



#### Membership

[Join as a Business](#)  
[Cloud Customers](#)  
[Cloud Solution Providers](#)  
[SaaS Solution Providers](#)  
[CxO Initiative](#)  
[Contact Us](#)  
[Current Business Members](#)  
[Cloud Customers](#)  
[Cloud Solution Providers](#)  
[Join as an Individual](#)  
[Regional Chapters](#)  
[Circle Community Forum](#)  
[Research Working Groups](#)

#### STAR Program

[STAR Registry](#)  
[STAR Home](#)  
[Submit to Registry](#)  
[Provide Feedback](#)  
[What is the STAR Registry?](#)

Learn how to stay compliant in the cloud.

#### [CCAK Training](#)

Governance, Risk & Compliance Tools

[Cloud Controls Matrix \(CCM\)](#)

[Consensus Assessment Initiative Questionnaire \(CAIQ\)](#)

[GDPR Code of Conduct](#)

[STAR Level 1](#)

At level one organizations submit a self-assessment.

[View companies at level one](#)

[Learn about level one](#)

[STAR Level 2](#)

At level two organizations earn a certification or third-party attestation.

[View companies at level two](#)

[Learn about level two](#)

[CSA Approved STAR Assessment Firms](#)

Certificates & Training

[Events](#)

Learn and network while you earn CPE credits.

[Events](#)

[Virtual Events & Webinars](#)

[Certificates & Training](#)

[This website uses third-party profiling cookies to provide services in line with the preferences you reveal while browsing the Website. By continuing to browse this Website, you consent to the use of these cookies. If you wish to object such processing, please read the instructions described in our \[Privacy Policy\]\(#\)](#)

[Get the Cloud Security Knowledge \(CSK\)](#)

[Train my entire team](#)

[Training Instructors](#)

[Finders and](#)

[Become an Instructor](#)

[Training Partners](#)

[Become a Training Partner](#)

Research

[CSA Research](#)

[Latest Research](#)

[Working Groups](#)

[Open Peer Reviews](#)

[CxO Initiative](#)

[CloudBytes Webinars](#)

Awards & Recognition

[Ron Knode Awards](#)

[Research Fellows](#)

Industry Specific Research

[Financial Services](#)

[Healthcare](#)

Getting Started with CSA Research

[Best practices for cloud security](#)

[Assess your compliance to cloud standards](#)

[Security questionnaire for vendors](#)

[The top threats to cloud computing](#)

[View more](#)

Architectures and Components

[Enterprise Architecture](#)

[Hybrid Cloud Security](#)

Emerging Technologies

[Blockchain/Distributed Ledger](#)

[Internet of Things \(IoT\)](#)

[Quantum-safe Security](#)

Securing DevOps

[Application Containers and Microservices](#)

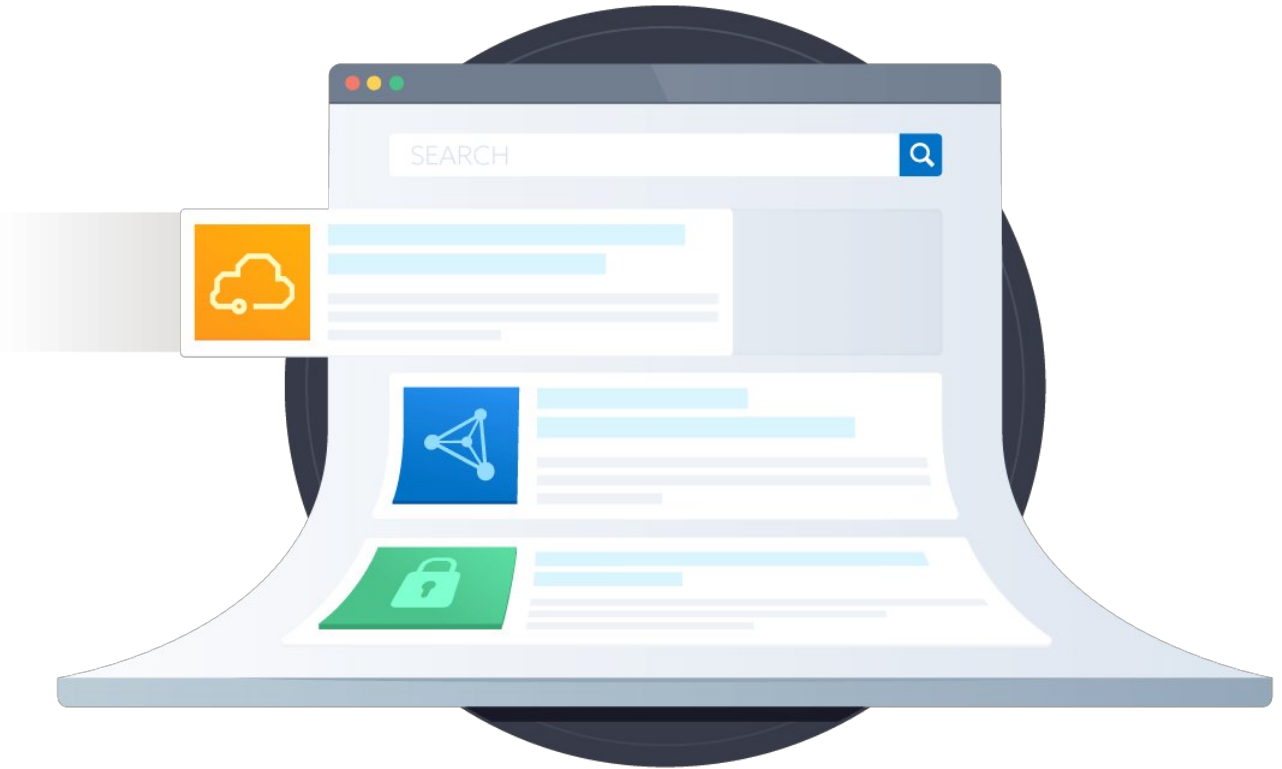
[DevSecOps](#)

[Serverless](#)

Security Services

[Support](#)

## How Security Changes With Cloud Networking

[Home](#)[Industry Insights](#)

How Security Changes With Cloud Networking

Blog Article Published: 09/08/2021



Common on-premises network practices work differently for the cloud user and provider due to the lack of direct management of the underlying physical network. The most commonly used network security patterns rely on control of the physical communication paths and insertion of security appliances. This isn't possible for cloud customers, since they only operate at a virtual level.



Communications between hosts are mirrored and inspected by traditional virtual or physical Intrusion Detection Systems, which are not supported in cloud environments. Customer security tools need to rely on an in-line virtual appliance, or a software agent installed in instances. This creates either a chokepoint or increases processor overhead, so be sure you really need that level of monitoring before implementing. Some cloud providers may offer some level of built-in network monitoring (and you have more options with private cloud platforms) but this isn't typically to the same degree as when sniffing a physical network.

### Challenges of Virtual Appliances

Since physical appliances can't be inserted (except by the cloud provider), they must be replaced by virtual appliances if still needed and if the cloud network supports the necessary routing. This brings the same concerns as inserting virtual appliances for network monitoring:

- Virtual appliances become bottlenecks, since they cannot fail open, and must intercept all traffic.
- Virtual appliances may take significant resources and increase costs to meet network performance requirements.
- When used, virtual appliances should support auto-scaling to match the elasticity of the resources they protect. Depending on the product, this could cause issues if the vendor does not support elastic licensing compatible with auto-scaling.
- Virtual appliances should also be aware of operating in the cloud, as well as the ability of instances to move between different geographic and availability zones. The velocity of change in cloud networks is higher than that of physical networks and tools need to be designed to handle this important difference.

Additionally, cloud application components tend to be more distributed to improve resiliency and, due to auto-

scaling, virtual servers may have shorter lives and be more prolific. This changes how security policies need to be designed:

- This induces that very high rate of change that security tools must be able to manage (e.g., servers with a lifespan of less than an hour).
- IP addresses will change far more quickly than on a traditional network, which security tools must account for. Ideally they should identify assets on the network by a unique ID, not an IP address or network name.
- Assets are less likely to exist at static IP addresses. Different assets may share the same IP address within a short period of time. Alerts and the Incident Response lifecycle may have to be modified to ensure that the alert is actionable in such a dynamic environment. Assets within a single application tier will often be located on multiple subnets for resiliency, further complicating IP-based security policies. Due to auto-scaling, assets may also be ephemeral, existing for hours or even minutes.

## Recommendations

### Infrastructure security of your provider or platform

- Make sure the provider (or whoever maintains the private cloud platform) has the burden of ensuring the underlying physical, abstraction, and orchestration layers of the cloud are secure. This follows the shared security model.
- Review compliance certifications and attestations.
- Check [industry-standard and industry-specific compliance certifications and attestations](#) on a regular basis to assure that your provider is following cloud infrastructure best practices and regulations.

### Compute/workload

- Leverage immutable workloads whenever possible.
- Disable remote access.
- Integrate security testing into image creation.
- Alarm with file integrity monitoring.
- Patch by updating images, not patching running instances.
- Choose security agents that are cloud-aware and minimize performance impact, if needed.
- Maintain security controls for long-running workloads, but use tools that are cloud aware.
- Store logs external to workloads.
- Understand and comply with cloud provider limitations on vulnerability assessments and penetration testing.

If you want to learn about cloud security we recommend that you start by reading the [CSA Security Guidance for Cloud Computing](#).

If you are looking for more [formalized training](#) around cloud security, CSA also offers the [Certificate of Cloud Security Knowledge \(CCSK\)](#) that explains the information provided in the Security Guidance in more depth.

[VirtualizationApplication Containers and MicroservicesSecurity Guidance](#)

Share this content on your favorite social network today!



Related Articles:



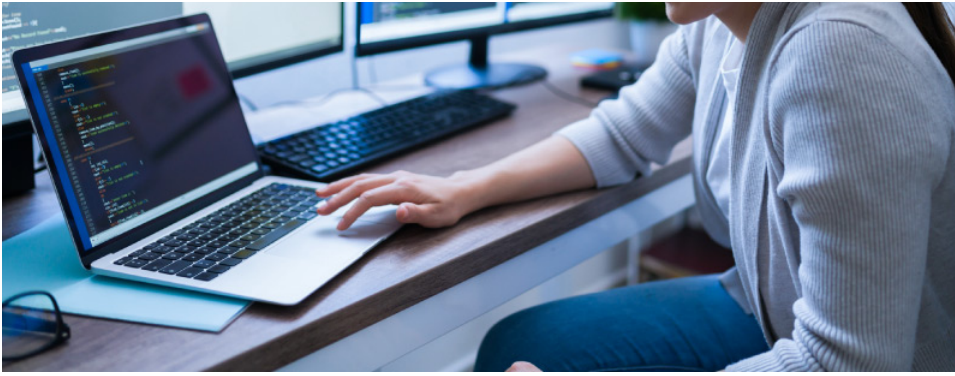
[CCSK Success Stories: From a Cloud Technical Specialist](#)

Published: 09/13/2021



[Kubernetes 1.22 – What's new?](#)

Published:  
09/06/2021



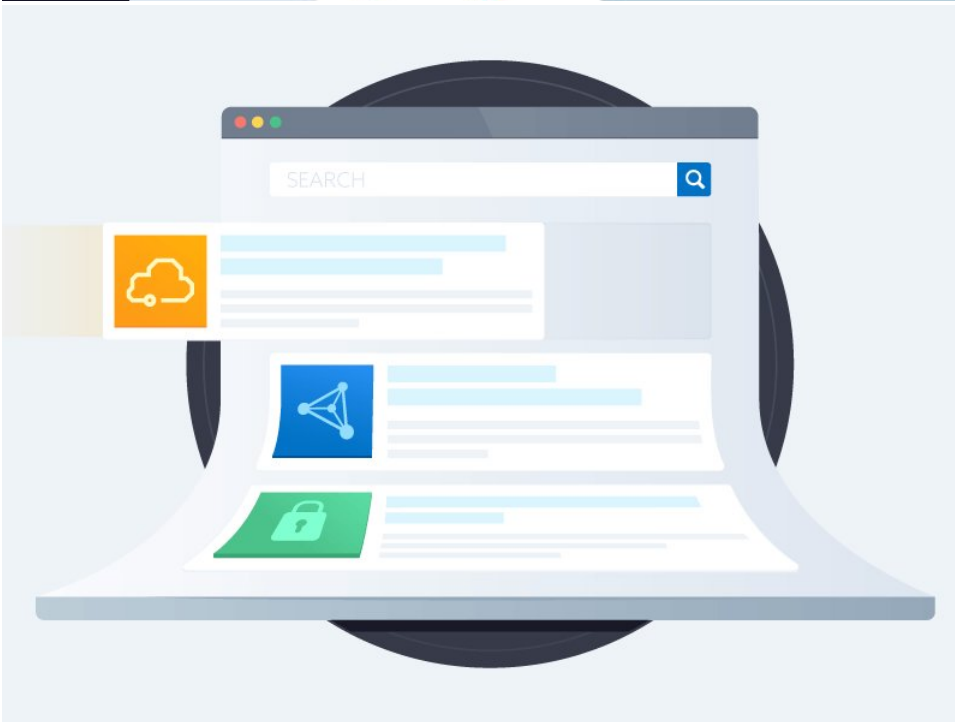
[The  
Microservices  
Architecture  
Pattern:  
Expanding  
Security  
Assurance  
Ideas in  
Containers  
and  
Microservices](#)

**Published:**  
09/02/2021



[Cloud  
Security  
Alliance  
Releases  
Guidance on  
Microservices  
Architectural  
Pattern for a  
Resilient,  
Approach to  
Architecting,  
Deploying  
Secure  
Systems](#)

**Published:**  
08/31/2021



cloud  
CSA security  
alliance®



© 2009–2021 Cloud Security Alliance.  
All rights reserved.

[Corporate Membership](#)

[Cloud Customers](#)[Cloud Solution Providers](#)[SaaS Solution Providers](#)

[Join as an Individual](#)

[Circle Community Forum](#)[Chapters](#)[Working Groups](#)

[Research](#)

[Download Publications](#)[View Working Groups](#)

Find a...

[Cloud Consultant](#)[Cloud Service Provider](#)

[Certificates](#)

[CCSK](#)[CCAK](#)

[Events](#)

[Americas](#)[EMEA](#)[APAC](#)

[Education](#)

[Blog](#)[Virtual Events & Webinars](#)[Training](#)

Popular Resources

[Security Guidance](#)[CCM](#)[CAIQ](#)[STARG](#)[DPR](#)

[About CSA](#)

[Contact Us](#)[Press Releases](#)[Affiliates](#)

[Our Team](#)

[Board of Directors](#)[Management & Staff](#)

[Legal](#)

[Privacy Notice](#)[Terms & Conditions](#)

▲