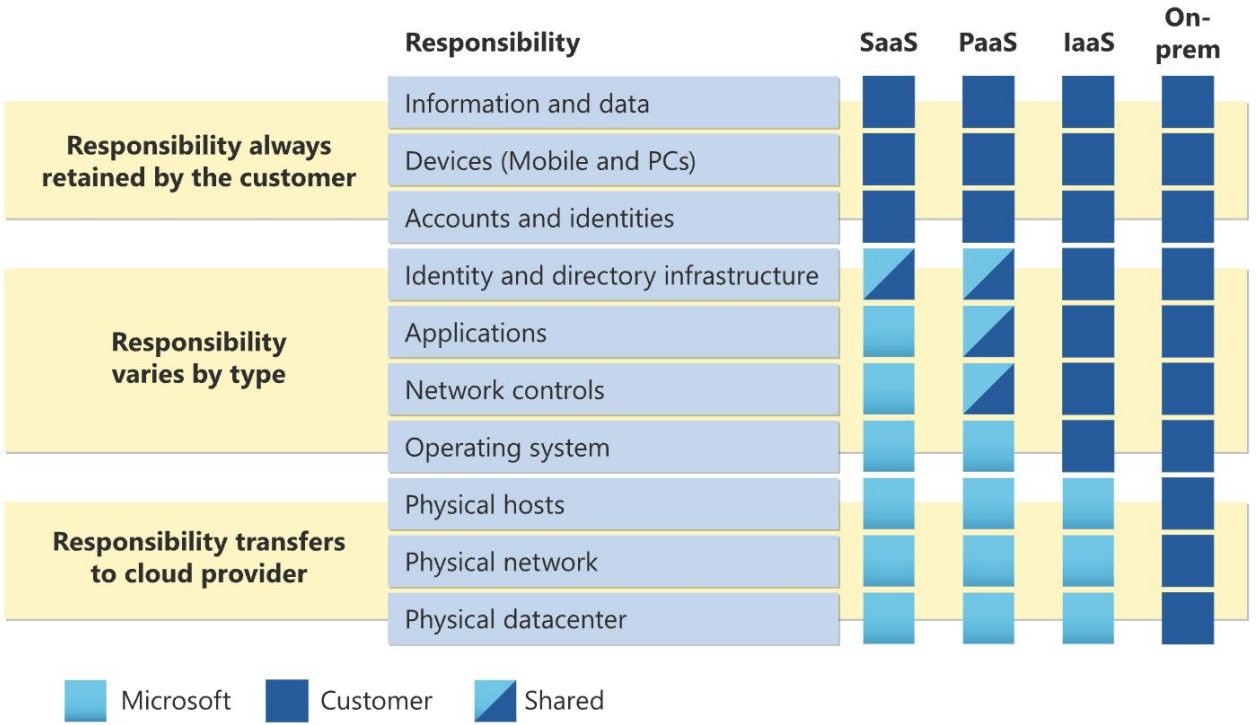
Cloud Models



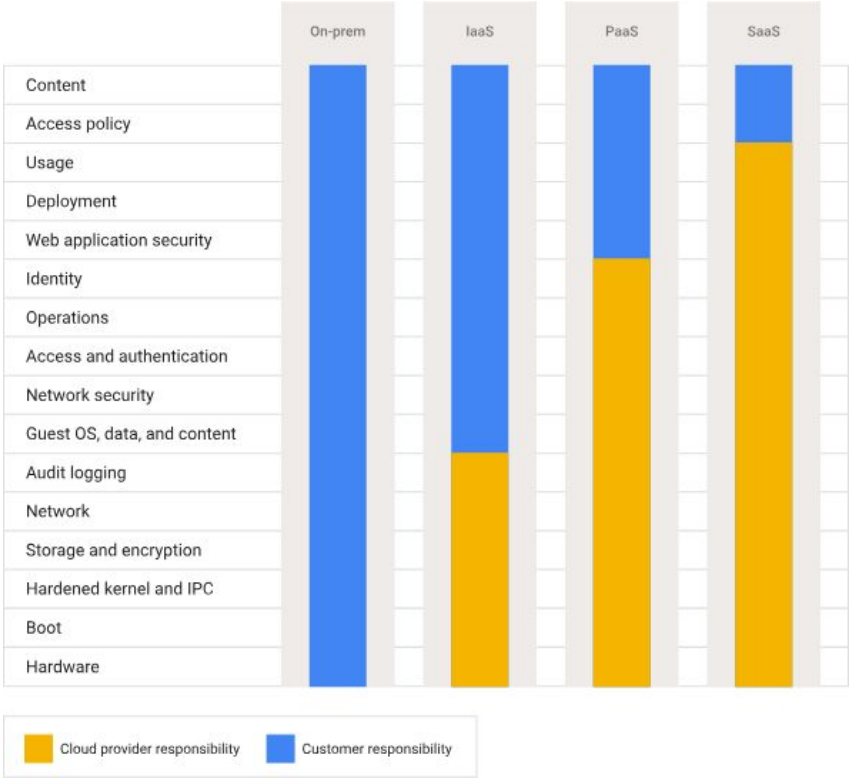
Amazon Web Services (AWS)



Microsoft Azure

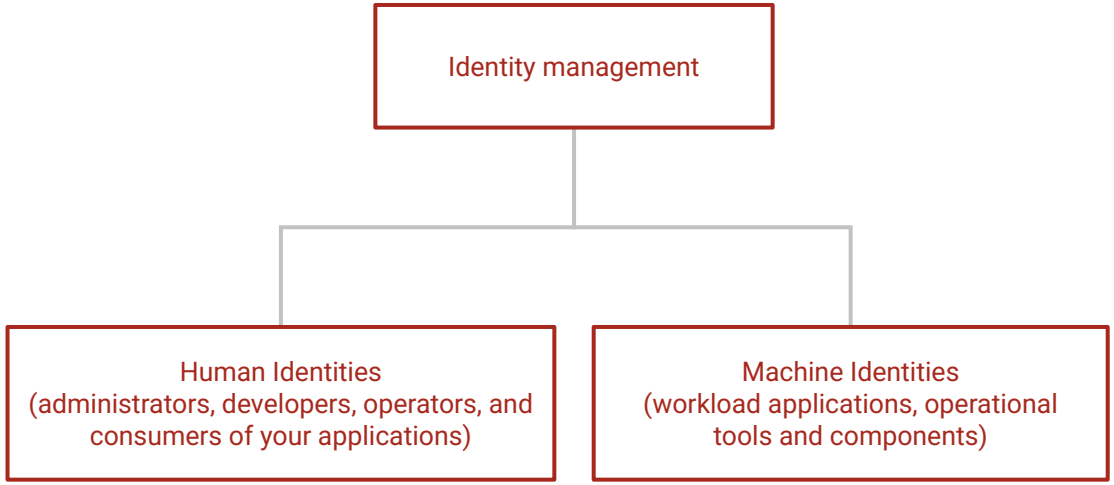


Google Cloud Platform (GCP)

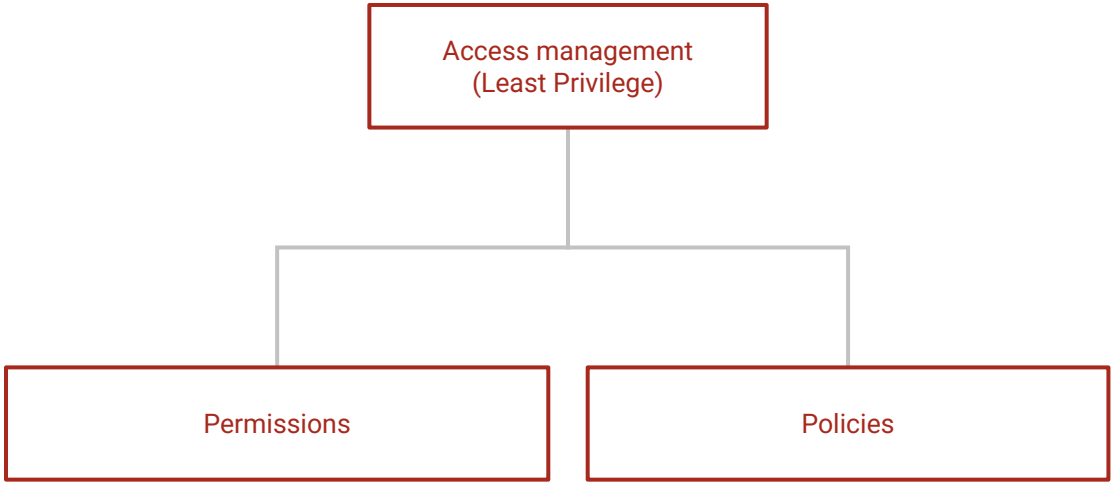


Security Pillars

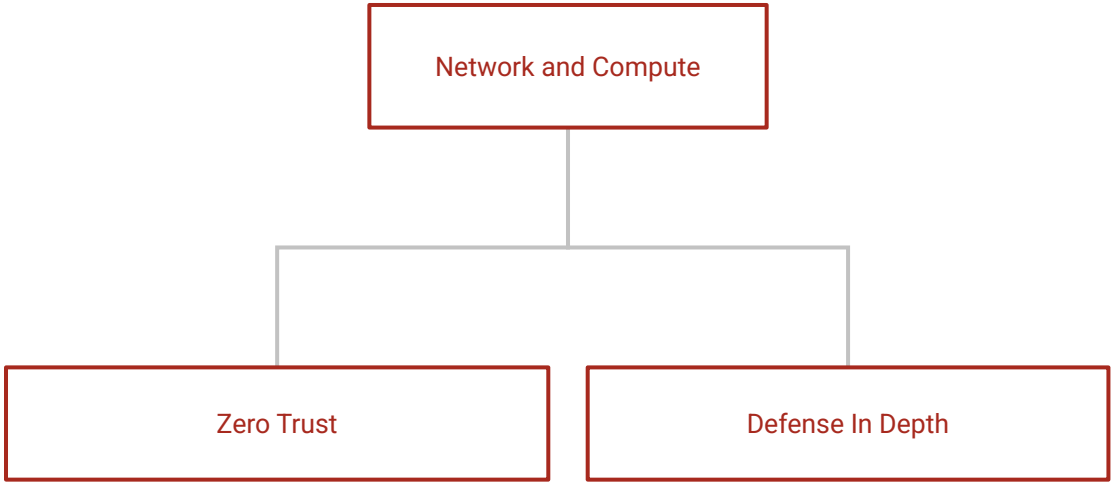
Identity and access management



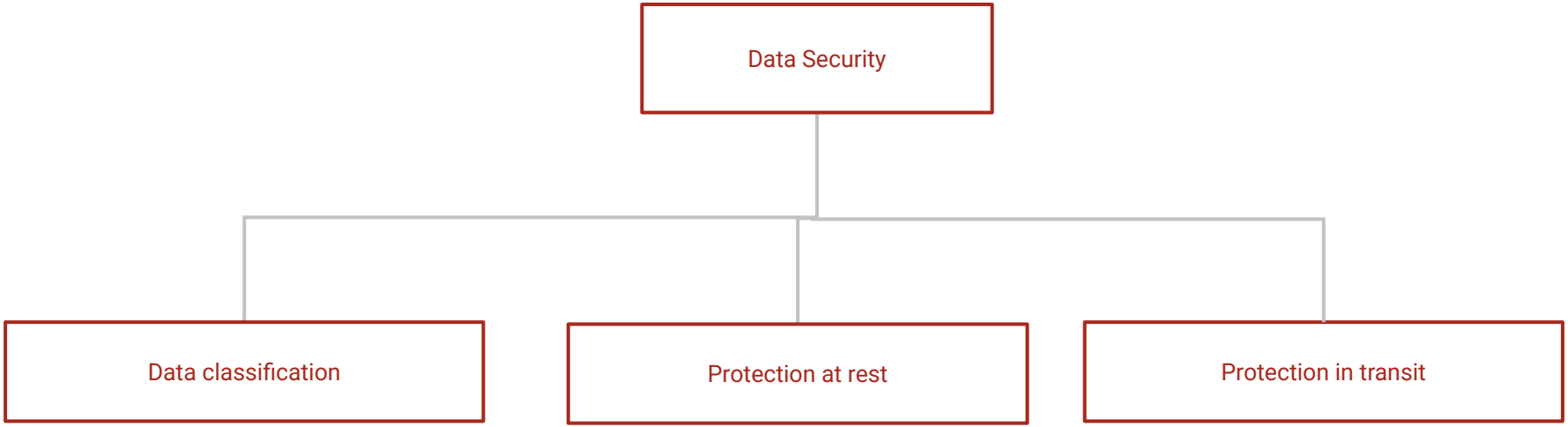
Identity and access management



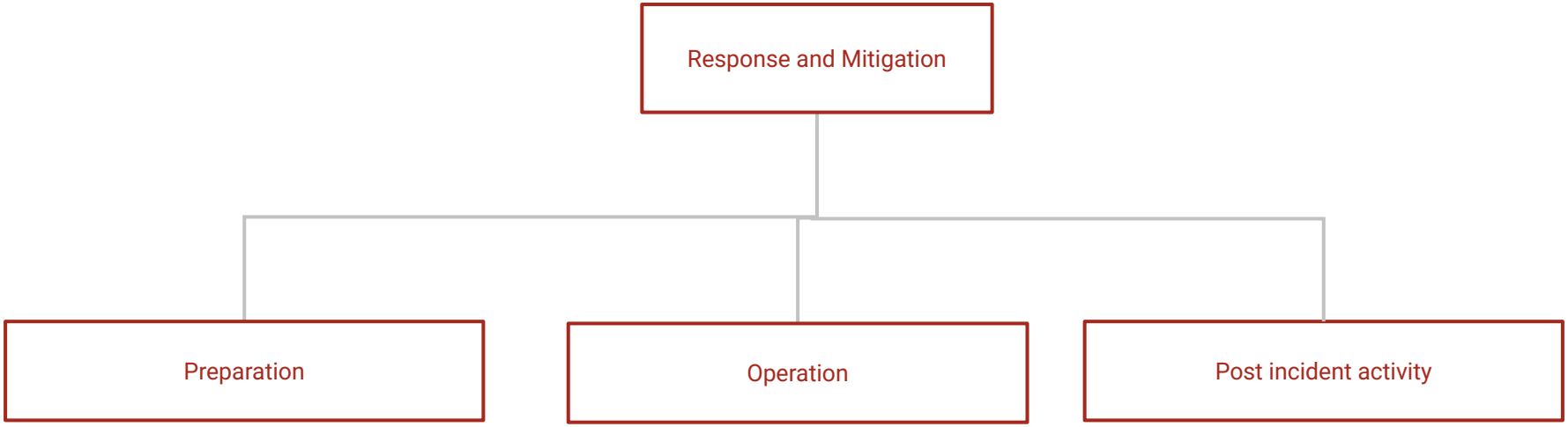
Infrastructure protection



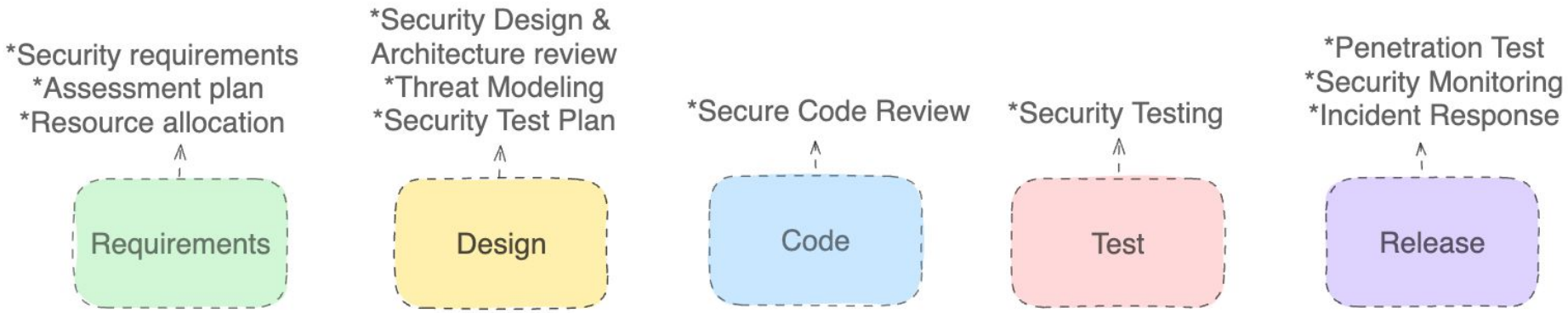
Data protection

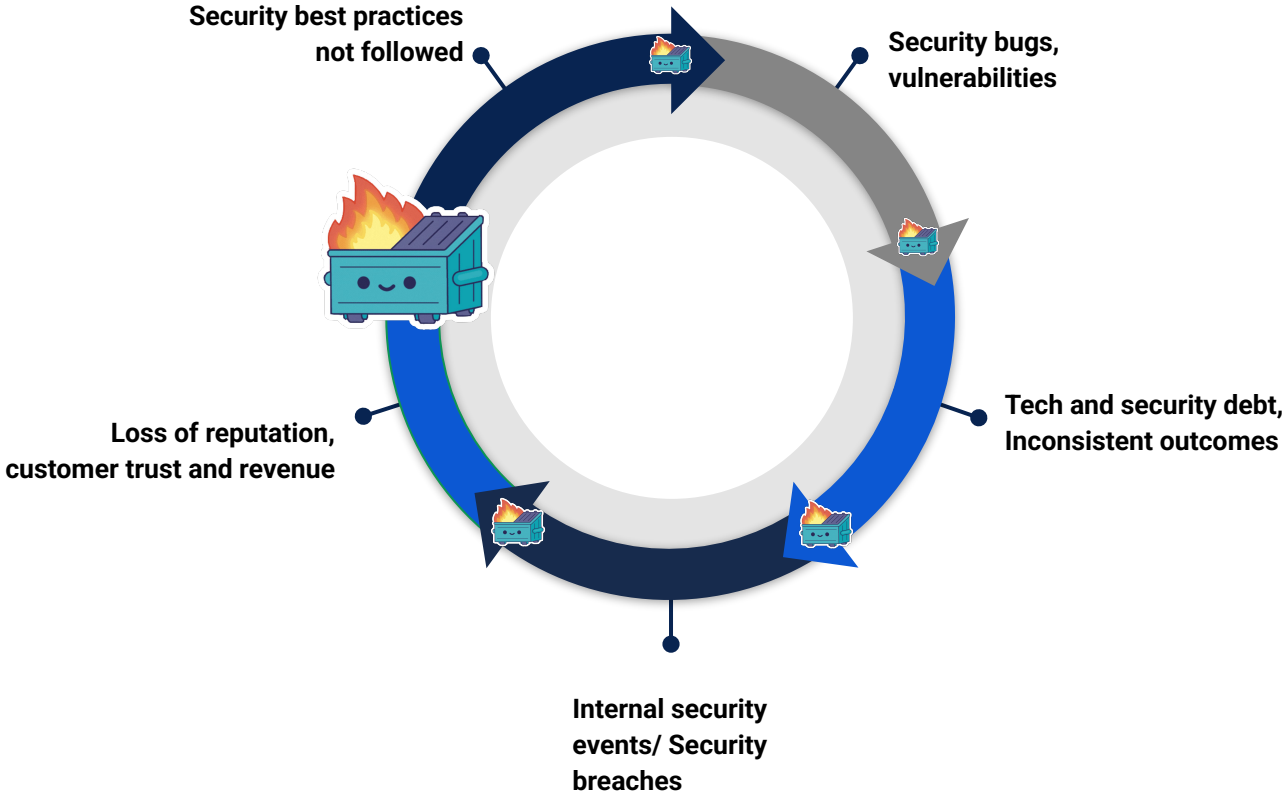


Incident Response



Application Security

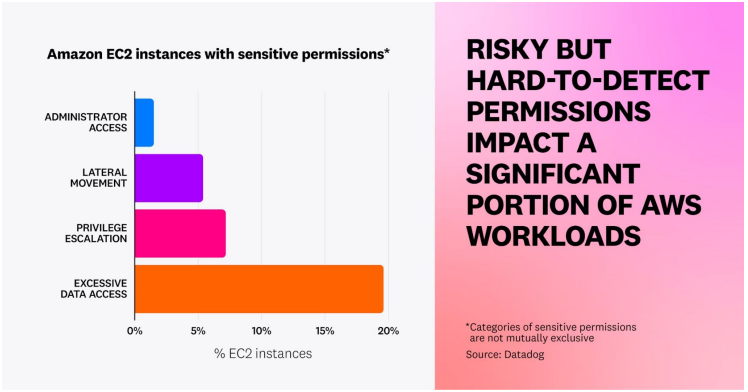



Security best practices not followed
Security bugs, vulnerabilities
Tech and security debt, Inconsistent outcomes
Internal security events/ Security breaches
Loss of reputation, customer trust and revenue

Misconfiguration exploits in cloud environments

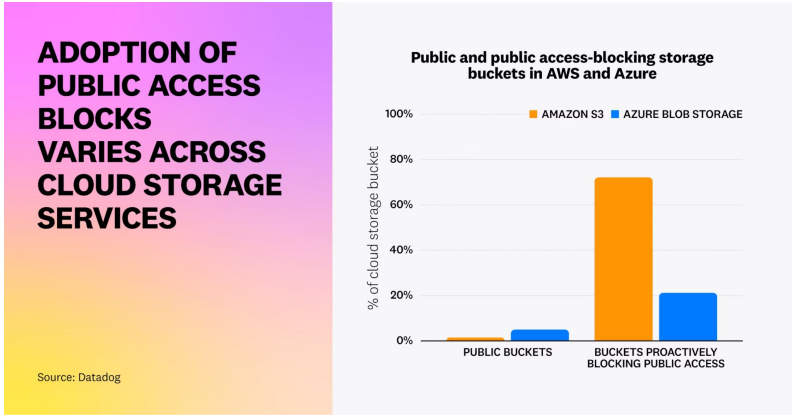
Excessive Permissions

- Overly broad permissions granted to users, apps, or services
- Not implementing the principle of least privilege
- Misconfigured identity and access management (IAM) policies



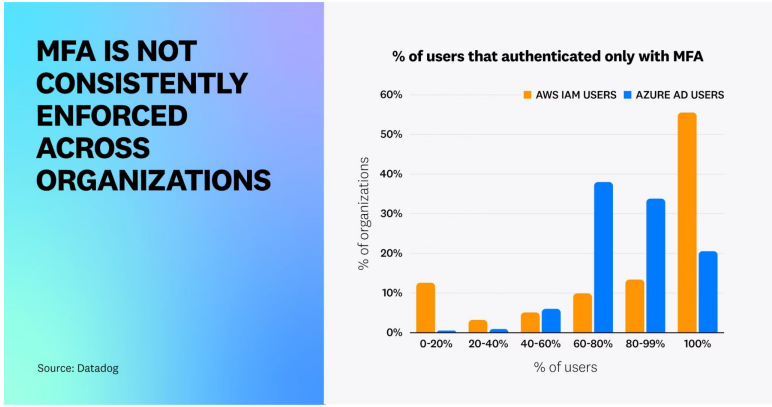
Insecure Storage Configuration

- Public access to storage buckets (e.g. AWS S3 buckets)
- Unencrypted data at rest or in transit
- Lack of access logging for storage resources



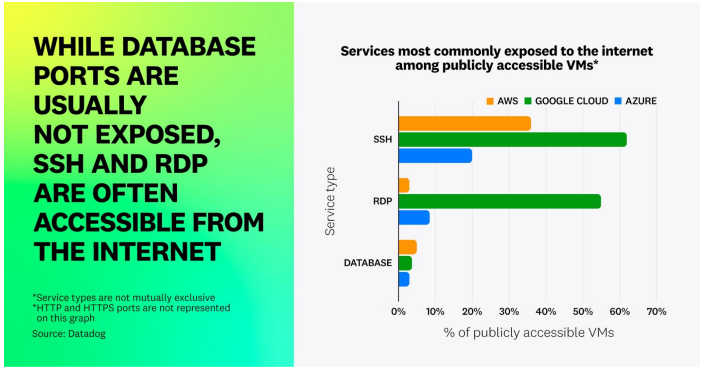
Exposed APIs and Endpoints

- Unsecured APIs without proper authentication/authorization
- Publicly accessible administrative interfaces or services
- Lack of API rate limiting



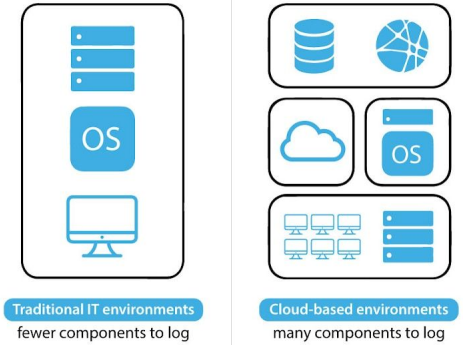
Network Misconfigurations

- Unrestricted inbound/outbound network access
- Open ports that shouldn't be publicly accessible (e.g. SSH, RDP)
- Lack of network segmentation



Inadequate Logging and Monitoring

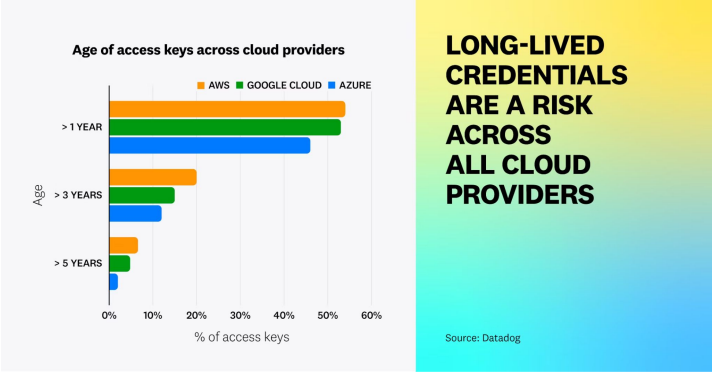
- Disabled or insufficient logging of cloud activities
- Lack of real-time monitoring and alerting
- Failure to review logs regularly

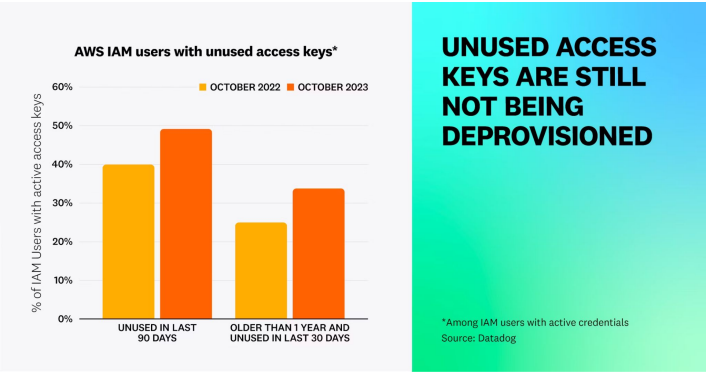


Source: Tek-Tools

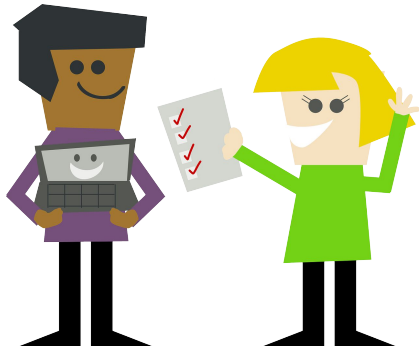
Neglected Cloud Resources

- Forgotten or unused cloud services that remain active
- Orphaned resources not properly decommissioned
- Long-lived credentials—i.e., those that are static and do not expire—are well-known as a major cause of cloud security breaches



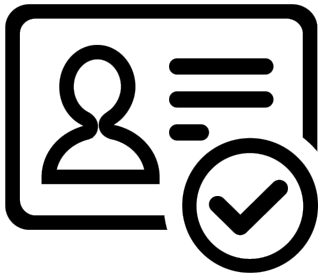


Security design for cloud environments



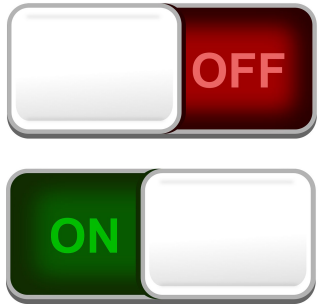
Implement a strong identity foundation

- Principle of least privilege
- Enforce separation of duties
- Centralized identity management
- Eliminate reliance on long-term static credentials
- Zero trust model



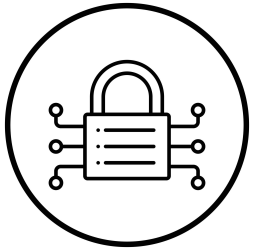
Apply security at all layers

- Defense in Depth approach with multiple security controls
- All layers secured
  - edge of network
  - virtual private cloud
  - load balancing
  - every instance and compute service
  - operating system
  - application
  - code



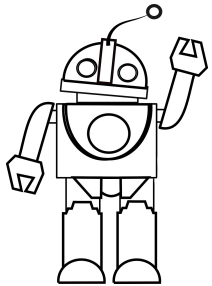
Protect data in transit and at rest

- Classify data into sensitivity levels
- Use mechanisms, such as encryption, tokenization, and access control where appropriate



Automate security best practices

- Automate Infrastructure Buildout with Infrastructure as code- Modules hardened for security configurations
- Automated Deployments- Using CI/CD pipelines for consistent deployments
- Automated Security Monitoring- quickly identify and address threats



Prepare for security events

- Incident management, investigation policy and processes
- Run incident response simulations
- Use tools with automation to increase your speed for detection, investigation, and recovery.

Takeaways

- Shared Responsibility is the Name of the Game
- Security is a Journey, Not a Destination
- Misconfigurations are the Achilles' Heel of Cloud Security
- Security by Design is Non-Negotiable

Q&A