

- Cloud Computing Background
- Cloud Models
- Why do you still hesitate to use cloud computing?
- Causes of Problems Associated with Cloud Computing

Cloud Computing Vs On-prem

Definitions

Cloud Computing

- A computing model where IT resources (servers, storage, networking, applications) are delivered over the internet by a third-party provider on a pay-as-you-go basis.

On-Premises

- A traditional computing model where all IT infrastructure is physically located, owned, and managed within the organization's facilities.

Cloud Computing Vs On-prem

Cloud Computing

Pros

- Low upfront cost (pay-as-you-go)
- High scalability and elasticity
- Fast deployment and time to market
- Built-in availability and disaster recovery
- Reduced operational overhead

Cons

- Less control over infrastructure
- Dependency on internet connectivity
- Ongoing operational costs
- Shared responsibility for security
- Potential data residency concerns

On-Premises

Pros

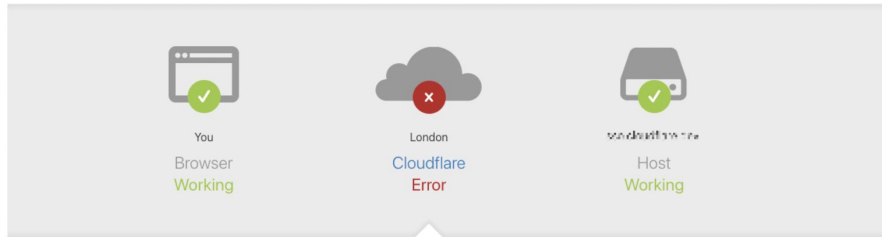
- Full control over systems and data
- High customization and flexibility
- Easier to enforce strict compliance
- No dependency on internet access
- Predictable long-term costs

Cons

- High upfront capital investment
- Limited scalability
- Longer deployment times
- Requires in-house maintenance and expertise
- Disaster recovery is costly and complex

Internal server error Error code 500

Visit cloudflare.com for more information.
2025-11-18 11:35:32 UTC



What happened?

There is an internal server error on Cloudflare's network.

What can I do?

Please try again in a few minutes.

Cloudflare Ray ID: 9a072a3bce88467f • Your IP: [Click to reveal](#) • Performance & security by Cloudflare

The issue was not caused, directly or indirectly, by a cyber attack or malicious activity of any kind. Instead, it was triggered by a change to one of our database systems' permissions which caused the database to output multiple entries into a "feature file" used by our Bot Management system. That feature file, in turn, doubled in size. The larger-than-expected feature file was then propagated to all the machines that make up our network.

Amazon reveals cause of AWS outage that took everything from banks to smart beds offline

AWS explains in a lengthy post how a bug in automation software brought down thousands of sites and applications

Record-breaking DDoS attack against Microsoft Azure mitigated

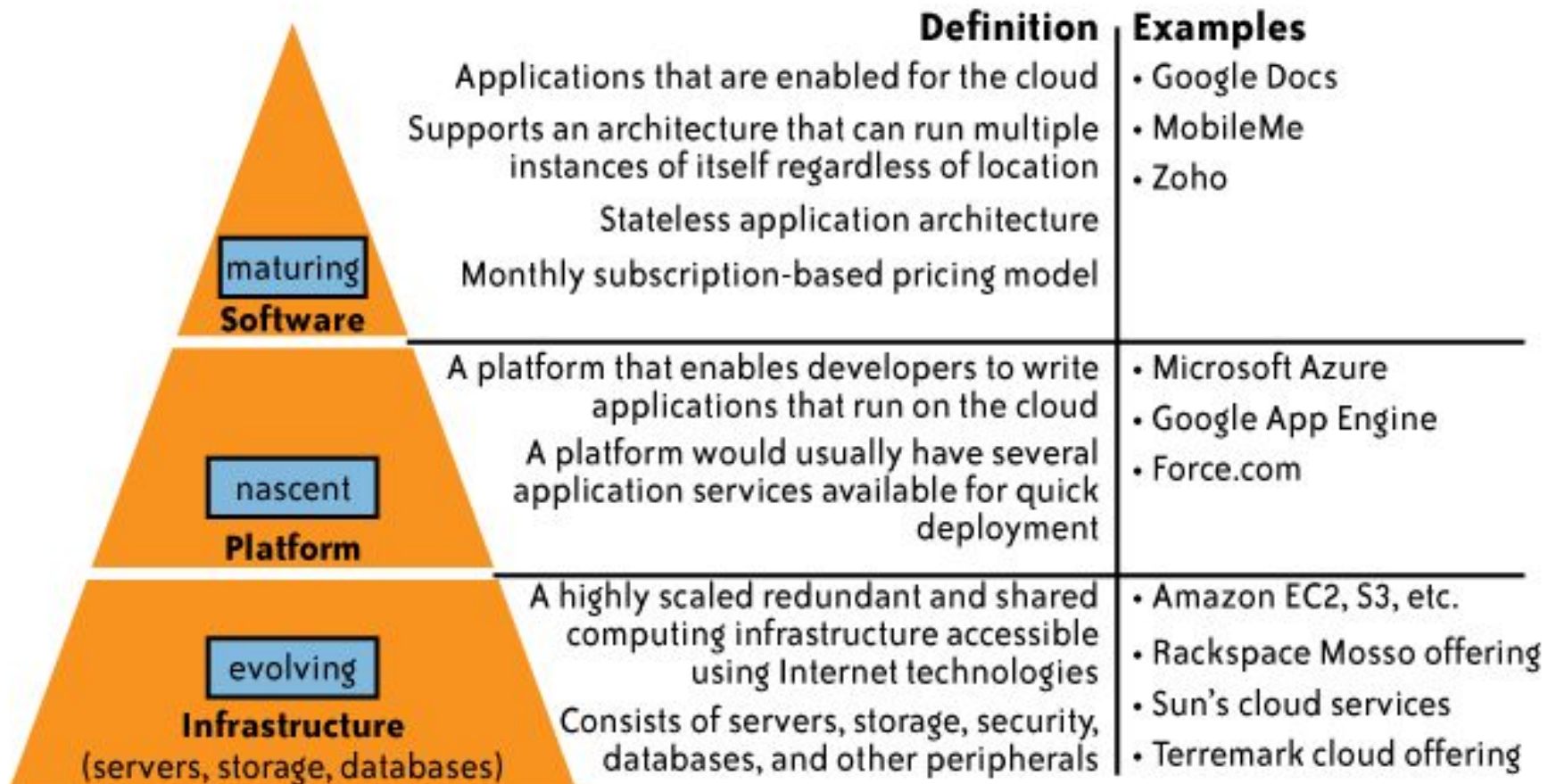
The attack was linked to the Aisuru botnet, which targets compromised home and cameras.

<https://blog.cloudflare.com/18-november-2025-outage/>

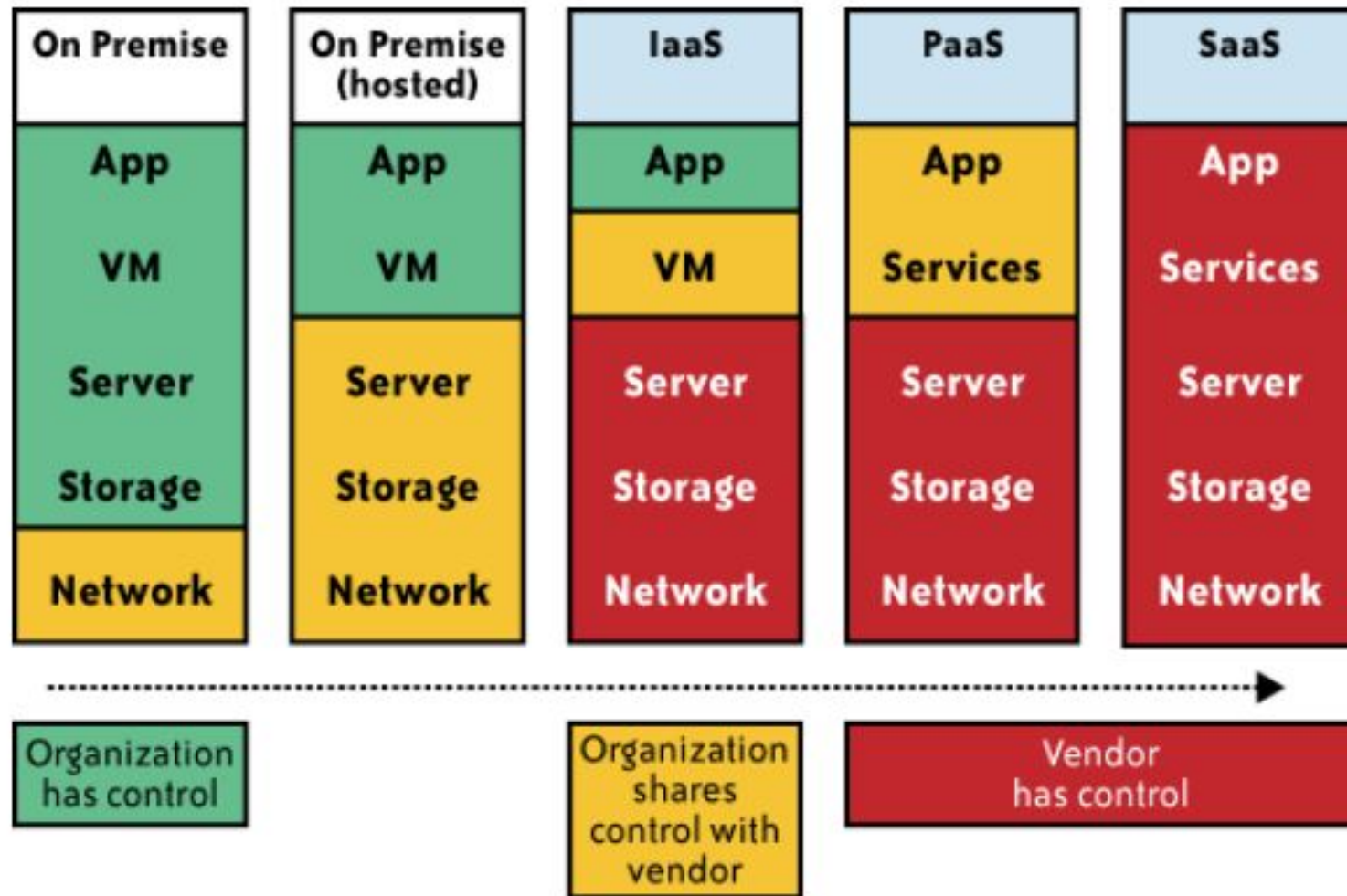
Cloud Models

- Delivery Models
 - SaaS
 - PaaS
 - IaaS
- Deployment Models
 - Private cloud
 - Community cloud
 - Public cloud
 - Hybrid cloud

Delivery Models



Impact of cloud computing on the governance structure of IT organizations



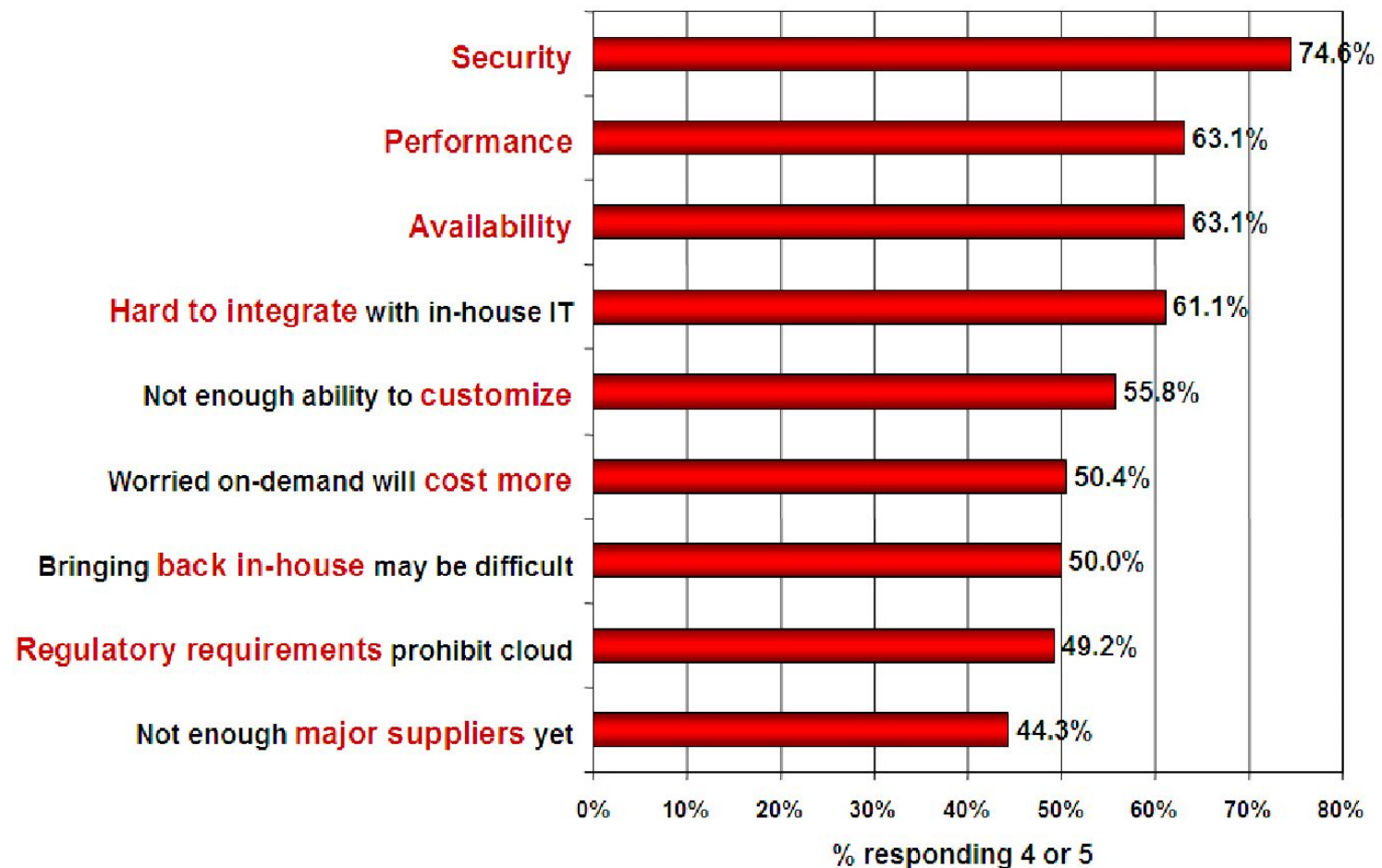
If cloud computing is so great, why isn't everyone doing it?

- The cloud acts as a big black box, nothing inside the cloud is visible to the clients
- Clients have no idea or control over what happens inside a cloud
- Even if the cloud provider is honest, it can have malicious system admins who can tamper with the VMs and violate confidentiality and integrity
- Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks

Companies are still afraid to use clouds

Q: Rate the **challenges/issues** ascribed to the 'cloud'/on-demand model

(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

MITRE | ATT&CK®

Matrices ▾Tactics ▾Techniques ▾Defenses ▾CTI ▾Resources ▾BenefactorsBlog 🔗Search 🔍

MATRICES

Enterprise

PRE

Windows

macOS

Linux

Cloud

Office Suite

Identity Provider

SaaS

IaaS

Network Devices

Containers

ESXi

Mobile

ICS

Cloud Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® cloud platforms. The Matrix contains information for the following platforms: Office Suite, Identity Provider, SaaS, IaaS.

layout: side ▾

show sub-techniques

hide sub-techniques

help

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
6 techniques	6 techniques	8 techniques	5 techniques	14 techniques	11 techniques	15 techniques	5 techniques	5 techniques	3 techniques	11 techniques
Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Automated Collection	Exfiltration Over Alternative Protocol	Account Access Removal
Exploit Public-Facing Application	Command and Scripting Interpreter (1)	Cloud Application Integration	Account Manipulation (5)	Domain or Tenant Policy Modification (1)	Credentials from Password Stores (1)	Cloud Infrastructure Discovery	Remote Services (2)	Data from Cloud Storage	Exfiltration Over Web Service (1)	Data Destruction
Phishing (2)	Poisoned Pipeline Execution	Create Account (1)	Domain or Tenant Policy Modification (1)	Email Spoofing	Exploitation for Credential Access	Cloud Service Dashboard	Software Deployment Tools	Data from Information Repositories (6)	Transfer Data to Cloud Account	Data Encryption Impact
Supply Chain Compromise	Serverless Execution	Event Triggered Execution	Event Triggered Execution	Exploitation for Defense Evasion	Forge Web Credentials (2)	Cloud Service Discovery	Taint Shared Content	Data Staged (1)	Email Collection (2)	Defacement
Trusted Relationship	Software Deployment Tools	Implant Internal Image	Valid Accounts (2)	Hide Artifacts (1)	Modify Authentication Process (3)	Cloud Storage Object Discovery	Use Alternate Authentication Material (2)			Email Bombing
Valid Accounts (2)	User Execution (1)	Modify Authentication Process (3)		Impersonation	Multi-Factor Authentication Request Generation	Local Storage Discovery				Endpoint Denial Service
		Office Application Startup (6)		Indicator Removal (1)	Network Sniffing	Log Enumeration				Financial Record Access
		Valid Accounts (2)		Modify Authentication Process (3)	Steal Application Access Token	Network Service Discovery				Network Denial Service
				Modify Cloud Compute Infrastructure (5)	Steal or Forge Authentication Certificates	Network Sniffing				Resource Hijack
				Modify Cloud Resource Hierarchy	Steal Web Session Cookie	Password Policy Discovery				Service Disruption
				Unused/Unsupported Cloud Regions	Unsecured	Permission				
				Use Alternate Authentication Material (2)						

Causes of Problems Associated with Cloud Computing

- Most security problems stem from:
 - Loss of control
 - Lack of trust (mechanisms)
 - Multi-tenancy
- These problems exist mainly in 3rd party management models
 - Self-managed clouds still have security issues, but not related to above

Loss of Control in the Cloud

- Consumer's loss of control
 - Data, applications, resources are located with provider
 - User identity management is handled by the cloud
 - User access control rules, security policies and enforcement are managed by the cloud provider
 - Consumer relies on provider to ensure
 - Data security and privacy
 - Resource availability
 - Monitoring and repairing of services/resources

Lack of Trust in the Cloud

- A brief deviation from the talk
 - (But still related)
 - Trusting a third party requires taking risks
- Defining trust and risk
 - Opposite sides of the same coin (J. Camp)
 - People only trust when it pays (Economist's view)
 - Need for trust arises only in risky situations
- Defunct third party management schemes
 - Hard to balance trust and risk
 - e.g. Key Escrow (Clipper chip)
 - Is the cloud headed toward the same path?

Multi-tenancy Issues in the Cloud

- Conflict between tenants' opposing goals
 - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
 - Can tenants get along together and 'play nicely' ?
 - If they can't, can we isolate them?
- How to provide separation between tenants?
- Cloud Computing brings new threats
 - Multiple independent users share the same physical infrastructure
 - Thus an attacker can legitimately be in the same physical machine as the target

Taxonomy of Fear

- Confidentiality
 - Fear of loss of control over data
 - Will the sensitive data stored on a cloud remain confidential?
 - Will cloud compromises leak confidential client data
 - Will the cloud provider itself be honest and won't peek into the data?
- Integrity
 - How do I know that the cloud provider is doing the computations correctly?
 - How do I ensure that the cloud provider really stored my data without tampering with it?

Taxonomy of Fear (cont.)

- Availability
 - Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?
 - What happens if cloud provider goes out of business?
 - Would cloud scale well-enough?
 - Often-voiced concern
 - Although cloud providers argue their downtime compares well with cloud user's own data centers

Taxonomy of Fear (cont.)

- Privacy issues raised via massive data mining
 - Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients
- Increased attack surface
 - Entity outside the organization now stores and computes data, and so
 - Attackers can now target the communication link between cloud provider and client
 - Cloud provider employees can be phished

Taxonomy of Fear (cont.)

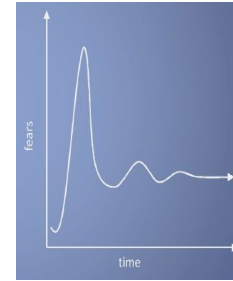
- Auditability and forensics (out of control of data)
 - Difficult to audit data held outside organization in a cloud
 - Forensics also made difficult since now clients don't maintain data locally
- Legal quagmire and transitive trust issues
 - Who is responsible for complying with regulations?
 - e.g., SOX, HIPAA, GLBA ?
 - If cloud provider subcontracts to third party clouds, will the data still be secure?

Taxonomy of Fear (cont.)



Cloud Computing is a **security nightmare** and it can't be handled in traditional ways.

John Chambers
CISCO CEO



- Security is one of the most difficult task to implement in cloud computing.
 - Different forms of attacks in the application side and in the hardware components
- Attacks with catastrophic effects only needs one security flaw

class exercise

Read

<https://cloudsecurityalliance.org/blog/2025/05/07/unpacking-the-2024-snowflake-data-breach#>

1. What was the attacker's primary goal after gaining access to Snowflake customer accounts?
2. Which MITRE ATT&CK Cloud tactic best describes the use of stolen Snowflake credentials to login successfully?
3. Which MITRE Cloud technique explains how the attacker accessed data without exploiting a software vulnerability?
4. Which cloud-focused ATT&CK tactic covers the large-scale extraction of sensitive data from Snowflake environments?
5. Which MITRE Cloud tactic applies to advertising stolen Snowflake data for sale and extorting victims?
6. What are the mitigation the blog mentions?

class exercise

1. **Attacker's primary goal:** Financial gain via data exfiltration and extortion.
2. **MITRE Cloud tactic for stolen credential login:** Initial Access – **Valid Accounts (T1078.004)**
3. **MITRE Cloud technique for accessing data without exploiting a vulnerability:** Initial Access – **Valid Accounts (T1078.004)**
4. **MITRE Cloud tactic for large-scale data extraction:** Collection – **Data from Cloud Storage (T1530)**
5. **MITRE Cloud tactic for selling/extorting data:** Exfiltration – **Exfiltration Over Web Service (T1567.002)**
6. **Mitigations mentioned in the blog:**
 - **Preventive:** MFA, least privilege, conditional access, anti-malware, DLP, secure design
 - **Detective:** Security monitoring, baseline deviation detection, audit log monitoring, incident management
 - **Corrective:** Breach notification, supply chain assessments, vulnerability/patch management