***Fundamentals of Cloud Security***

This training introduces the viewer to the fundamentals of cloud security, including concepts they must understand to recognize threats and potentially defend data centres, public/private clouds, enterprise networks, and small office/home office (SOHO) networks from cloud-based attacks.

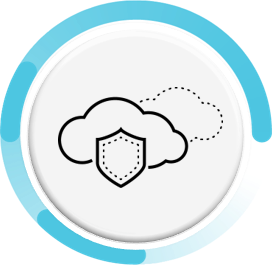
After you complete this training, you should be able to:

* Describe cloud computing models, virtualization, hypervisors, public cloud service provider options, and private deployment options
* Explain the development operations (DevOps) strategy that unites teams to discover and remediate issues, automate deployment, and reduce time to market
* Describe the evolution of data centres through mixed traditional and cloud computing technologies
* Detail how Secure Access Service Edge (SASE) solutions help organizations embrace the concepts of cloud and mobility
* Describe how SaaS solutions provide data classification, sharing and permission visibility, and threat detection within the application
* Describe how the Prisma Cloud security platform detects and prevents security risks

**Lesson Topics**

This training comprises 7 lessons and takes about 2 hours and 30 minutes to complete.

* Lesson 1: Cloud Computing
* Lesson 2: Cloud Native Technologies
* Lesson 3: Cloud Native Security
* Lesson 4: Hybrid Data Centre Security
* Lesson 5: Prisma Access SASE Security
* Lesson 6: Prisma SaaS
* Lesson 7: Prisma Cloud Security



***Lesson 1: Cloud Computing***

The move toward cloud computing not only brings cost and operational benefits but also technology benefits. Data and applications are easily accessed by users no matter where they reside, projects can scale easily, and consumption can be tracked effectively.

**Definition**

Cloud computing is not a location but rather a pool of resources that can be rapidly provisioned in an automated, on-demand manner. Read the quote below for the definition of cloud computing according to the U.S. National Institute of Standards and Technology.

**Cloud Computing Ecosystem**

The cloud computing ecosystem consists of service models, deployment models, responsibilities, and security challenges.

**Service Models, Deployment Models, and Responsibilities**

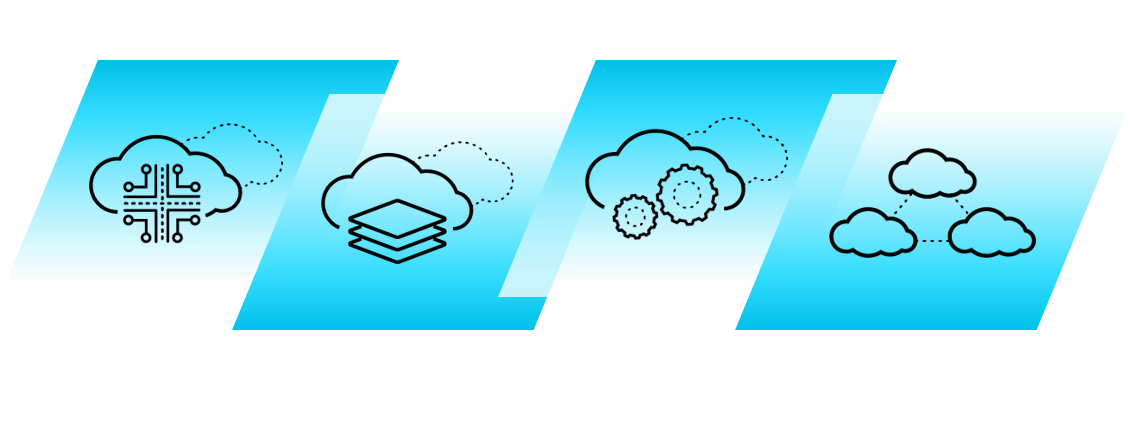
Virtualization is a critical component of a cloud computing architecture that, when combined with software orchestration and management tools that are covered in this course, allows you to integrate disparate processes so that they can be automated, easily replicated, and offered on an as-needed basis.

**Shared Responsibility Model**

The security risks that threaten your network today do not change when you move from on-premises to the cloud. The shared responsibility model defines who (customer and/or provider) is responsible for what (related to security) in the public cloud.

**Cloud Security Responsibilities**

In general terms, the cloud provider is responsible for security of the cloud, including the physical security of the cloud data centres, and foundational networking, storage, compute, and virtualization services.



***Lesson 2: Cloud Native Technologies***

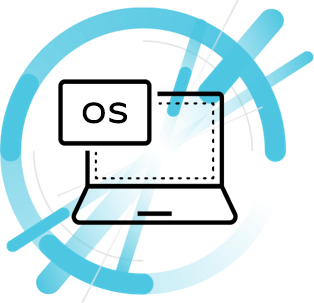
Like a new universe, the cloud native ecosystem has many technologies and projects quickly spinning off and expanding from the initial core of containers.

**Cloud Native Technology Properties**

A useful way to think of cloud native technologies is as a continuum spanning from virtual machines (VMs) to containers to serverless. On one end are traditional VMs operated as stateful entities, as we’ve done for over a decade now. On the other are completely stateless, serverless apps that are effectively just bundles of app code without any packaged accompanying operating system (OS) dependencies.

**Virtualization**

Virtualization is the foundation of cloud computing. You can use virtualization to create multiple virtual machines to run on one physical host computer.



**Overview**

You can think of virtual machines as separate computers running various operating systems on a physical host computer. Virtual machines and their associated operating systems often are referred to as “virtual guest operating systems.” These virtual guest operating systems all share the physical compute resources: processors, dynamic memory (RAM), and permanent storage media of a physical host machine.

**Hypervisor**

Hypervisor software allows multiple, virtual guest operating systems to run concurrently on a single physical host computer. The hypervisor functions between the computer operating system and the hardware kernel.

***Lesson 3: Cloud Native Security***

The speed and flexibility that are so desirable in today’s business world have led companies to adopt cloud technologies that require not just more security but new security approaches. In the cloud, you can have hundreds or even thousands of instances of an application, presenting exponentially greater opportunities for attack and data theft.

**The Four Cs of Cloud Native Security**

The CNCF defines a container security model for Kubernetes in the context of cloud native security. Each layer provides a security foundation for the next layer.

**Cloud**

The cloud (and data centres) provide the trusted computing base for a Kubernetes cluster. If the cluster is built on a foundation that is inherently vulnerable or configured with poor security controls, then the other layers cannot be properly secured.

**Clusters**

Securing Kubernetes clusters requires securing both the configurable cluster components and the applications that run in the cluster.

**Containers**

Securing the container layer includes container vulnerability scanning and OS dependency scanning, container image signing and enforcement, and implementing least privilege access.

**Code**

The application code itself must be secured. Security best practices for securing code include requiring TLS for access, limiting communication port ranges, scanning third-party libraries for known security vulnerabilities, and performing static and dynamic code analysis.