Cloud Security

ITN 4252 Advanced Topics in Networking

Partially based on resources from Cisco, Palo Alto, Snyk, AWS, and Microsoft

Year Over Year The Cloud Attack Surface Grow

Supply Chain Attacks

$50B

The cost of supply chain attacks in 2023 alone

Infosecurity Magazine

Data Loss

1/2 of orgs

Were victims of a significant data leaks in the last

Infosecurity Magazine

Cloud Breaches

82%

of breaches involved data in public, private or a combination of multiple clouds.

IBM

Artificial Intelligence

Seconds

The time it will take AI to find vulnerabilities

Security Intelligence

Average cost of a public cloud breach: $4.45 Million IBM

Modern Cloud Applications

INNOVATION

75%

Public cloud will be the primary platform by 2026

- Gartner

77%

Continuous delivery; every week

- Palo Alto Networks

10X

Generative AI acceleration of software

- Ark Invest

RISK

80%

OSS with Vulnerabilities

- Forrester

15 min

to exploit New Vulnerabilities

- Palo Alto Networks

40%

Generative AI proliferation of insecure code

- Cornell University

People cause 82% of cloud breaches

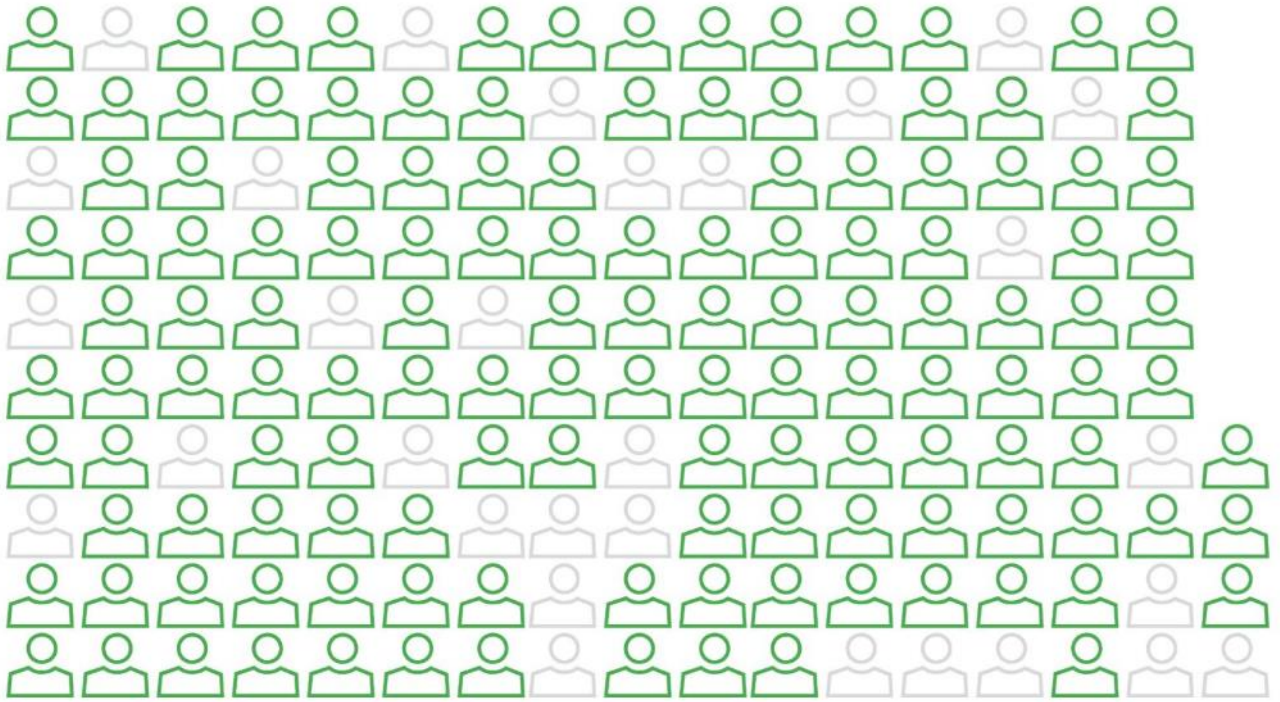


Figure 9. The human element in breaches (n=4,110)
Each glyph represents 25 breaches.

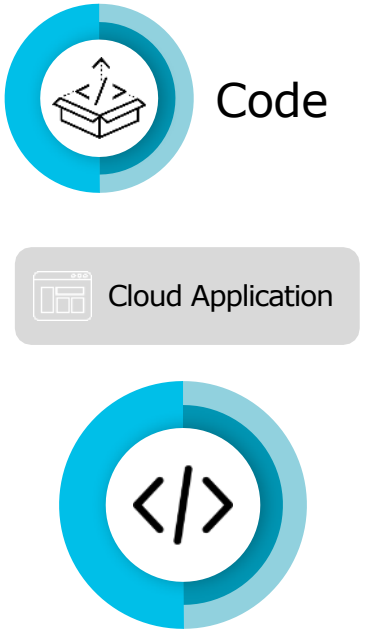
"The human element drives breaches. Errors caused by shipping malicious packages, misconfigured templates, or using stolen credentials play the most significant role in both incidents and breaches." – Verizon 2022 DBIR

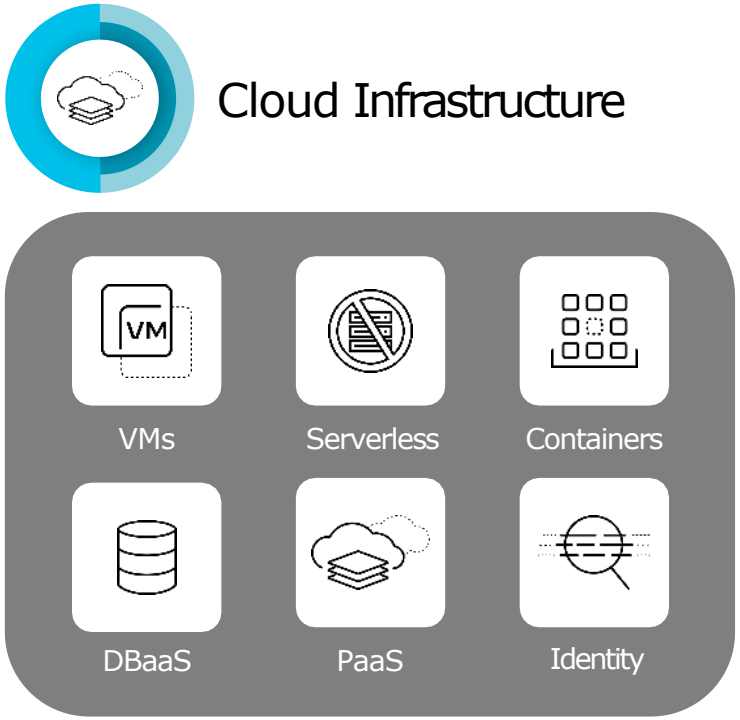
Why current approaches fail

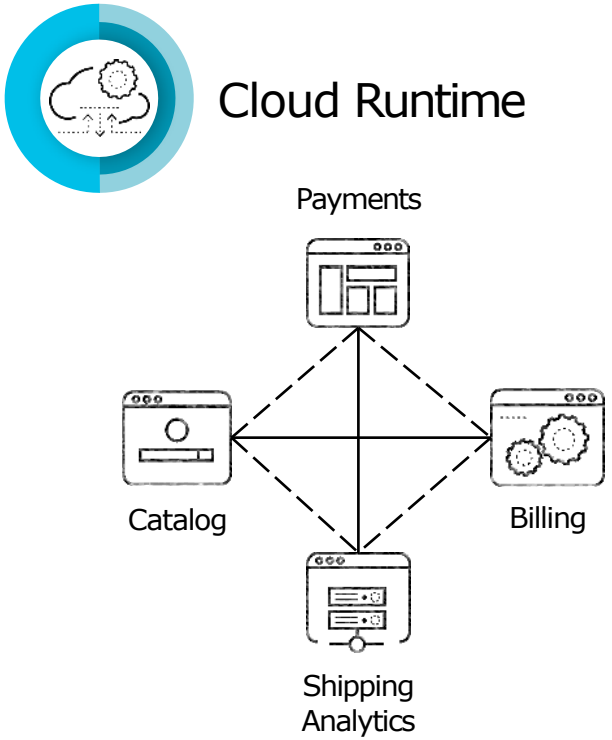
This leads to the rise in attacks

- Snowflake Data Theft (2024):
  - Data theft attacks targeted customers of Snowflake, a data warehousing company.
- AT&T Data Breaches (2024):
  - AT&T experienced two significant data breaches. The first breach in March exposed 73 million customer records, while the second breach in July affected nearly all of its customers, totaling around 110 million people.
- Football Australia Data Leak (2024):
  - Leaked secret keys opened access to 127 AWS buckets of data, including ticket buyers' personal data and players' contracts.
- Uber Data Leak (2023):
  - The personal information of more than 77,000 Uber customers was leaked due to a misconfigured cloud environment.
- CircleCI Malware Attack (2023):
  - A malware attack on a CircleCI engineer's laptop exposed secrets.
- CodeCov Supply Chain Attack (2022):
  - The CodeCov supply chain attack remained undetected for months and potentially affected nearly all major technology companies.

Everything in cloud starts as code

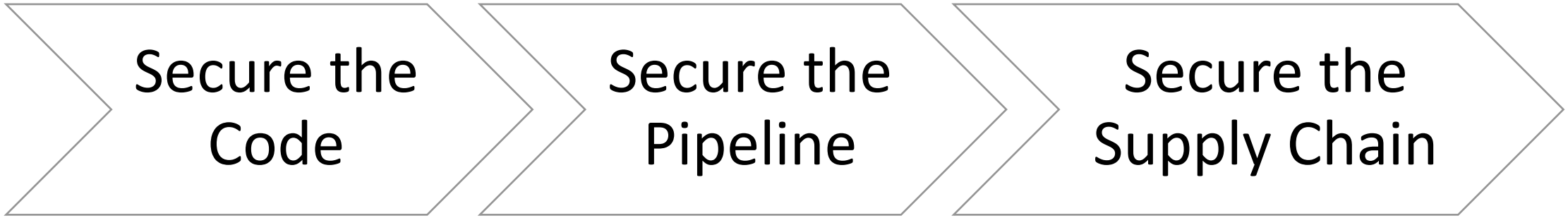






One issue in code → Becomes hundreds in runtime

Secure the Cloud



Secure the Code

- Easily implement Policy-as-Code
  - Enable developers to fix code flaws as they write
- Fix vulnerabilities at the source
  - Prioritise and fix vulnerable packages in code
- Prevent insecure code from reaching production
  - Prevent runtime risks with granular guardrails

Static Code Analysis (SCA)

- Scan code early
  - Integrate static code analysis tools into your development process.
  - These tools analyse code for security vulnerabilities without executing it.
- Automate scans
  - Run SCA scans automatically during code commits or builds.
  - Identify and fix issues before they propagate to production.

Dependency Scanning

- Monitor dependencies
  - Regularly scan third-party libraries and components for known vulnerabilities.
- Update dependencies
  - Keep dependencies up to date by applying security patches and fixes.

Code Reviews

- Peer reviews
  - Conduct thorough code reviews to catch security flaws, coding errors, and insecure practices.
- Security-focused reviews
  - Specifically look for security-related issues during code reviews.

Automated Testing

- Unit tests
  - Write and run unit tests to validate code behaviour and identify vulnerabilities.
- Integration tests
  - Test interactions between components to ensure security and functionality.

Secrets Management

- Avoid hardcoding secrets
  - Never store sensitive information (such as API keys, passwords, or tokens) directly in code.
- Use environment variables or secret management tools
  - Store secrets securely outside the codebase.

Key Management Service (KMS)

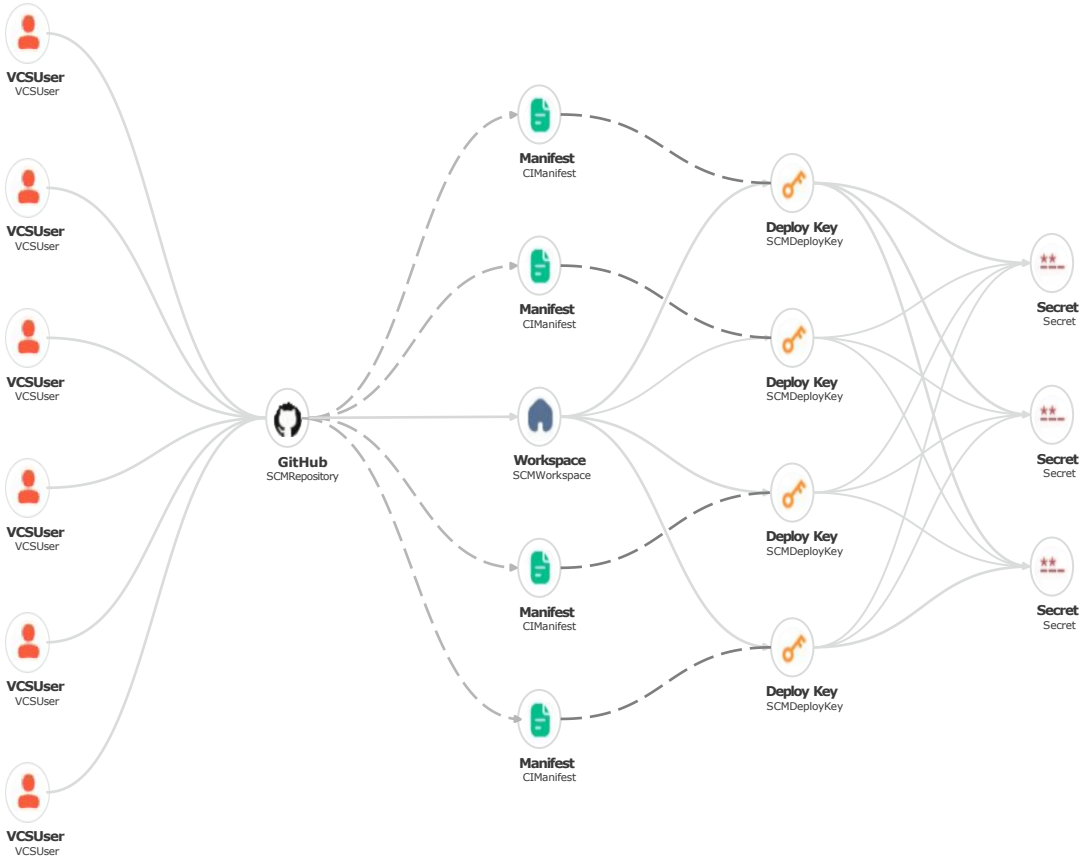
- A KMS enables encryption operations using cryptographic keys
- Key Management
  - Create, manage, and use cryptographic keys
  - Control key usage across various services and applications
- Access Control
  - Specify which users and roles can manage keys
  - Temporarily disable keys to prevent use
  - Keys remain secure and under your control

Secure the Pipeline

- Gain visibility across your Software Development Lifecycle (SDLC)
  - Gain visibility across repos, contributors, languages, etc.
  - Identify potential security issues early in the development process.
- Protect your CI/CD pipeline against the OWASP Top 10
  - Protect the delivery pipeline against the Top 10 CI/CD risks
  - Continuously monitor and update security measures.

Attack Path Analysis

- Analyse your attack surface with the Application Graph
  - Visualise and understand relationships and interactions within applications.
  - Identify how different components are connected and where security measures might be lacking.
- Uncover Breach Pathways with Graph Modelling
  - Graph modelling allows you to analyse potential pathways that an attacker might take to breach your system.
  - By understanding the pathways and connections, you can prioritise threats based on their potential impact and likelihood, allowing for more effective and targeted security measures.



Pipelines as Code

- Automate Pipelines
  - Define your CI/CD pipelines as code (YAML or other formats).
  - Store them alongside your application code.
- Version Control
  - Keep pipeline definitions in version control systems (VCS) to track changes and ensure consistency.

Version Control Systems (VCS) Workflow

- Code Management
  - Use VCS to manage code changes, including infrastructure as code (IaC) and pipeline definitions.
  - VCS allows multiple developers to work on the same project simultaneously without overwriting each other's work.
- Pull Requests
  - Implement pull requests for code review and collaboration. Only merge approved changes into protected branches.
  - Pull requests help maintain code quality by catching bugs and issues early through peer reviews and automated testing.

Restricted Access to Protected Branches

- Protected Branches
  - Designate specific branches (e.g., production or releases) as protected.
  - Only allow changes via pull requests.
- Enforce Workflow
  - Configure the server to reject direct changes to protected branches.
  - Developers must create pull requests targeting these branches.

Encryption

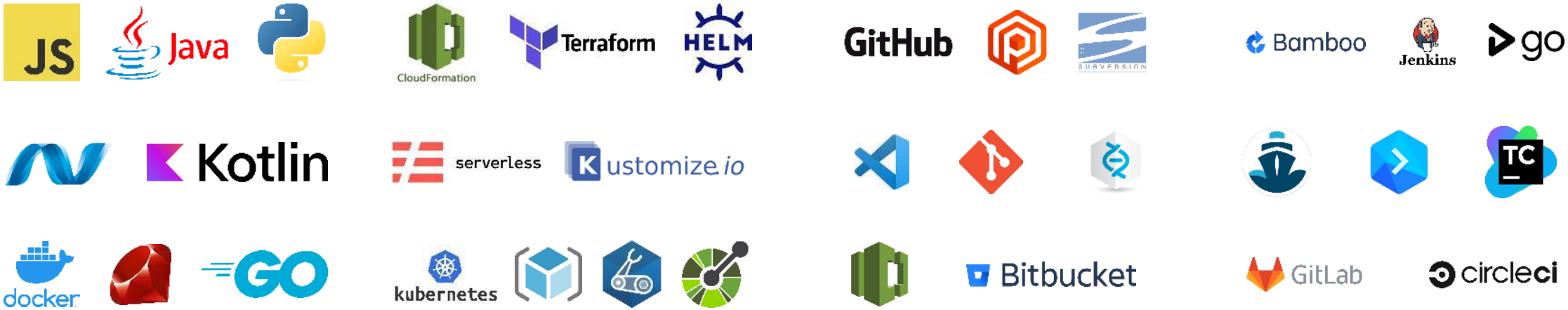
- Encryption at Rest
  - Data is stored securely and protected from unauthorised access
  - Example: Server-side encryption with key management
- Encryption in Transit
  - Data is encrypted during transfer between systems
  - Example: Secure Sockets Layer (SSL) connections

Secure the Supply Chain

- Govern usage of your ecosystem
  - Gain visibility across the ecosystem and control dependencies
- Maintain compliance with trusted artifacts
  - Monitor software supply chain and generate SBOM of ecosystem
- Detect and prevent drift with tracing
  - Trace the source of issues and alert on workloads that deviate from source code

Visibility and Discovery

- Identify Components
  - Discover all components in your supply chain, including dependencies, libraries, and third-party software.
- Catalogue Assets
  - Maintain an inventory of software assets, their versions, and associated risks.



Security Services

- Automated Security Assessments
  - Run security checks on your infrastructure
  - Identify vulnerabilities and provide remediation recommendations
- Threat Detection
  - Analyse metadata and network activity for threats
  - Use machine learning and threat intelligence for accurate detection

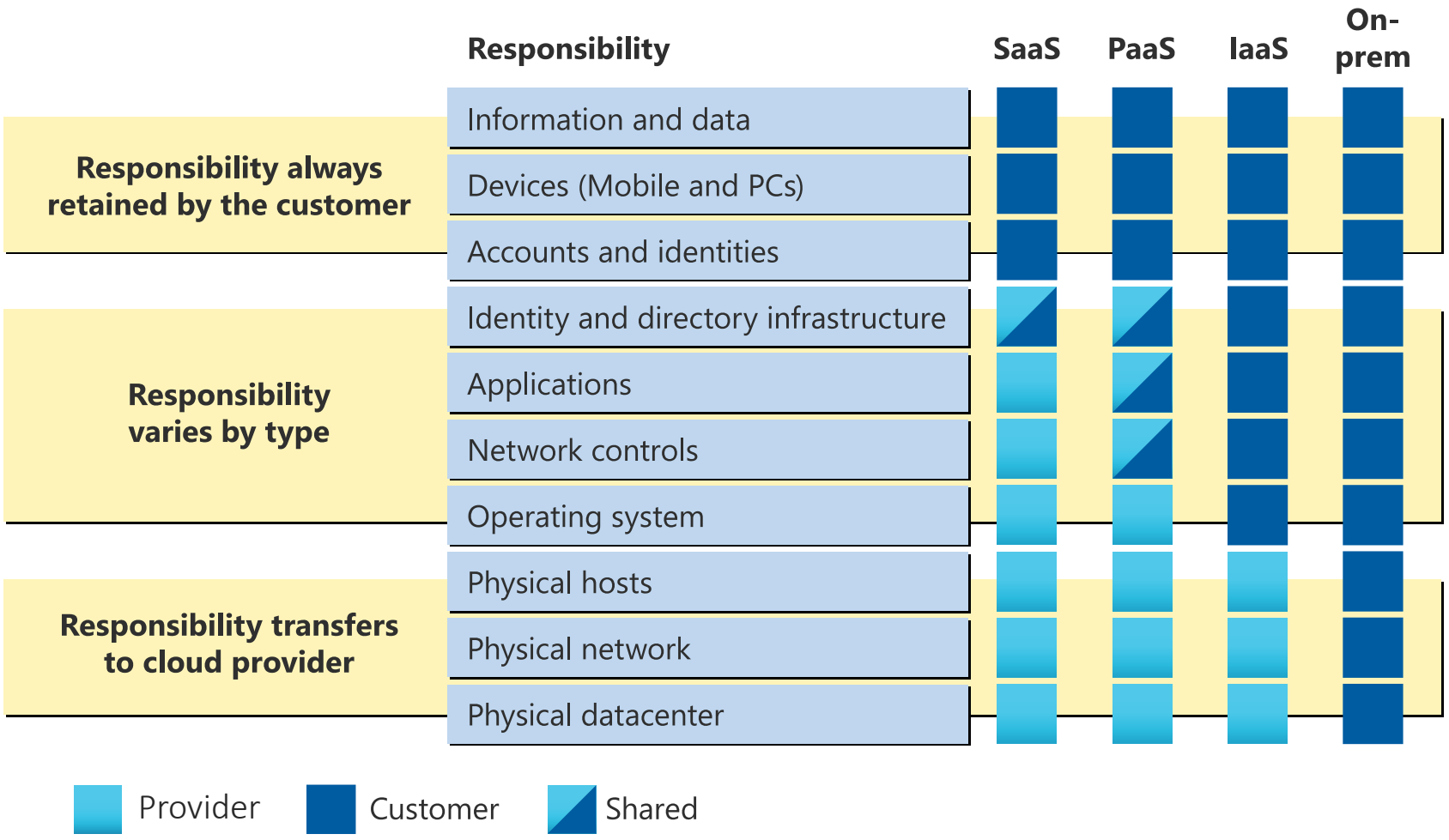
Risk Assessment and Scanning

- Vulnerability Scans
  - Regularly scan components for known vulnerabilities.
  - Use tools like SCA (Software Composition Analysis) to identify security issues.
- License Compliance
  - Check licenses of third-party components to ensure compliance and avoid legal risks.

Supply Chain Auditing and Monitoring

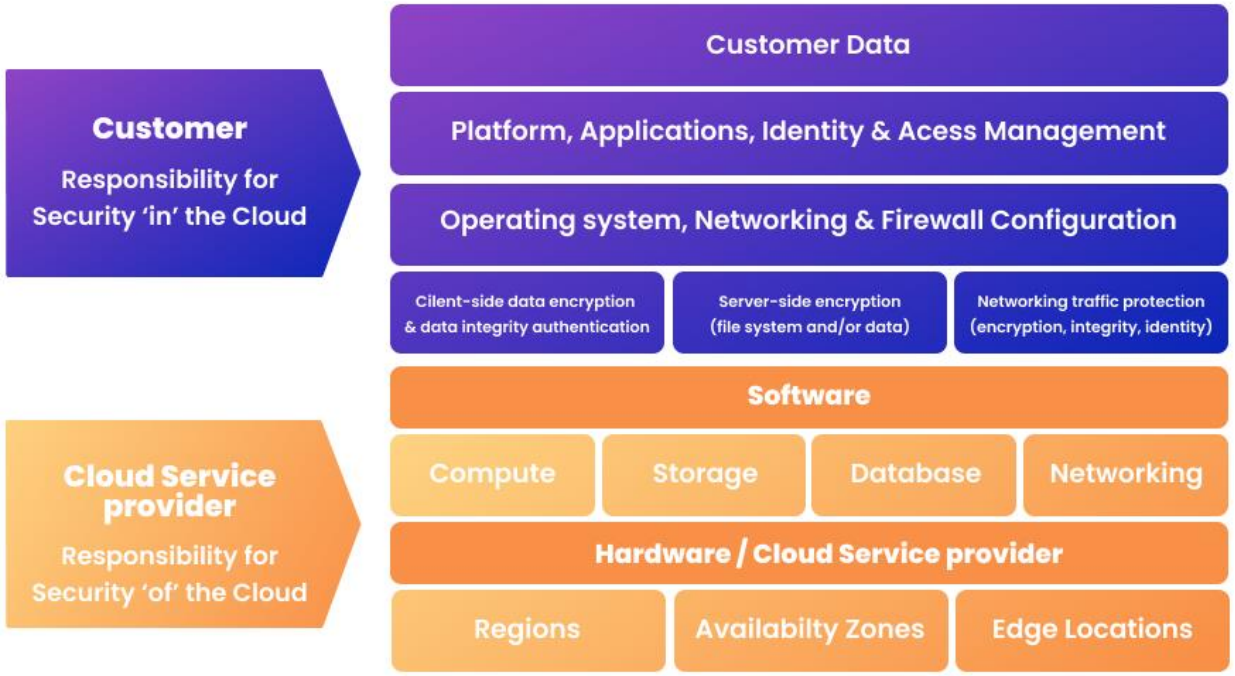
- Continuous Monitoring
  - Monitor supply chain components for changes or anomalies.
- Audit Trail
  - Maintain an audit trail of supply chain activities.

Who does what…



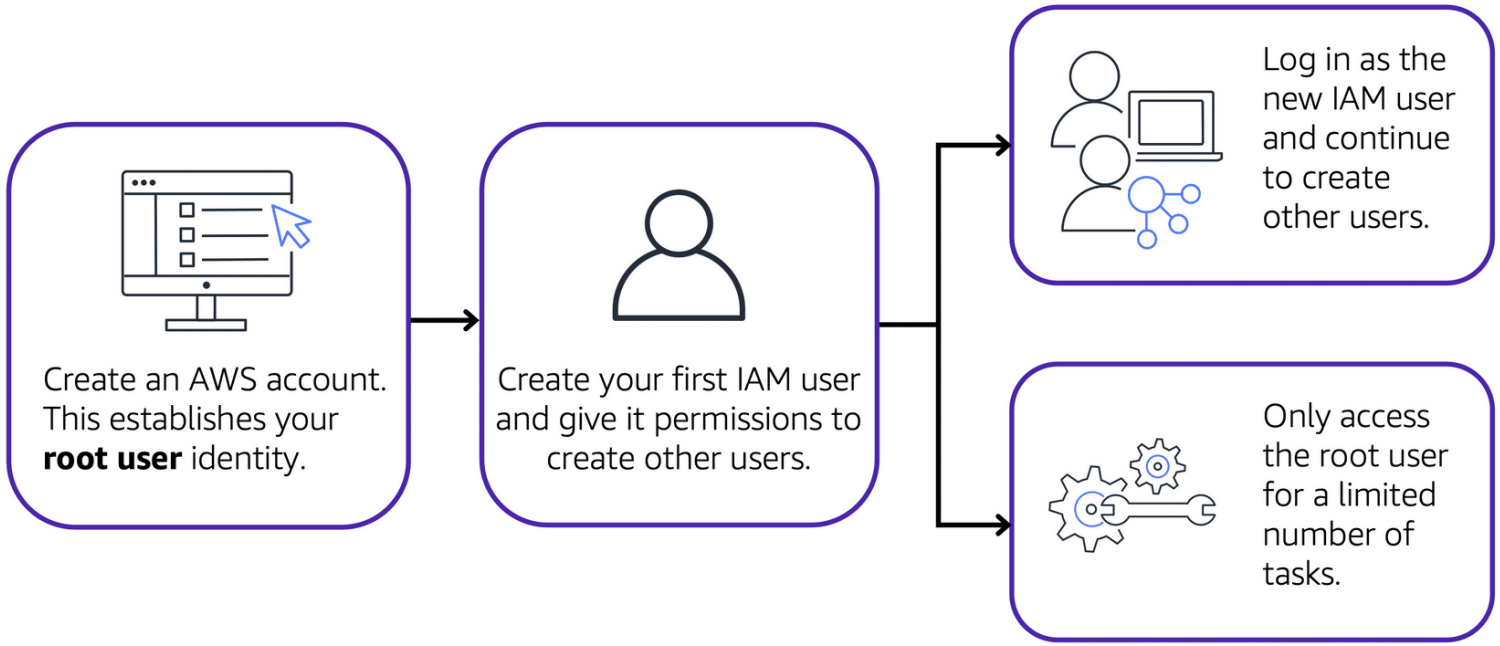
Shared Responsibility Model

- Customer Responsibilities ("Security in the Cloud")
  - Security of everything created and stored in the cloud
  - Control over content, access rights, and security requirements
  - Tasks include:
    - Selecting, configuring, and patching operating systems
    - Configuring security groups
    - Managing user accounts
- Service Provider Responsibilities ("Security of the Cloud")
  - Security of the infrastructure and services
  - Manages components at all infrastructure layers
  - Responsibilities include:
    - Physical security of data centres
    - Hardware and software infrastructure
    - Network infrastructure
    - Virtualisation infrastructure



Identity and Access Management

- Employee Identity and Access
  - Each user has a unique login and access permissions
- Owner's Access
  - Owner has unrestricted access to all systems



Identity and Access Management Principles

- Granular Access Control
  - Use of identity and access management (IAM) to control permissions
  - Default no permissions for new users; explicit permissions required
- Least Privilege Principle
  - Grant users only the access they need
  - Use IAM policies to define permissions (allow or deny actions)

Managing Permissions, Roles, and Federation

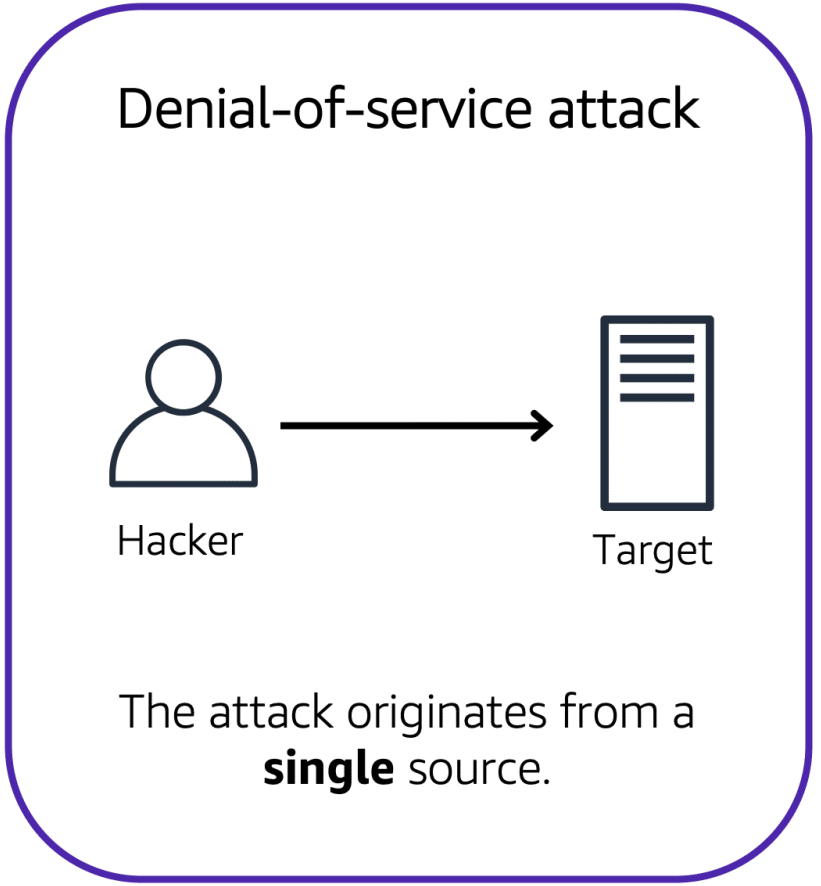
- IAM Policies
  - JSON documents specifying allowed or denied actions
  - Example: Allowing a user to list contents of a specific storage bucket
- IAM Groups
  - Grouping users to manage permissions collectively
  - Example: Granting all cashiers access to the register
- Roles
  - Temporary permissions for users, applications, or services
  - Example: Assigning different roles to an employee based on daily tasks
- Federation
  - Using corporate credentials to access cloud services
  - Mapping corporate identities to IAM roles for streamlined access

Multi-Factor Authentication (MFA)

- MFA is important for enhanced security in cloud environment
  - Essential for root users (and best to have for all)
  - Requires multiple pieces of information to verify identity
  - Adds an extra layer of security to your account
  - Example: Password + random code sent to your phone
- MFA device could be:
  - Hardware security key
  - Hardware device
  - MFA application on a smartphone

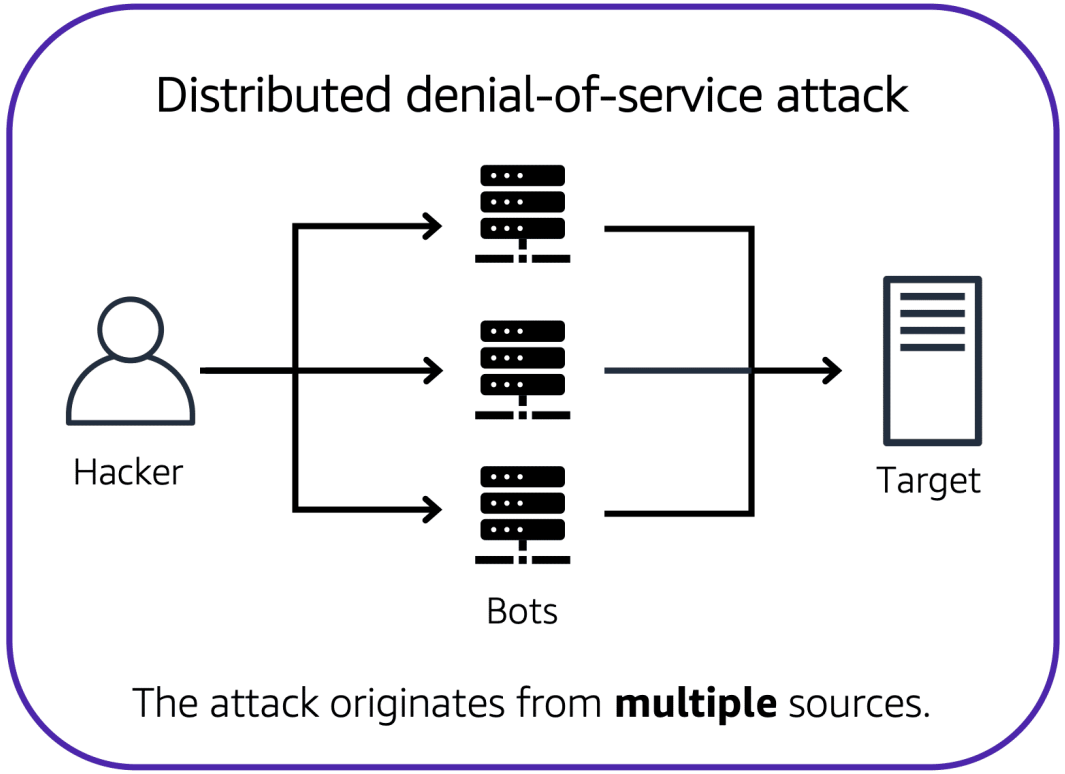
Denial-of-Service (DoS) Attacks

- A deliberate attempt to make a website or application unavailable to users
- Single threat actor targets a website or application
- Example
  - Attacker floods a website with excessive network traffic
  - Website becomes overloaded and unresponsive, denying service to legitimate users



Distributed Denial-of-Service (DDoS) Attacks

- Multiple sources are used to start an attack
- Aims to make a website or application unavailable
- Example
  - Multiple attackers or infected computers (bots) send excessive traffic



Common DDoS Attack Tools

- Low Orbit Ion Cannon (LOIC): An open-source stress testing tool for TCP and UDP attacks, with a user-friendly interface. Web-based derivatives exist.
- High Orbit Ion Cannon (HOIC): An advanced version of LOIC using HTTP for targeted attacks, requiring coordinated efforts of at least 50 people.
- R.U.D.Y (R-U-Dead-Yet): A point-and-click tool for slow attacks, using multiple open HTTP POST requests to gradually overwhelm servers.
- Slowloris: A low-resource tool for slow attacks on servers, keeping connections open to exhaust server resources.
- UDP Flood: Fake requests overload your server with data
- HTTP Level Attacks: Bots mimic normal user requests to exhaust resources

Defending Against DDoS Attacks

- Fundamental Defence Strategies
  - Security Groups: Allow only proper request traffic
  - Load Balancers: Handle traffic efficiently and scale to meet demand
  - Rate limiting: Limiting the number of requests a server will accept over a certain time window
- Advanced Defence Tools
  - Web Application Firewalls (WAF): Filter incoming traffic for malicious patterns
  - Machine Learning: Recognise and adapt to new threats
- A well-architected system inherently defends against most DDoS attacks
  - Use advanced tools and best practices to enhance security

Web Application Firewall (WAF)

- A web application firewall that monitors network requests to web applications
- How WAF Works
  - Works with content delivery and load balancing services
  - Uses web access control lists (ACLs) to block or allow traffic
- Blocking Malicious Requests
  - Identify and block requests from specific IP addresses
  - Ensure legitimate users can still access the application
- Process
  - Configure web ACL to allow all requests except those from specified IP addresses
  - WAF checks incoming requests against the web ACL rules
  - Allows access if the request is not from a blocked IP address
  - Denies access if the request is from a blocked IP address

Incident Response and Recovery

- Plan for Incidents
  - Develop incident response plans specific to supply chain security.
- Backup and Recovery
  - Regularly back up critical components and have recovery procedures in place.

Cloud security best practices

- Know Your Responsibility
  - Understand the shared responsibility model. While cloud service providers secure the infrastructure, you are responsible for securing your data, applications, and user access.
  - Manage and secure anything you place on the cloud.
- Integrate Compliance
  - Regulations drive demand for next-gen cloud security services. Integrate compliance into your daily activities.
  - Monitor your network topology and stay alert to any policy changes.
- Secure the Perimeter
  - Implement perimeter security measures to protect against external threats.
  - Regularly monitor for misconfigurations and unauthorised access.
- Identity and Access Management (IAM)
  - Control user access to cloud resources using IAM.
  - Enforce least privilege principles and regularly review permissions.
- Incident Response and Recovery
  - Develop incident response plans specific to cloud security incidents.
  - Regularly back up critical components and have recovery procedures in place.

Summary

- Cloud security is essential for **protecting sensitive information**, managing permissions, and safeguarding against malware attacks in the cloud infrastructure.
- Cloud security ensures that users can access their data at any time, which is vital for **business continuity**.
- Many industries have regulations requiring them to protect customer data and privacy. Cloud security helps businesses **comply with these regulations**.
- In the cloud, security is a **shared responsibility** between the cloud service provider and the user.
- Cloud security can **enable better business outcomes** by being fast and frictionless.