Cloud Application Security for CCSP®

Cloud Application Security Testing

Kevin Henry
CISM CISSP CCSP

kevin@kmhenrymanagement.com

Cloud Application Security

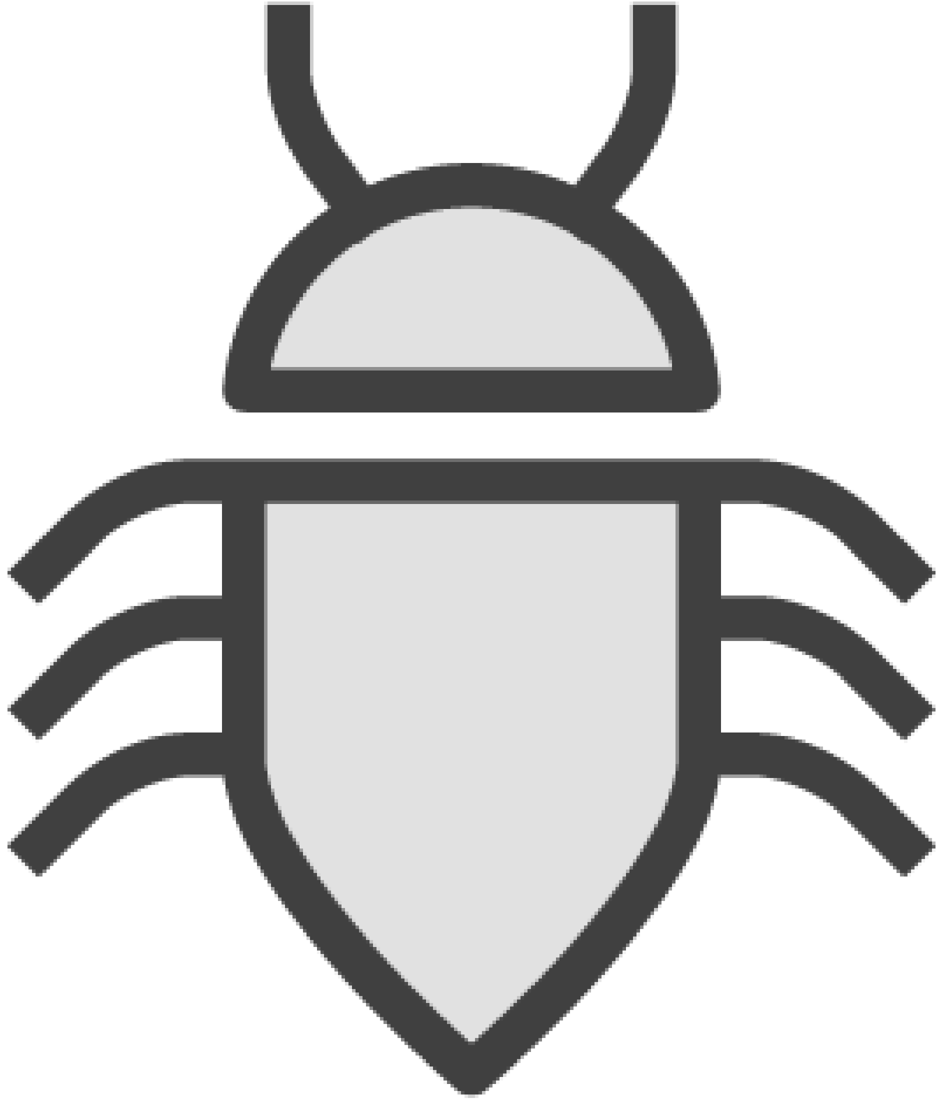
Agenda:

Cloud Application Development Security

Cloud Application Security Testing

The Purpose of Testing

Testing Objective



Prevent release of bad software into production

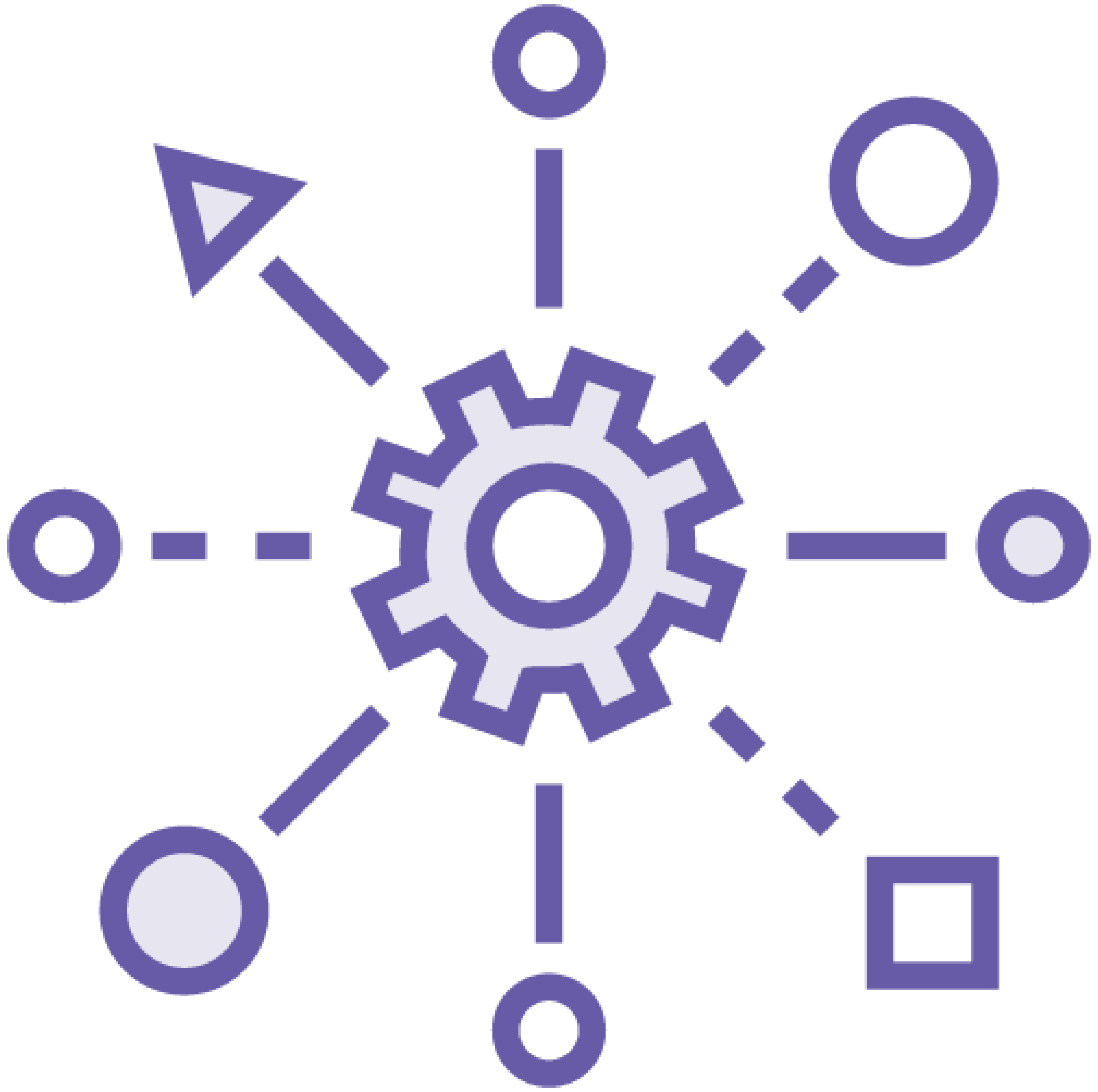
- Discover any flaws or bugs in software
- Ensure that application functionality works as intended/required

Verification

Ensure that the software works

- All functionality in the design is provided in the deliverable

Validation



Ensure that it is the right application for the business requirement

Systems Authorization

Security Control Assessment (previously known as Certification) reviews the software throughout the development to ensure that:

- Risk was properly identified
- Adequate controls were designed
- Controls were implemented and tested

Systems Authorization

Management approves the system for deployment (formerly known as accreditation) based on the acceptance of risk and the results of the security control assessment

Testing Methodologies

Testing

Unit tests

- White box – SAST

Integrated tests

- Black box – DAST

IAST – Interactive Application Security Testing

Regression tests

Sociability testing

- Operational environment

ISO 15408 – Common Criteria

Testing of security in system components

- Tests functionality in relation to the rigor of the test
    - Security Functional Requirements
    - Evaluation Assurance Levels

Types of Tests

Vulnerability Assessments

Penetration Tests

Tests for Application Security

PA-DSS

CSA Treacherous Twelve

NIST SP 800-115

OWASP Top Ten - 2021

Critical Web Application Security Risks

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server Side Request Forgery (SSRF)

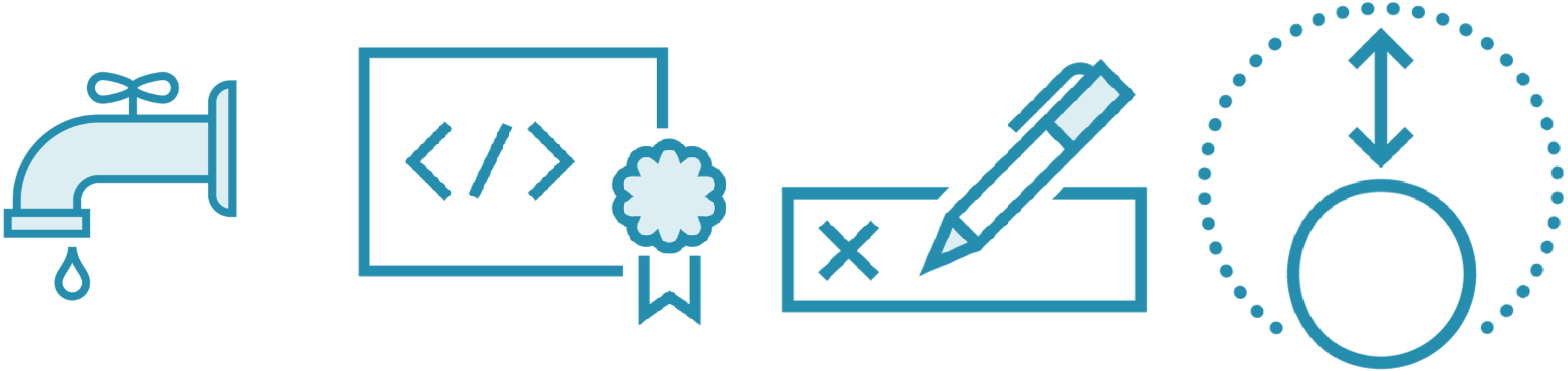
Benefits of Cloud-based Development

Versatile environment

Similar to production environment

Collaborative teams

Cloud Development and Testing Risks



Disclosure of sensitive data
- Jurisdiction

Ownership of code
- Escrow

Contractual disputes

Change management

Key Points Review

Testing should be required – not optional

Tests should be thorough and creative to discover any vulnerabilities

Verified Secure Software

Open Source Software

Many advantages – but also disadvantages

- Trusted source
- Thoroughly tested

APIs

Library of trusted (tested) APIs

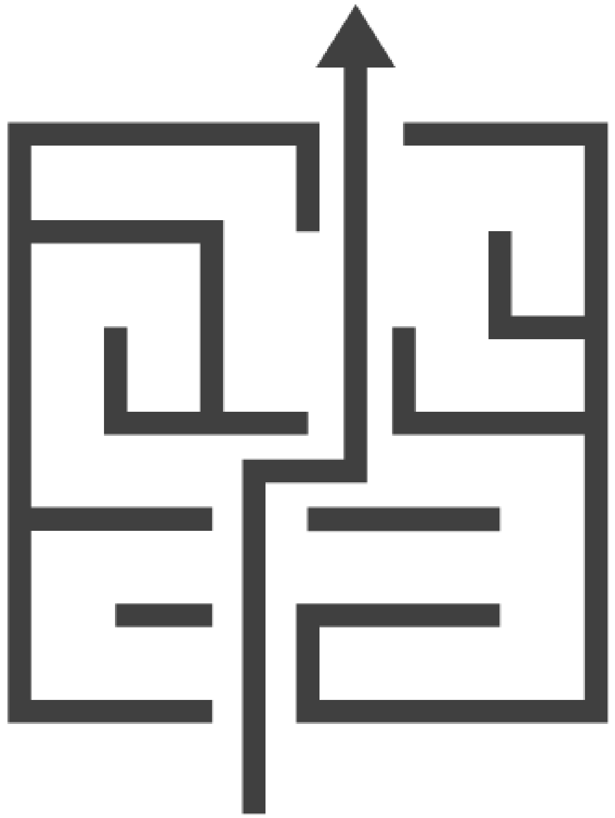
Prohibit use of untested APIs

Malicious modules found in NPM library were downloaded thousands of times
https://www.itworldcanada.com

Proprietary Software

Difficult to do in-depth testing

Signed software and patches



Proper configuration

Escrow

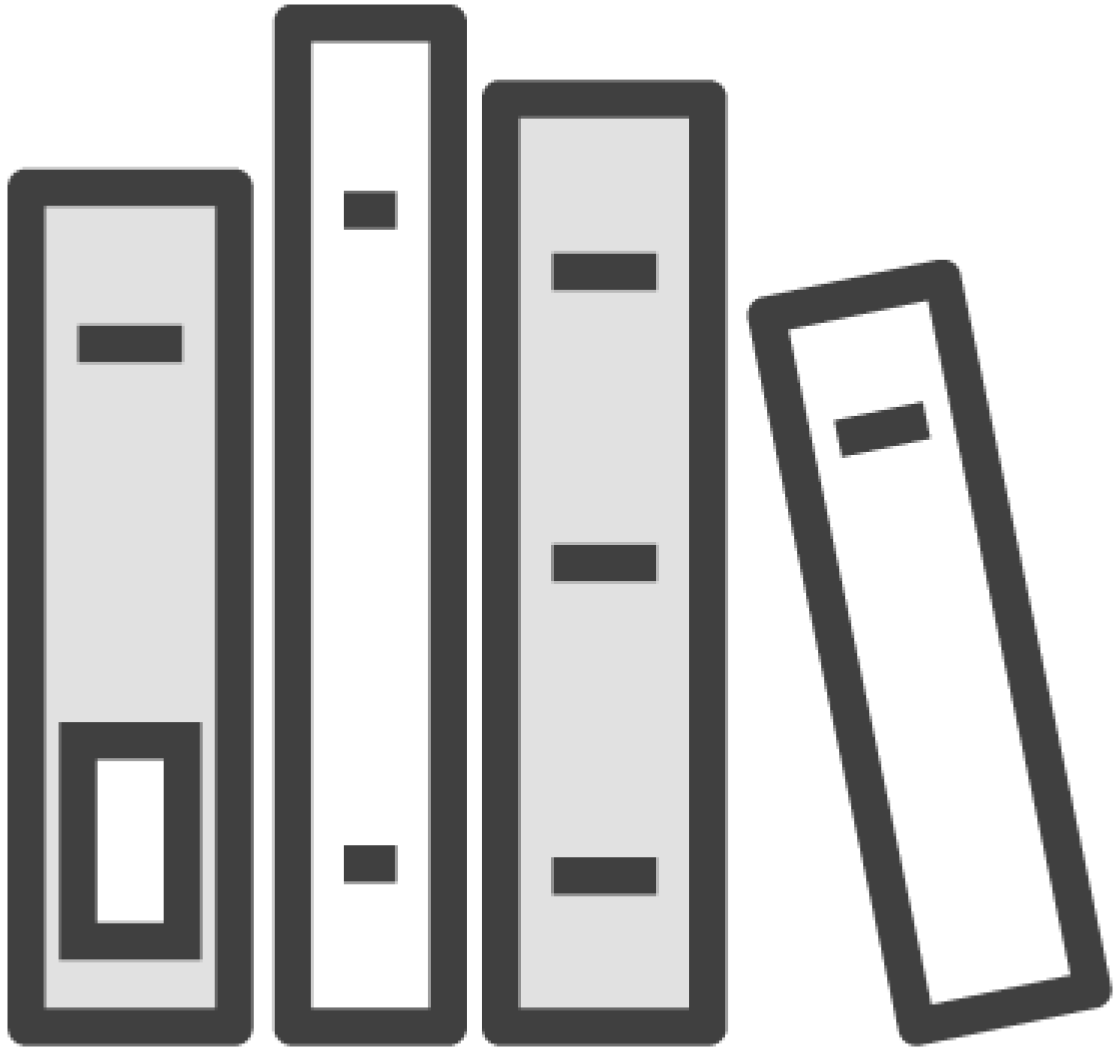
Summary

Software is on the front line of the organization and provides the interface to the outside world as well as support for business functions

It must be secure and have required levels of performance

Secure Application Standards

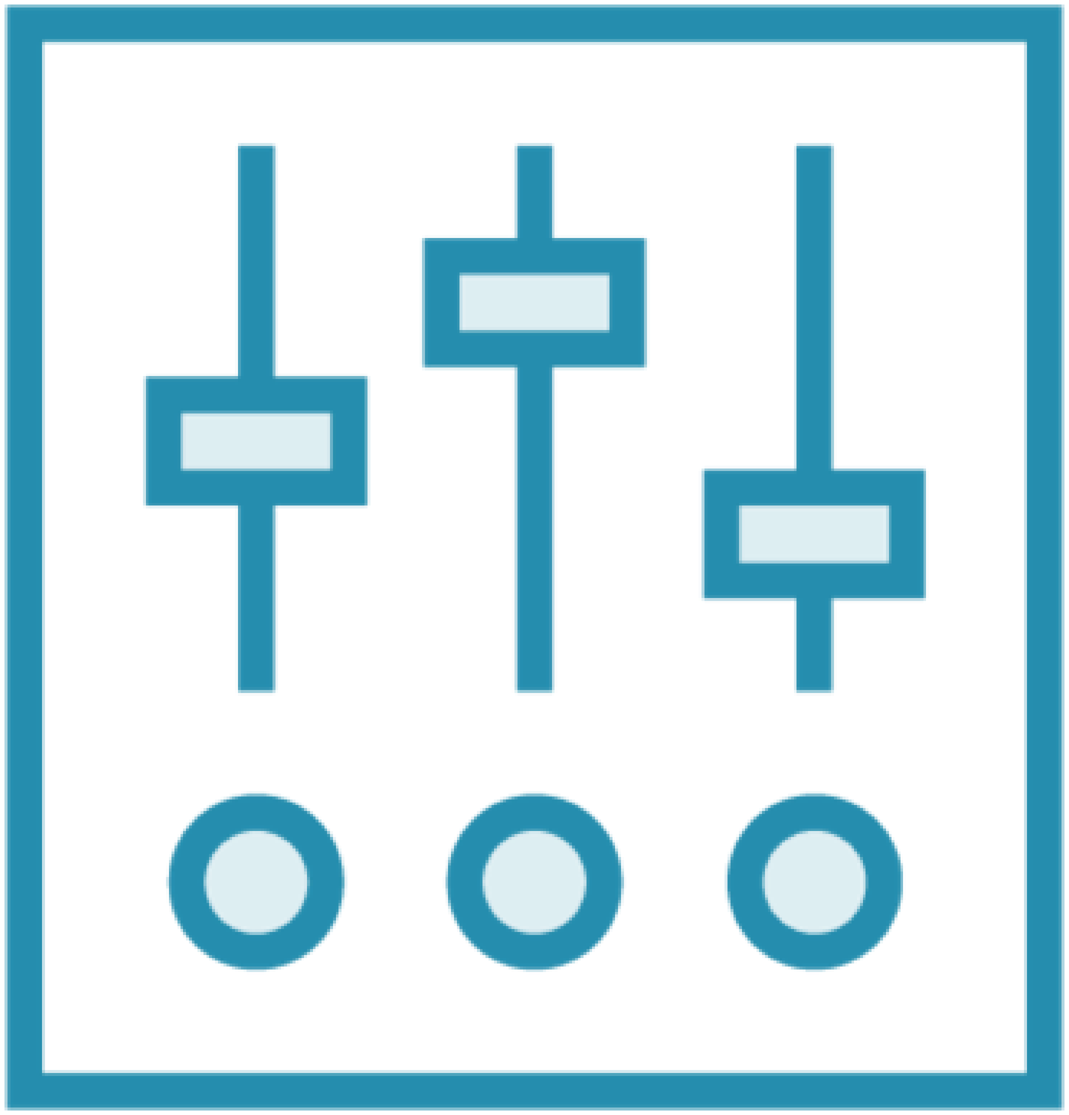
ISO/IEC 27034



Standard for Application Security

- ONF – Organizational Normative Framework
    - Library of security controls used by the Organization

ISO/IEC 27034

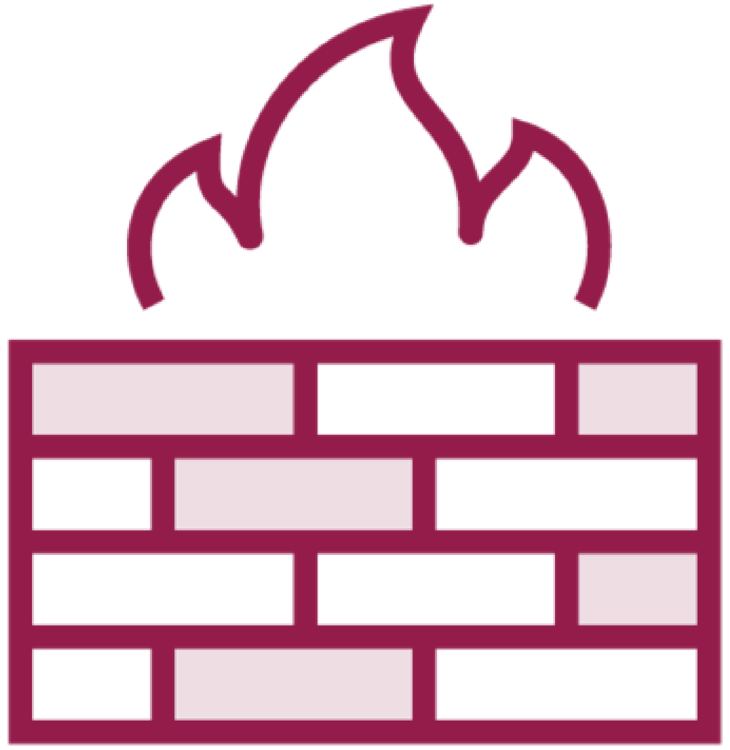


ANF – Application Normative Framework

- The specific security controls used in an application
- A subset of the ONF

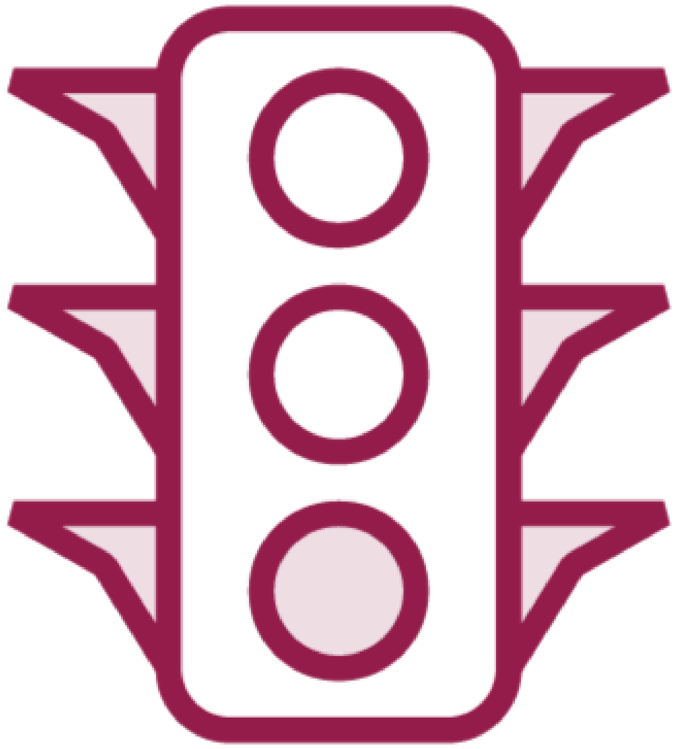
Cloud Security Components

Network Security



Network Firewall

- Managed by CSP or Customer
- At security perimeter and internally

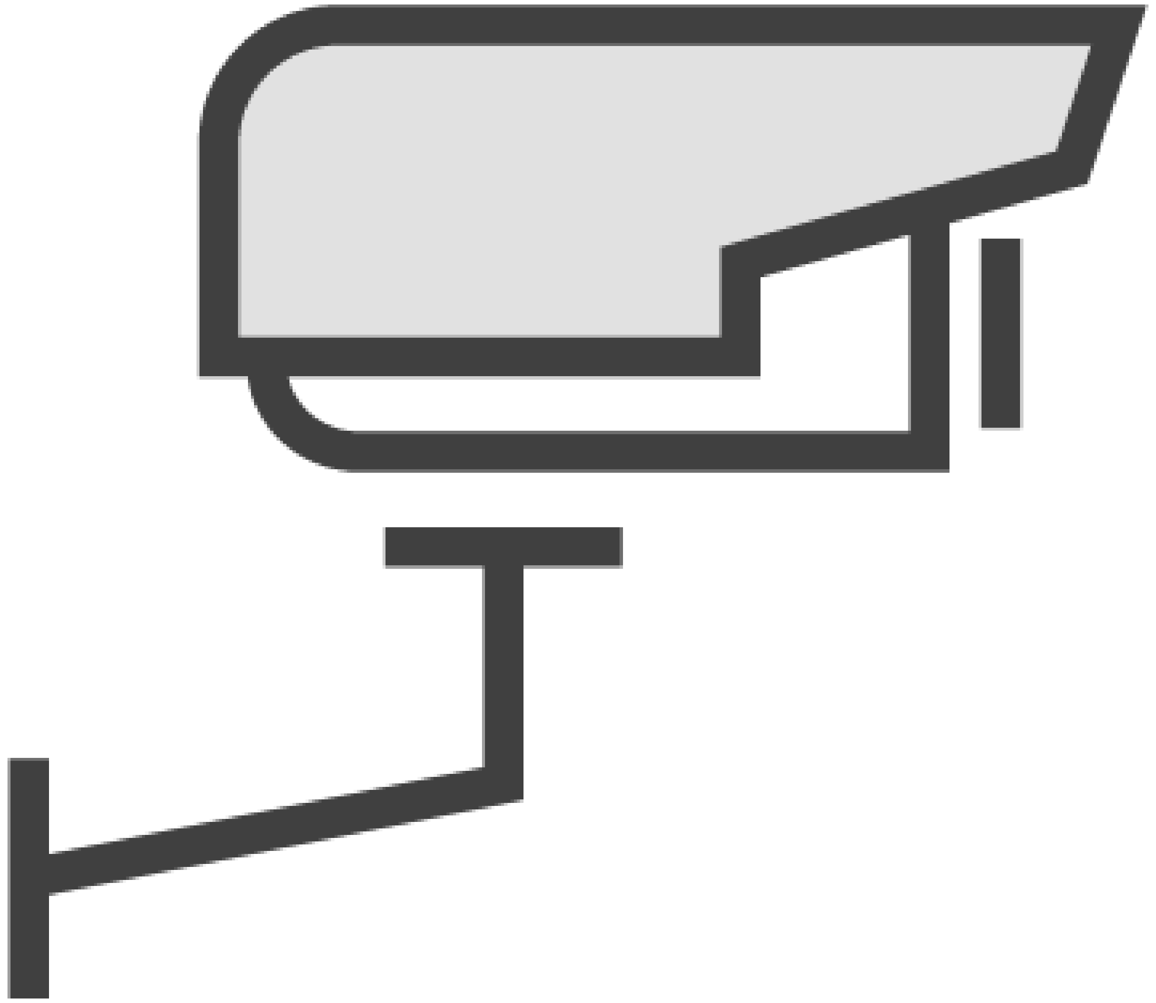


Web Application Firewall (WAF)

- In-depth examination of traffic to web application

Defense in depth

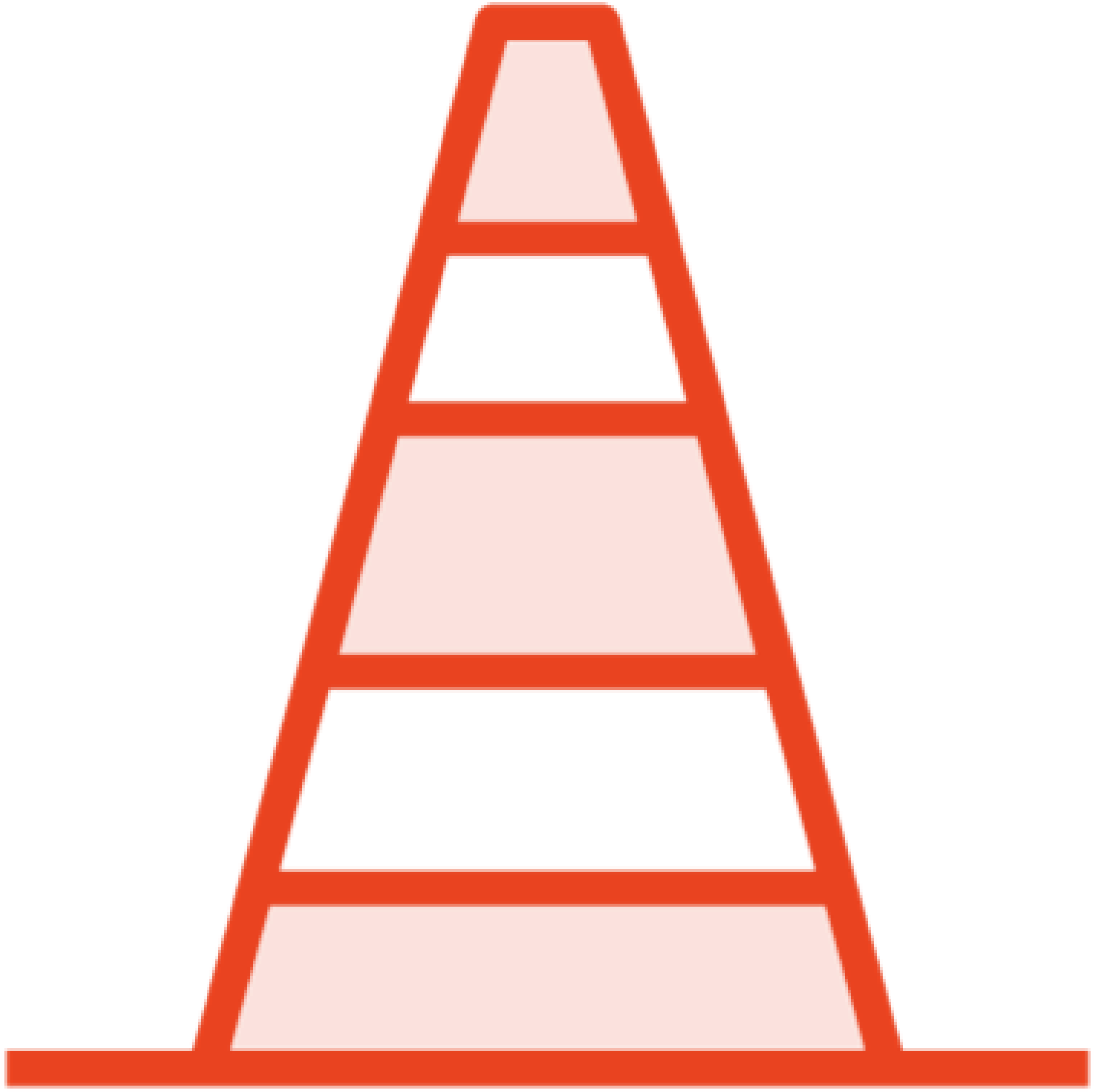
Cloud Security Components



Network and Host-based

- IDS/IPS
    - Monitor and log network traffic
    - Detect changes or requested changes on a host
    - Alert to suspicious traffic or changes
        - Block suspicious activity

Cloud Security Components



API Gateways

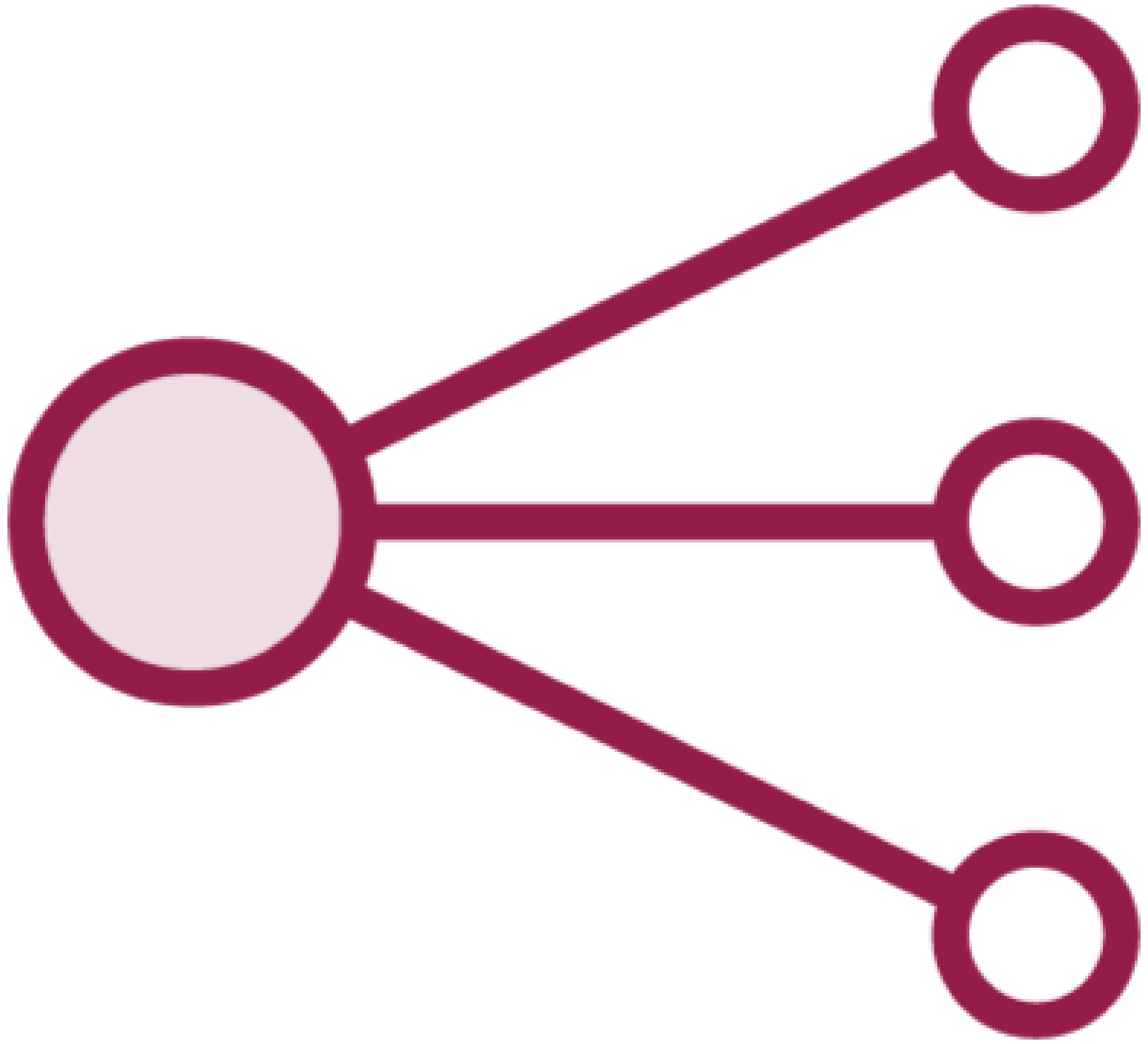
- Monitor/manage traffic at API level
  - Logging
  - Proxy services
  - Limiting bandwidth utilization
  - Manages API level access control

Cloud Security Components

Database Activity Monitoring (DAM)

- Monitor and manage traffic to the database
  - Excessive requests or volumes of traffic

Cloud Security Components



Load Balancing

- Assist with availability
  - Improve response times
  - Adjust to network or equipment failures
    - Software defined networking
    - Content distribution networks

Cloud Security Components

Hardware

Isolation

- Multi-tenancy

Supply chain

- Security
- Reliability

Disposal

Cloud Security Components

Sandboxing

- Isolation
  - VM
  - Containers
- Secure configuration

Cloud Security Components

Cryptography

Selection of algorithms

- Built into applications
- Built into databases

Key management

- HSM – hardware security module
- Who has the key?
- CSP using the same keys for stored data of multiple consumers

Cloud Security Components

Orchestration

Scheduling

Dependencies

Key Points Review

The security of applications is dependent on the security of the infrastructure and networks the application runs on

And on the knowledge of the staff managing the security controls