# COMP482 Cybersecurity Week 3 - Friday

Dr. Nicholas Polanco
(he/him)

KALAMAZOO COLLEGE

# Attendance

1. What is the chemical symbol for gold?
2. Which British rock band released the album *A Night at the Opera* in 1975, featuring the song “Bohemian Rhapsody”?
3. What planet in our solar system has the shortest day, completing a full rotation in just 10 hours?
4. What type of alcohol is used in a traditional Mojito cocktail?
5. How many players are there on a standard soccer team on the field during play?

COMP482 - Attendance: Week 3 Friday

# Attendance

1. Gold
2. Queen
3. Jupiter
4. Rum
5. 11

COMP482 - Attendance: Week 3 Friday

KALAMAZOO COLLEGE

# Important Notes

1. It seems Autonomous Vehicles is the lecture people would want to do, and we had lots of votes for a work day later in the term. We can revisit this as we get closer.
2. You have an additional week for your Activity: Keylogger and Buffer Overflow. It will now be due Week 4 - Friday (April 25th).

# Important Dates (Week 4)

| Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday |
|---|---|---|---|---|---|---|
| | | | | Activity: Keylogger or Buffer Overflow<br><br>Reflection Week 3 | | |

# Outline

1. Cloud Computing
2. Cloud Malware
3. Data Breaches
4. Insecure API’s
5. Insider Threats
6. In-Class Work

# Cloud Computing Types

# Cloud Computing

The term cloud computing refers to the delivery of computing services – like servers, storage, databases, networking, and software – over the internet ("the cloud").

This allows organizations and individuals to access and store information without managing their own physical infrastructure

Image Credit

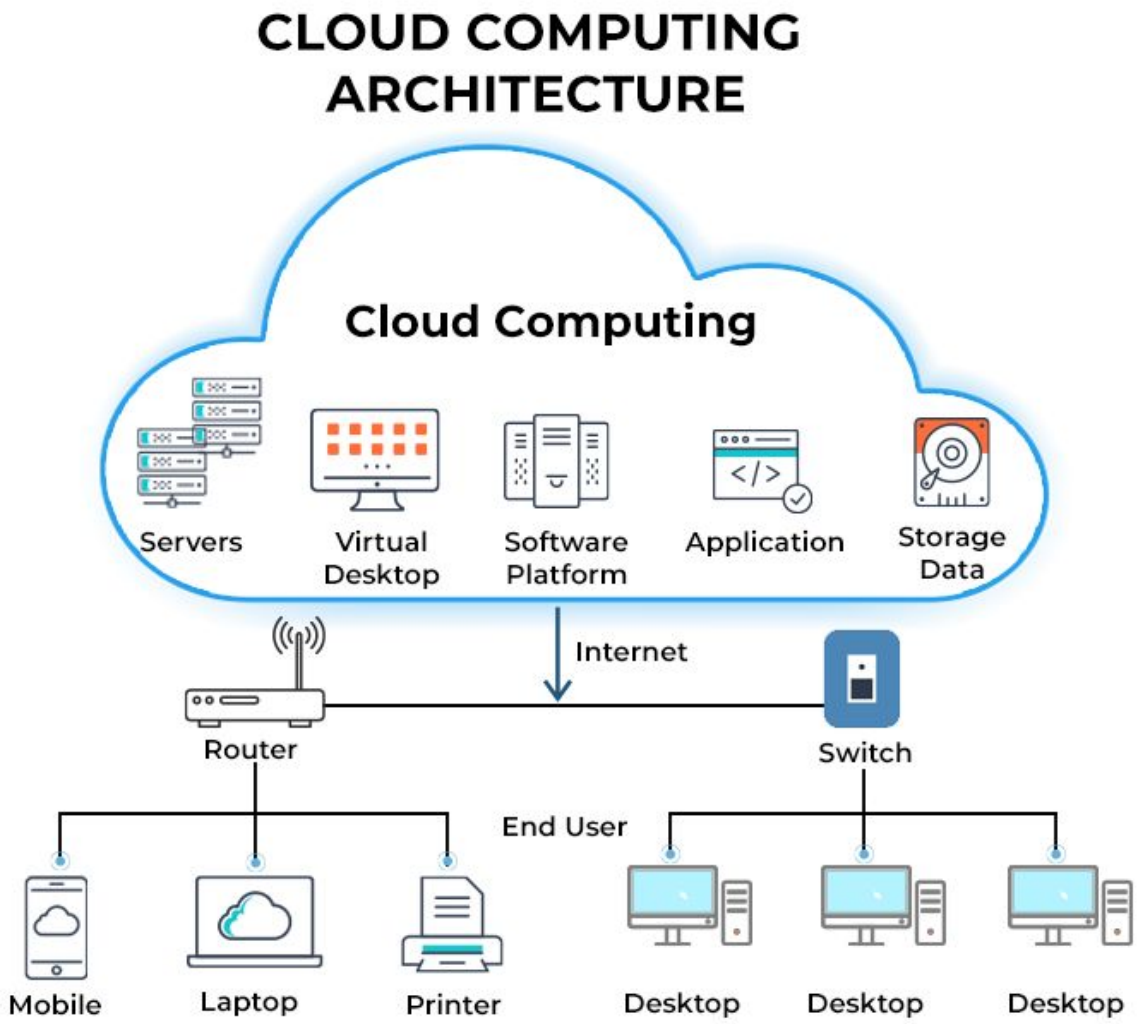


Image Credit
https://www.spiceworks.com/tech/cloud/articles/what-is-cloud-computing/

KALAMAZOO COLLEGE

# Cloud Computing Types

Infrastructure as a Service (IaaS) - This delivers on-demand infrastructure resources to organizations via the cloud, such as compute, storage, networking, and virtualization.

- The customers don’t have to manage, maintain, or update their own data center infrastructure, but are responsible for the operating system, middleware, and any apps or data.

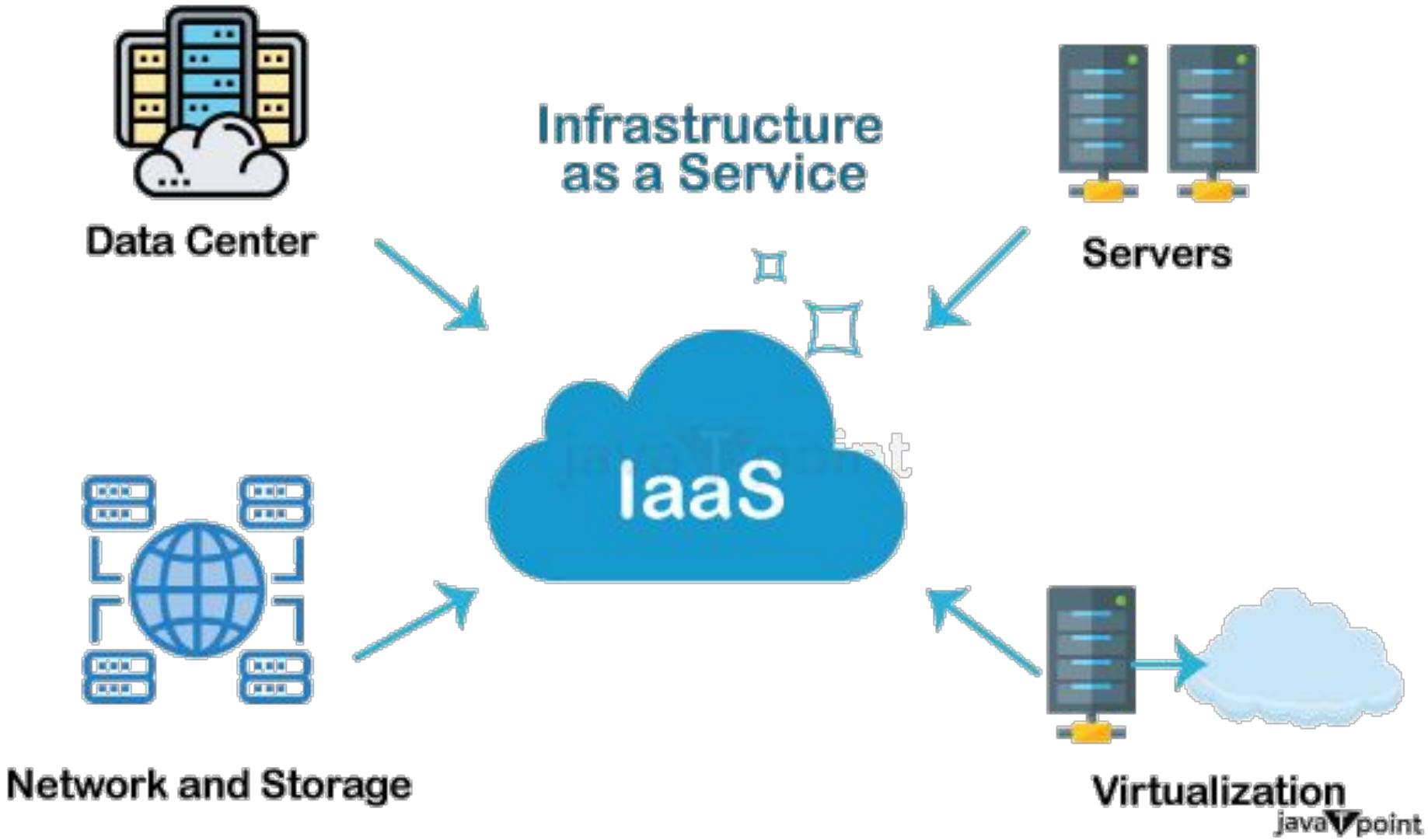


Image Credit
https://www.tpointtech.com/infrastructure-as-a-service

KALAMAZOO COLLEGE

# Cloud Computing Types (continued)

Containers as a Service (CaaS) - This delivers and manages all the hardware and software resources to develop and deploy applications using containers.

- The customers still have to write the code and manage their data and applications, but the environment to build and deploy containerized apps is managed and maintained by the cloud service provider.

Image Credit

# What's included in a Container?

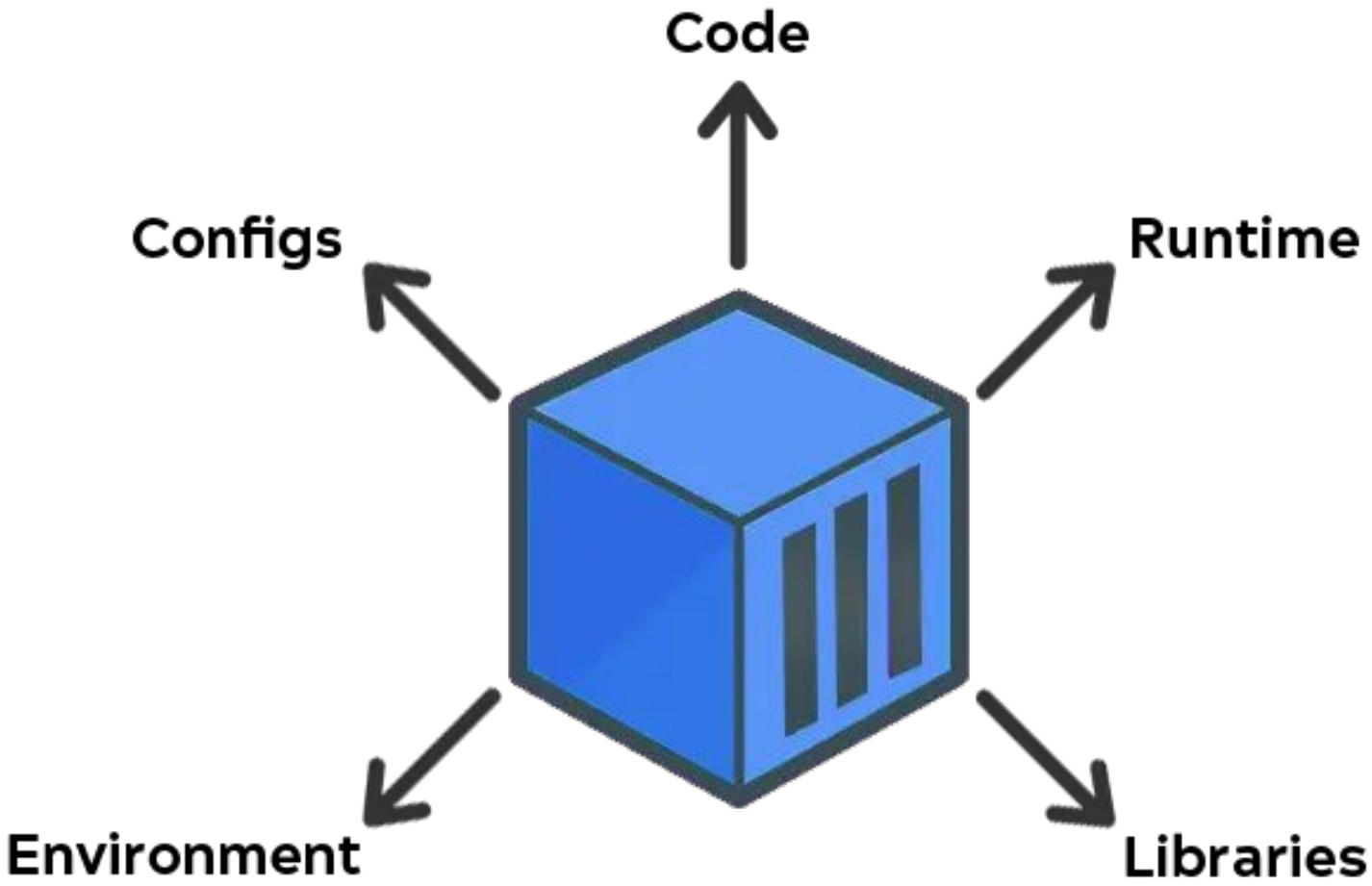


Image Credit
https://blog.back4app.com/what-are-containers-in-cloud-computing/

KALAMAZOO COLLEGE

# Cloud Computing Types (continued)

Platform as a Service (PaaS) - This delivers and manages all the hardware and software resources to develop applications through the cloud.

- The customers still have to write the code and manage their data and applications, but the environment to build and deploy apps is managed and maintained by the cloud service provider.


Image Credit
https://63sats.com/blog/platform-as-a-service-in-cloud-computing/

KALAMAZOO COLLEGE

# Cloud Computing Types (continued)

Function as a Service (FaaS) - This delivers platform-level cloud capability that enables its users to build and manage microservices applications with low initial investment for scalability

- The customers can run code in response to events, without managing the complex infrastructure typically associated with building and launching microservices applications.
- *You can think of running a single function.

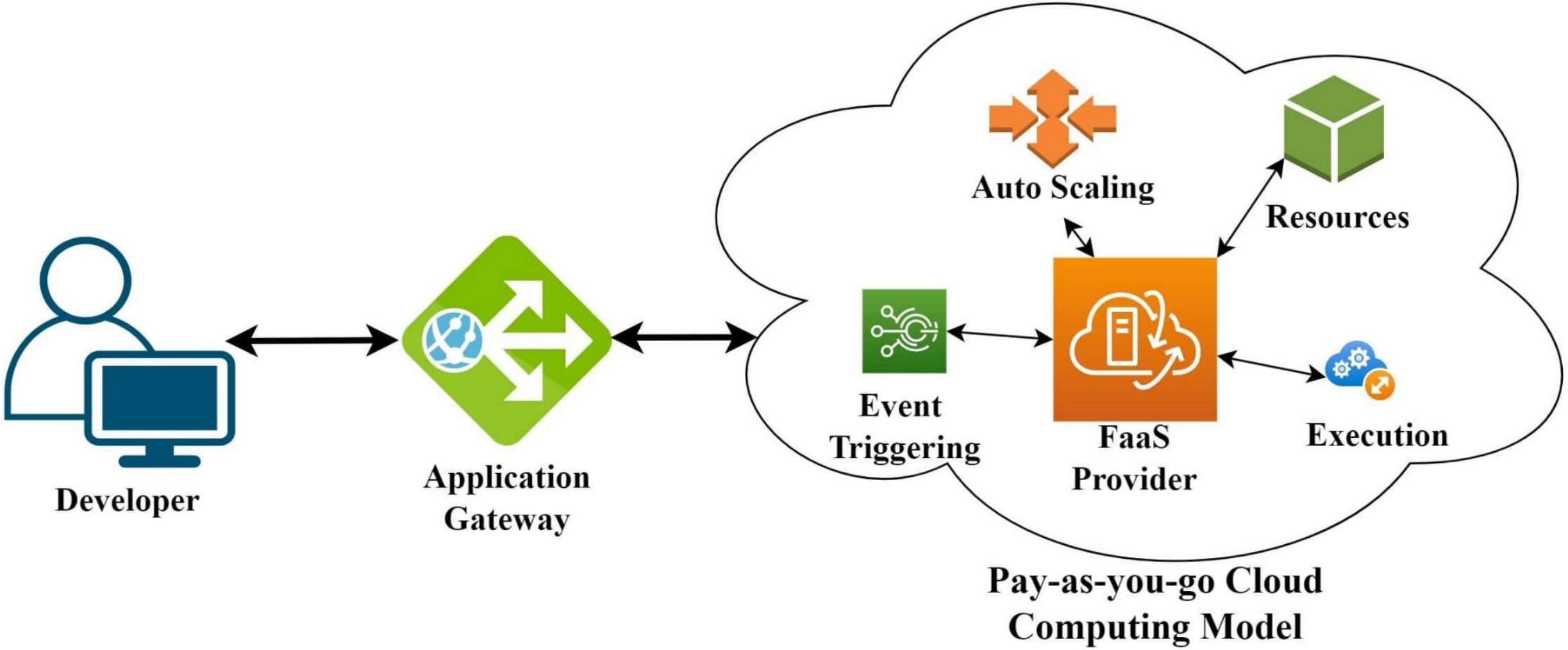


Image Credit
https://www.baeldung.com/cs/faas

KALAMAZOO COLLEGE

# Cloud Computing Types (continued)

Software as a Service (SaaS) - This provides the entire application stack, delivering an entire cloud-based application that customers can access and use.

- The customers applications are accessed directly through a web browser, which means customers don't have to download or install anything on their devices.

<u>Do we know any examples?</u>

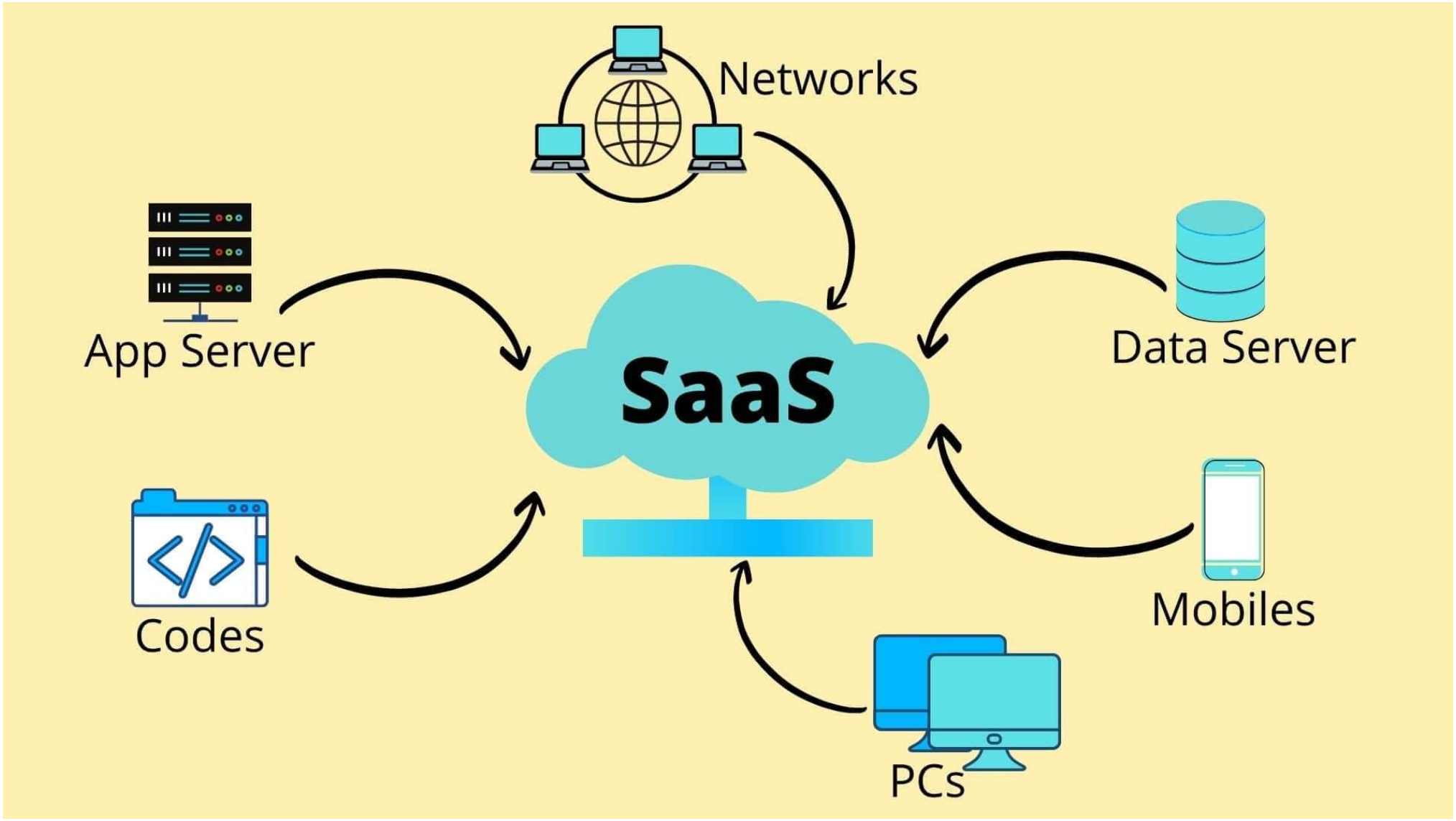


Image Credit
https://ceymox.com/saas-software-as-service-e-commerce-supply-chain/

KALAMAZOO COLLEGE

# Pause: Shared Responsibility Model

The shared responsibility model is a framework establishing who is responsible for securing different aspects of the cloud-computing environment between the cloud service provider (CSP) and the customer.

Image Credit

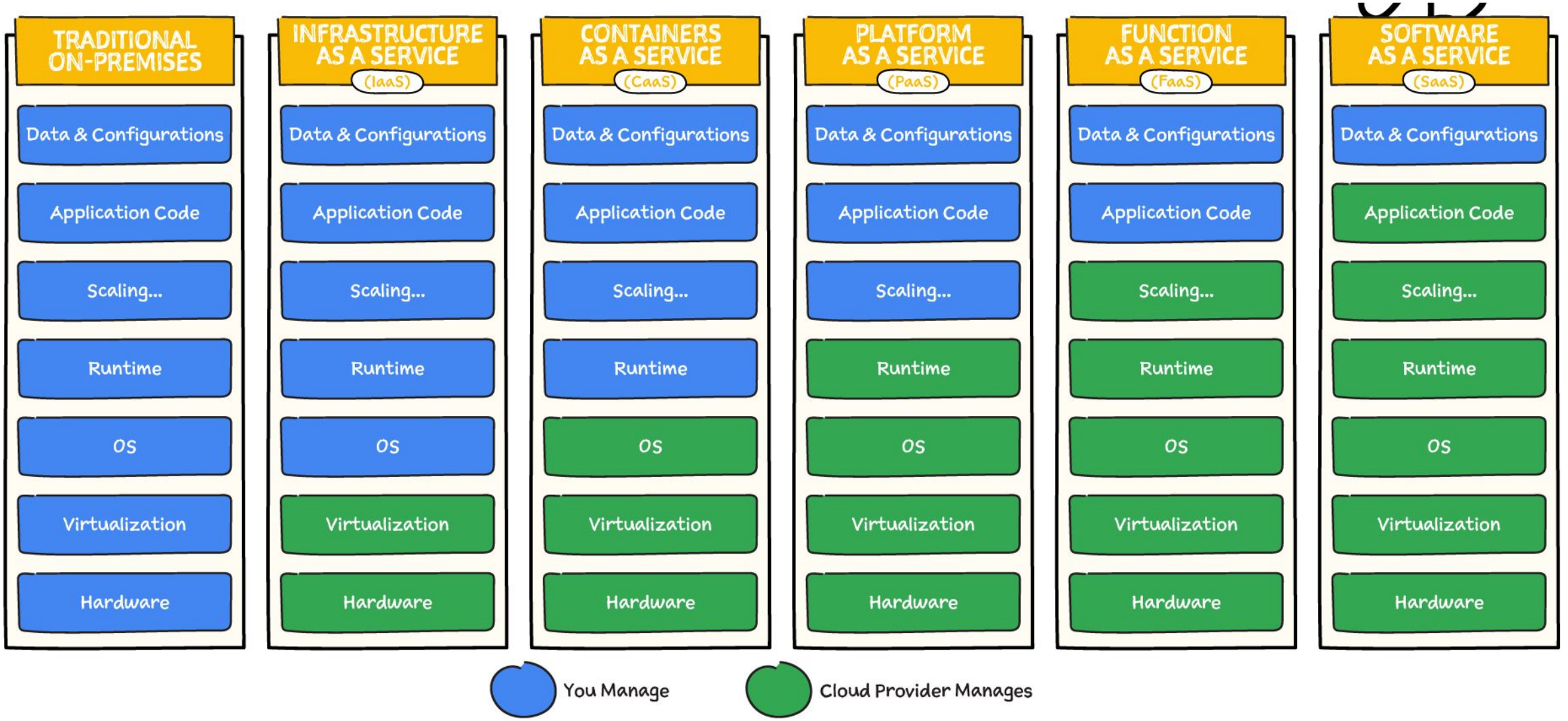


Image Credit
https://cloud.google.com/learn/paas-vs-iaas-vs-saas?hl=en

KALAMAZOO COLLEGE

# Discussion Questions

What cloud services do you personally use (Google Drive, Dropbox, AWS, etc.)? How confident are you in those services?

Do you think separating the responsibilities would help secure systems *more* or cause harm?

What role does user education play in the effectiveness of the shared responsibility model?

Image Credit

# Cloud Malware

# Cloud Malware

Cloud malware refers to any malware that targets cloud computing environments, or uses the cloud to carry out malicious activities. This exploits the features and architecture of cloud platforms to infiltrate systems, steal data, or disrupt services.

Image Credit

# Cloud Malware (continued)

Why do you think we have attackers targeting cloud-based systems?

Image Credit

# Cloud Malware (continued)

<u>Why do you think we have attackers targeting cloud-based systems?</u>

The services offered by cloud systems (like storage, processing, and applications) are delivered over the internet and has transformed how businesses operate.

This area is susceptible to attacks because of:

- The use of shared resources and multiple users sharing the same infrastructure
- The ability to access from anywhere remote
- The third-party management, these cloud providers control parts of the infrastructure

Image Credit

# Cloud Malware Threats

Malware Hosted in the Cloud - This can be when attackers upload malicious code or files to cloud storage services (like Google Drive or Dropbox) and then distribute the links to victims.

- This can include a phishing email including a link to a cloud-hosted file containing malware.

Compromising Cloud-Based Applications - The malware can be injected into SaaS applications. Once the user logs in, malicious scripts can be executed, often without the user knowing.

- This can be something like a browser-based cloud CRM (Customer Relations Manager) with a malicious plugin that exfiltrates customer data.

# Cloud Malware Threats (continued)

Exploiting Cloud Infrastructure - The malware targets the underlying infrastructure—like virtual machines, containers, or misconfigured cloud settings.

- An example is cryptojacking malware infects cloud VMs and uses them to mine cryptocurrency.

Cloud-to-Cloud Propagation - These infected cloud applications can spread malware to other connected platforms through APIs or integrations.

- This includes a compromised cloud email account automatically sends malicious links to all contacts stored in the cloud.

# Cloud Malware Defense

- Cloud Security Posture Management (CSPM) - These tools continuously scan cloud configurations for vulnerabilities or misconfigurations.
- Identity and Access Management (IAM) - This implements strict control about who has access to what resources, and enforce least privilege.
- Monitoring and Logging - They can use tools like AWS CloudTrail, Azure Monitor, or Google Cloud's Operations Suite to detect unusual activity.
- Endpoint Detection and Response (EDR) - These install EDR tools on virtual machines and cloud-hosted workloads to catch malware early.
- User Education - The use of phishing remains a major cloud malware delivery vector, so employee training is critical.

Image Credit

# Data Breach

# Data Breach

A cloud data breach occurs when unauthorized users access, steal, or leak sensitive data hosted on cloud infrastructure—whether public (like AWS, Azure, or Google Cloud), private, or hybrid environments.

The reason this may be a *slightly* bigger risk is due to:

1. The shared responsibility models
2. The number of users
3. Remote accessibility

<u>Do we agree that the cloud may be more susceptible to data breaches?</u>

Image Credit

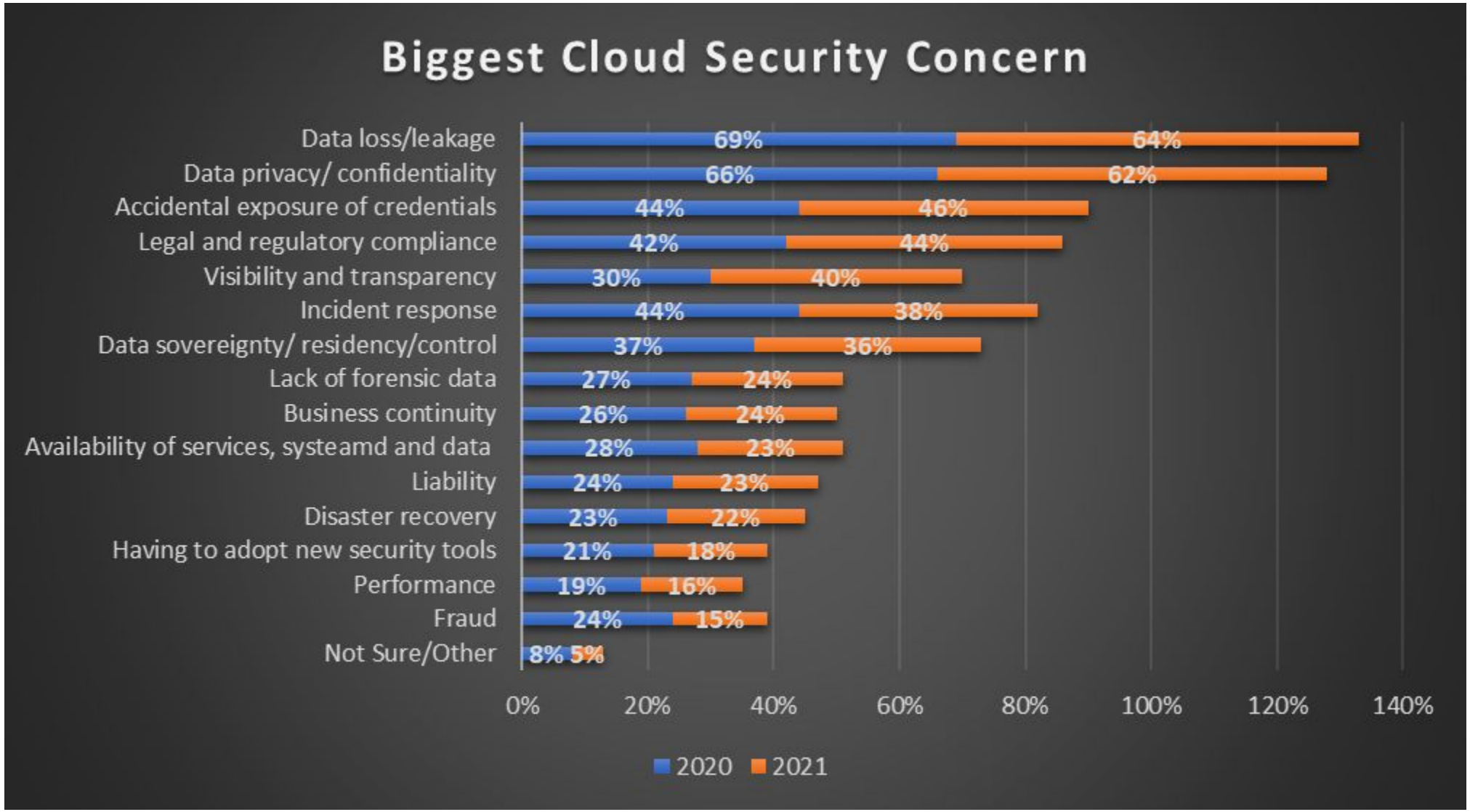


Image Credit
https://edgedelta.com/company/blog/cloud-security-statistics

KALAMAZOO COLLEGE

# Data Breach Risks

Misconfigured Cloud Storage - You can have default-open S3 buckets (folders), unprotected blobs (binary large objects), or misconfigured access controls.

- You can have exposed AWS S3 buckets publicly accessible without authentication.

Poor Identity and Access Management (IAM) - The use of overly permissive roles or credentials not following the Principle of Least Privilege.

- You can have a user with admin rights to all cloud resources instead of just the needed services.

# Pause: Principle of Least Privilege

The principle of least privilege (PoLP) is a security concept that dictates users, applications, and systems should only have the minimum necessary access to perform their tasks.

Image Credit

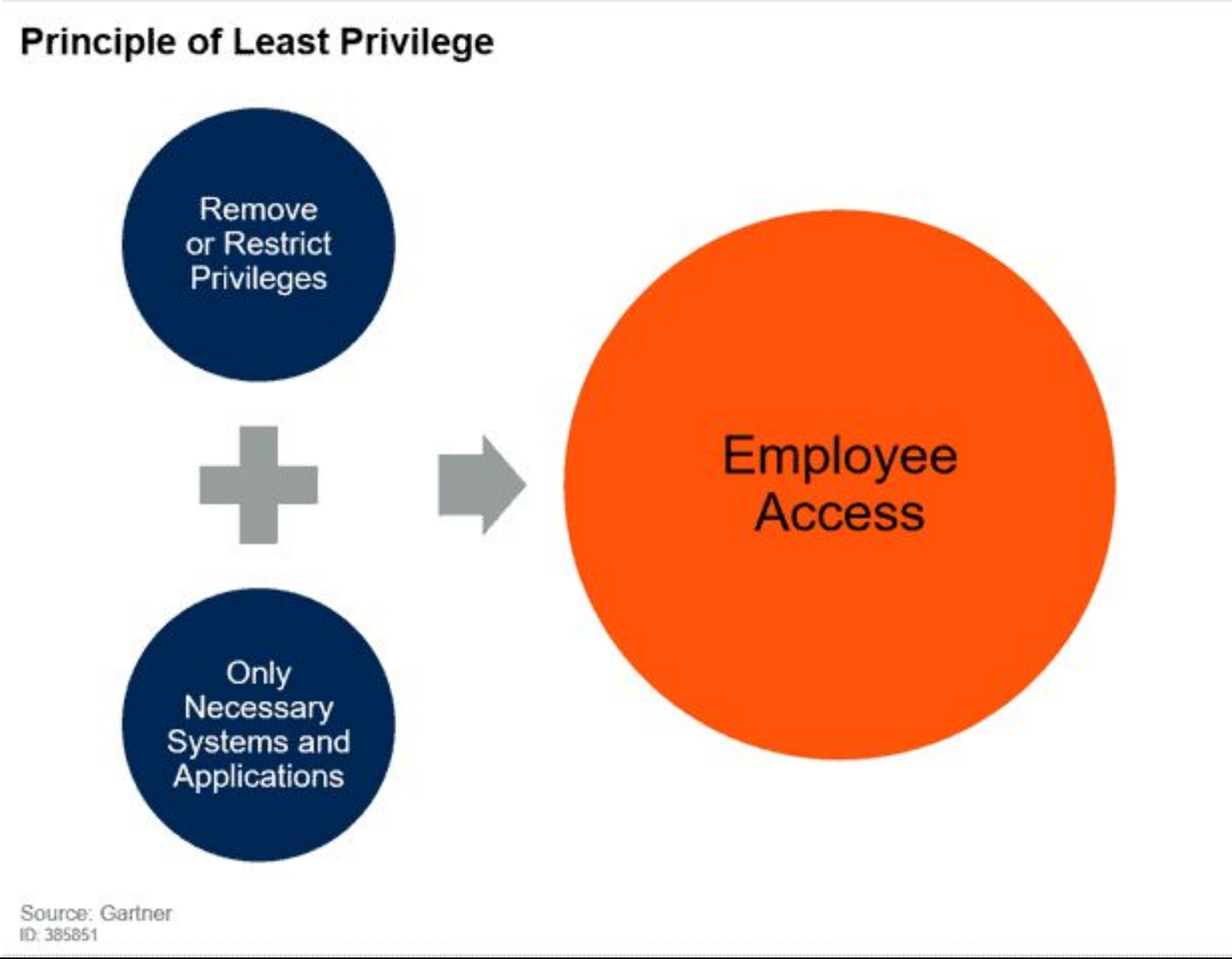


Image Credit
https://instasafe.com/blog/zero-trust-least-privilege-access-models/

KALAMAZOO COLLEGE

# Data Breach Risks (continued)

Third-party Vendor Risks - The cloud services often integrate with external tools or apps. A breach in one vendor can cascade into others.

Insufficient Encryption - The data not being encrypted at rest or in transit in the cloud environment.

- You can have a database backup stored in plaintext in a cloud storage bucket.

<u>Does anyone feel like implementing good cybersecurity is easy, and it most the time people just “forgot” some defense mechanicms?</u>

# Data Breach Prevention

1. Apply the Principle of Least Privilege
2. Use Strong IAM Policies & MFA
3. Secure and Audit APIs
    a. We can use authentication, rate limiting, and regular API security assessments.
4. Encrypt Data
5. Regularly Audit and Monitor Configurations

<u>Who do we think has more impact in cybersecurity, the user or the cloud-computing platform?</u>

Image Credit

# Insecure APIs

# Insecure APIs

An insecure API is an application programming interface that lacks proper security controls, exposing cloud resources to unauthorized access, data leaks, manipulation, or service disruption.

Cloud providers like AWS, Azure, and Google Cloud expose APIs to let users manage their infrastructure — but if these APIs aren't secured properly, attackers can exploit them.

Image Credit

# Insecure APIs Weaknesses

Lack of Authentication / Authorization - You can have an API endpoint that allows access to user data without verifying identity, or that doesn't check if the user has permission.

- We allow anyone with the link to download our entire customer list

# Insecure APIs Weaknesses (continued)

Improper Rate Limiting - We don’t limit rates so APIs are vulnerable to DDoS attacks or brute force login attempts.

Unencrypted Communication- We use HTTP instead of HTTPS.

- This may seem simple, but in bad multi-tenant cloud setups this can be an issue

Verbose Error Messages - We have too detailed errors that can leak internal structure (like database names or stack traces).

# Insecure APIs Security

Human-Factors - MFA, Principle of Least Privilege, Education.

Validate Inputs - We ensure the input is not injecting any malicious attacks or code.

# Insider Threats

# Insider Threats

These are security breaches or misuse of systems from within an organization, rather than external attackers. These threats are particularly dangerous because insiders often bypass traditional security perimeters.

Image Credit

# Discussion Questions

What are the different types of insider threats (e.g., malicious, negligent, accidental)? Can you think of real-world examples for each?

What motivates insiders to act maliciously? How might personal, financial, or ideological factors play a role?

How can a well-meaning employee accidentally become an insider threat?

Image Credit

# Insider Threat Motivations

**Financial gain** - Selling sensitive data or intellectual property.
**Revenge** - Disgruntled employees may try to damage systems or leak data.
**Espionage** - Stealing data for a competitor or foreign entity.
**Ideology** - Hacktivism or whistleblowing with a moral/political motive.
**Phishing** - Falling for phishing attacks and unknowingly exposing access.
**Misconfigurations** - Improperly setting permissions or exposing data buckets (e.g., public S3 buckets).
**Shadow IT** - Using unauthorized cloud apps or storage, bypassing IT controls.

# Insider Threats (continued)

The nature of cloud-computing makes these a bit tricky because:

- The distributed and remote nature of cloud access.
- You *can* have less visibility into user activity compared to on-site systems.
- The flexibility in resource access

# Insider Threats Attacks

Credential Abuse - The employees with excessive privileges use their credentials to access or exfiltrate data.

- Example: An employee downloads a full customer database from Salesforce before quitting.

Cloud Misconfiguration - Insiders (or careless admins) miss configure security settings — like leaving a folder open to the internet.

- Example: A dev accidentally allows public read/write access on storage.

Third-Party Risks - The vendors or contractors with cloud access might intentionally or unintentionally compromise security.

- Example: A contractor uses weak passwords or stores credentials in plaintext.

Image Credit

# Insider Threats Attacks (continued)

Data Exfiltration via Cloud Services - You can use tools like Dropbox, Google Drive, or email to quietly exfiltrate files. This can be hard to detect if no data loss prevention (DLP) tools are in place.

Abuse of Shared Responsibility - The cloud providers handle some security, but the customer must secure data, applications, and access controls. Insiders may exploit gaps in this shared model.

<u>Do you think it is easy to falsely claim that some of these attacks were accidental?</u>

# Insider Threats Prevention

Zero Trust Model: Trust no one by default, verify everything — even internal traffic.

Least Privilege Access: Give users only the access they need, and no more.

User Behavior Analytics (UBA): Use tools to detect anomalies like sudden large file transfers or unusual login locations.

Audit Logs & Monitoring: Continuously monitor cloud activity logs (AWS CloudTrail, Azure Monitor, etc.).

# Insider Threats Prevention (continued)

Data Loss Prevention (DLP): Prevent sensitive data from being leaked or misused.

Security Awareness Training: Educate users to avoid phishing and shadow IT risks.

Access Reviews: Regularly audit user permissions and remove unnecessary rights.

Multi-Factor Authentication (MFA): Prevent unauthorized logins even if credentials are compromised.

# Debate Team (not really)

We are going to be moving around for this activity and choosing sides!

You are to look at the prompt, and choose **yes or no!** The agree students will be on one side, and the disagree students will be on the  other.

- Your group should discuss 1 reason you want to share with the class.
- These teams will each share, then afterwards members can chose to **stay or go to the other side.**
- *This is intended to be **fun**, please be respectful!

Image Credit

Should employees be monitored at all times to prevent insider threats, even if it invades their privacy?

Is it ethical to use AI to predict which employees might become insider threats?

Should whistleblowers be classified as insider threats, or are they serving a greater ethical duty?

Should companies be held legally accountable if an insider threat succeeds due to lax internal controls?

Can transparency with employees reduce the risk of insider threats, or does it make systems more vulnerable?

# Questions?