Securing Cloud Native Applications Using the *OWASP Cloud-Native Application Security Top 10* Guide

Modern cloud native applications provide critical functionality to various business processes. The number of web applications is increasing, and APIs exposed to the internet are growing exponentially. Today's enterprises continue to move to the cloud and take advantage of emerging cloud native architectures. The Palo Alto Networks 2022 State of Cloud Native Security Report found that organizations expect to host 68% of their workloads in the cloud within two years. On top of that, by 2023, over 500 million apps will be developed using cloud native approaches.[1]

1. Frank Gens, et al., *IDC FutureScape: Worldwide IT Industry 2020 Predictions*, IDC, October 2019, https://www.idc.com/research/viewtoc.jsp?containerId=US45599219.

Table of Contents

Cloud native applications offer a fundamentally new and exciting approach to designing and building software. However, they also raise a completely new set of security challenges. For example, when you move to a microservice model, end-to-end visibility, monitoring, and detection become more complex and difficult to execute.

Cloud native application security is a modern approach to securing modern applications throughout the application lifecycle at scale. This guide provides information about what the most prominent security risks are for cloud native applications, the challenges involved, and how to overcome them. In addition, it will detail how the Palo Alto Networks Web Application and API Security solution delivered as a part of the Prisma Cloud platform can help your organization implement protection against the *OWASP Cloud-Native Application Security Top 10* guide.

About OWASP

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve software security. The *OWASP Cloud-Native Application Security Top 10* guide details the top 10 most critical cloud native application security risks and guidance for organizations to protect against those risks. The purpose of the guide is to offer developers, cloud architects and web application security professionals insight into the most common security risks so that they may incorporate the report's findings and recommendations into their security best practices, with the goal of minimizing risks to their applications.

About Prisma Cloud

Prisma® Cloud is a Cloud Native Application Protection Platform (CNAPP) that combines functionality for Cloud Security Posture Management (CSPM), Cloud Workload Protection Platforms (CWPP), Cloud Infrastructure Entitlement Management (CIEM), Cloud Network Security (CNS), and Cloud Code Security (CCS) into a unified solution to secure cloud native applications across the full application lifecycle. The platform is API-enabled and capable of protecting your cloud native applications across all clouds (public, private, and hybrid).

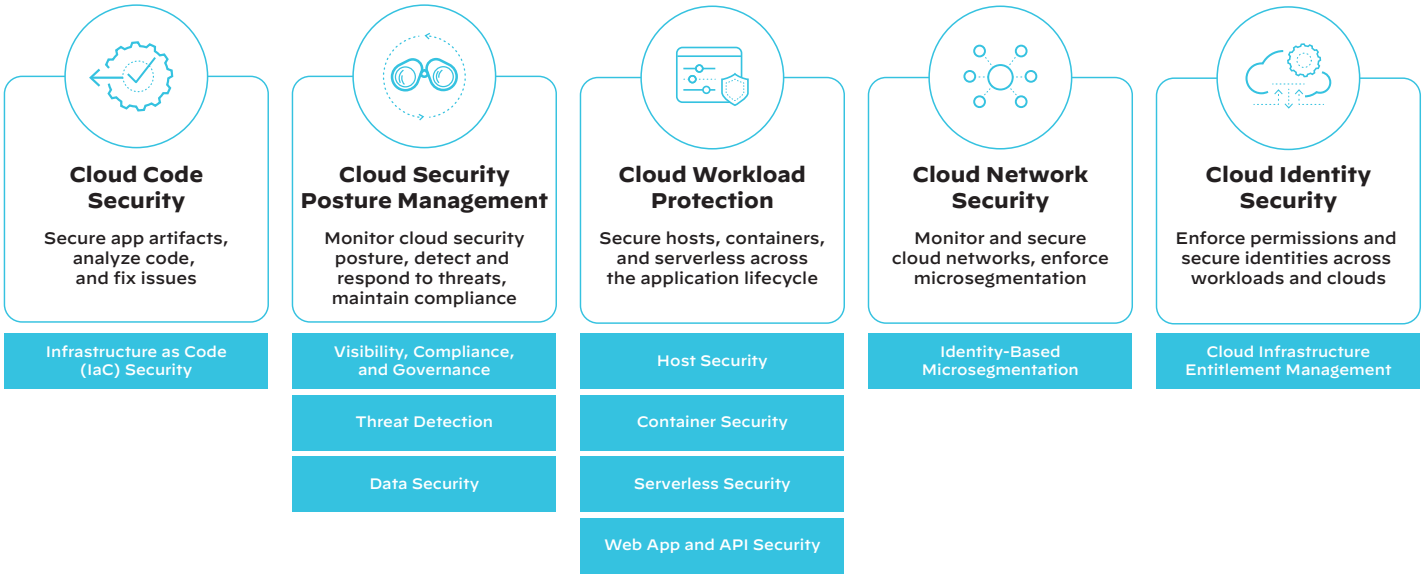

Figure 1: Prisma Cloud integrated capabilities for complete cloud native application protection

The Web Application and API Security (WAAS) module is integrated into the cloud native security platform to provide comprehensive detection and protection of web applications and APIs for any cloud native architecture. The WAAS module provides protection from a single agent that also provides Cloud Workload Protection (CWP) capabilities. DevOps and security teams can confidently leverage best-in-class protection across web applications and APIs seamlessly integrated into the CI/CD pipeline.

OWASP Cloud-Native Application Security Top 10 Risks

CNAS-1: Insecure Cloud, Container or Orchestration Configuration

The number one risk on the list is insecure cloud environments, containers, or the configuration of the environment where the application is deployed. Since cloud native applications are deployed on top of multiple layers of infrastructure (cloud, cluster, orchestration, containers), it is crucial to enforce security best practices on all configurations related to these layers.

Examples: Unencrypted and publicly exposed storage buckets, leaving SSH/RDP ports open to the world, containers granted privileged capabilities, turning off encryption for Kubernetes® component communication, and more.

Secure Clouds, Containers & Configurations with Prisma Cloud

- **Cloud Security Posture Management**
  - » Customers leverage the industry-leading Cloud Security Posture Management (CSPM) capabilities within Prisma Cloud to automatically generate and assess the inventory of all public cloud assets and the risks created by insecure configuration.
  - » Auto remediation capabilities can minimize the number of misconfigurations that expose an organization.
- **Cloud Identity Security**
  - » Prisma Cloud delivers Cloud Infrastructure Entitlement Management (CIEM) to detect overly permissive access to cloud resources, including storage buckets, and suggest corrections to reach least-privileged entitlements.
- **Cloud Workload Protection**
  - » Prisma Cloud Compute checks for Kubernetes and container security best practices and compliance violations. Customers can prevent host and image misconfigurations from getting deployed by leveraging CI/CD build tests and the Open Policy Agent (OPA) integration.
  - » As a secondary line of defense, Prisma Cloud has container runtime protection, learns the container's behavior and prevents known malicious behavior and anomalies.
- **Cloud Code Security**
  - » Securing cloud infrastructure can shift left to start with developers. Infrastructure as Code (IaC), including Terraform, CloudFormation, ARM, Kubernetes manifests, and Dockerfiles can be scanned by Prisma Cloud Code Security to ensure all configurations are secure and compliant before they are deployed.

CNAS-2: Injection Flaws (App Layer, Cloud Events & Cloud Services)

Injection flaws are security vulnerabilities that allow a user to gain access to the operating system or backend database when the web app takes user input without properly validating it first. Bad actors and hackers attempt to add additional information within user-supplied input so they can create, read, update, or delete data. They may be able to append entire scripts into applications to execute larger commands. A common example is SQL injection, where the attacker adds additional values to the query to access sensitive data or when attackers inject OS commands into user input, which is later on used within a shell environment.

Examples: SQL injection, XML external entity injection, OS command injection, serverless event data injection, and more.

Stop Injections with Prisma Cloud

- **Cloud Workload Protection**
  - » Prisma Cloud Compute's runtime protection capability can be leveraged to detect and prevent unauthorized behavior and actions such as unauthorized code execution.
  - » Prisma Cloud Compute can be leveraged to scan VM and container images and prevent their deployment in case a known injection-based vulnerability (e.g., CVE) exists.
  - » Prisma Cloud Web App & API Security module prevents injection flaw attacks in web traffic and API calls with high accuracy and confidence.
  - » Prisma Cloud's Web App & API Security module prevents automated injection attacks generated by bots and scanning tools, using its Bot Protection capability.

CNAS-3: Improper Authentication & Authorization

Identity and access management (IAM) in cloud environments is a major concern for businesses as they move to the cloud. Today, the capabilities offered by cloud service providers (CSPs) are not enough for an advanced organization using multiple services or clouds. This often leads to over-providing access to certain cloud native applications where users should not have access. For example, developers create insecure APIs without proper authentication by mistake.

Examples: Unauthenticated API access on a microservice, over-permissive cloud IAM role, lack of orchestrator node trust rules (e.g., unauthorized hosts joining the cluster), unauthenticated orchestrator console access, and more.

Prevent Improper Authentication & Authorization with Prisma Cloud

- **Cloud Workload Protection**
  - » The Prisma Cloud Web App & API Security module can be leveraged to prevent unauthorized access to APIs and web applications using its "Access Control" capability. In addition, customers can leverage the API protection capability to enforce strict security over APIs.
  - » The Prisma Cloud Web App & API Security module can be used to only allow access to known API endpoints using approved HTTP methods and legitimate data payloads by enforcing the OpenAPI specification file for each API.
  - » Prisma Cloud Compute locks down user and control plane access to Docker and Kubernetes to decrease the attack surface area.
- **Cloud Identity Security**
  - » Prisma Cloud delivers Cloud Infrastructure Entitlement Management to analyze effective IAM permissions and enforce least-privileged access to cloud resources. Prisma Cloud automatically calculates effective permissions across cloud service providers, detects overly permissive access and suggests corrections to reach least privilege entitlements.
- **Cloud Code Security**
  - » Prisma Cloud Code Security can catch and prevent low-hanging fruit, like over-permissive IAM and RBAC policy updates in IaC.

CNAS-4: CI/CD Pipeline & Software Supply Chain Flaws

Businesses leverage the CI/CD pipelines to rapidly deploy capabilities for their services and applications. This allows the vendor to quickly innovate and build, but it also allows the vendor to quickly fix or patch components of the application should vulnerabilities or misconfigurations be identified. Some attackers deliberately target SaaS vendors with the specific mission of compromising that vendor's CI/CD pipeline to insert malicious code into a portion of the application's containerized ecosystem.

Examples: Insufficient authentication on CI/CD pipeline systems, use of untrusted images, use of stale images, insecure communication channels to registries, overly permissive registry access, and more.

Mitigation of CI/CD Pipeline flaws with Prisma Cloud

The following Prisma Cloud capabilities can be leveraged to create and maintain a secure CI/CD pipeline:

- **Cloud Code Security**
  - » Prisma Cloud Infrastructure as Code (IaC) Security can be leveraged as part of the CI/CD pipeline to identify and fix misconfigurations in Terraform, CloudFormation, ARM, Kubernetes, and other IaC templates and vulnerabilities in open source dependencies.
  - » Version Control System (VCS) and CI/CD configurations can be scanned to prevent common misconfigurations like leaving MFA turned off or not adding branch protection rules.
- **Cloud Workload Protection**
  - » Prisma Cloud Compute scans container images and enforces policies as part of continuous integration and continuous delivery workflows, continuously monitors code in repositories and registries, and secures both managed and unmanaged runtime environments—combining risk prioritization with runtime protection at scale.
  - » Prisma Cloud Compute can create trusted images and registries to prevent code tampering and image injection attacks.

CNAS-5: Insecure Secrets Storage

Insecure secrets storage can occur when development teams assume that hackers will not have access to the sensitive information that has been stored on filesystems, such as API keys or passwords. When sensitive data is not protected properly, it can result in data loss where hackers can reuse this information to further exploit additional cloud native applications.

Examples: Orchestrator secrets stored unencrypted, API keys or passwords stored unencrypted inside containers, hardcoded application secrets, poorly encrypted secrets (e.g., use of obsolete encryption methods, use of encoding instead of encryption, etc.), and mounting of storage containing sensitive information.

Prevent Insecure Secrets Storage with Prisma Cloud

- **Cloud Workload Protection**
  - » Prisma Cloud Compute can detect sensitive information that is improperly secured inside images and containers. Scans can detect embedded passwords, login tokens, and other types of secrets.
- **Cloud Code Security**
  - » Prisma Cloud Infrastructure as Code (IaC) Security can be leveraged as part of the CI/CD pipeline to identify and fix misconfigurations in Terraform, CloudFormation, ARM, Kubernetes, and other IaC templates. IaC security scans include the ability to detect secrets stored in IaC templates.

CNAS-6: Overly Permissive or Insecure Network Policies

It is easy to configure broad rules to allow microservices to communicate with each other. Overly permissive rules that grant too much access to a cloud native application are often created by mistake but are not addressed because the application is working. In addition, insecure network policies such as no defined segmentation for containers can weaken the security posture of cloud native applications.

Examples: Overly permissive pod-to-pod communication allowed, internal microservices exposed to the public internet, no network segmentation defined, end-to-end communications not encrypted, network traffic to unknown or potentially malicious domains not monitored and blocked.

Prevent Overly Permissive or Insecure Network Policies with Prisma Cloud

- **Cloud Security Posture Management**
  - » Prisma Cloud Threat Detection employs advanced unsupervised machine learning to learn the normal network behavior of each customer's cloud environment to detect network anomalies and zero-day attacks effectively with minimal false positives.
  - » Prisma Cloud Visibility, Governance, and Compliance delivers True Internet Exposure, which analyzes end-to-end public cloud network configurations to accurately identify, alert on and remediate overly exposed cloud instances.
- **Cloud Network Security**
  - » Prisma Cloud Identity-Based Microsegmentation visualizes application dependencies, enforces microsegmentation on hosts and containers, and stops lateral movement of threats. This can be used to block unsanctioned pod-to-pod communication, unauthorized ingress/egress traffic, and more.

CNAS-7: Using Components with Known Vulnerabilities

Cloud native applications often use third-party open source packages or additional components as building blocks for their applications. Components typically run with the same privileges as the application itself, so flaws in any component can result in serious impact. Such flaws can be accidental (e.g., coding error) or intentional (e.g., backdoor in component). While some known vulnerabilities lead to only minor impacts, some of the largest breaches to date have relied on exploiting known vulnerabilities from components.

Examples: Vulnerable third-party open source packages, vulnerable versions of application components, and use of known vulnerable container images.

Detect & Fix Known Vulnerabilities in Components with Prisma Cloud

- **Cloud Workload Protection**
  - » Prisma Cloud Compute scans container and VM images as well as serverless functions and enforces policies as part of continuous integration and continuous delivery workflows, continuously monitors code in repositories and registries, and secures both managed and unmanaged runtime environments—combining risk prioritization with runtime protection at scale.
- **Cloud Code Security**
  - » Prisma Cloud Code Security identifies vulnerable open source packages in repositories and suggests remediations.

CNAS-8: Improper Assets Management

Improper asset management is not centered around coding flaws when building cloud native applications. Instead, it relates to undocumented APIs or forgotten cloud resources. APIs tend to expose more endpoints than traditional web applications, making proper and updated documentation highly important. When a new cloud native application is spun up to meet certain needs, the forgotten APIs associated with it are still in use. These older or unmanaged services pose a risk in production environments because researchers might have discovered vulnerabilities in the older versions that attackers can leverage.

Examples: Undocumented microservices, APIs, and obsolete and unmanaged cloud resources.

Cloud Asset Management with Prisma Cloud

- **Cloud Security Posture Management**
  - » Prisma Cloud provides security teams with full visibility into all of their cloud assets and simplifies compliance reporting.
  - » Prisma Cloud maintains a history of configuration changes, enabling users to understand exactly when a new security issue was introduced and by whom, to simplify cloud forensics and auditing.
- **Cloud Workload Protection**
  - » Prisma Cloud's Web App & API Security module can be leveraged to prevent unauthorized access to APIs and web applications using its Access Control capability. In addition, customers can leverage the API protection capability to enforce strict security over APIs.
  - » Prisma Cloud's Web App & API Security module can be used to only allow access to known API endpoints using approved HTTP methods and legitimate data payloads by enforcing the OpenAPI specification file for each API.

CNAS-9: Inadequate 'Compute' Resource Quota Limits

Cloud compute resource quotas can limit how many resources a particular cloud compute workload can use. Resource quotas limit the CPUs, GPUs, persistent disk, and IP addresses a workload can use. Exceeding these quotas can make your applications fail or run slowly. Excessive resource usage can be a sign of malicious activity or unauthorized usage, such as crypto mining processes.

Examples: Resource-unbound containers and overly permissive request quota set on APIs.

Preventing Excessive Resource Usage by Cloud Workloads with Prisma Cloud

- **Cloud Workload Protection**
  - » Prisma Cloud Compute's runtime defense is a set of features that provide both predictive and threat-based active protection for running containers. Runtime defense includes capabilities like detecting when malware is added to a container or when a container connects to a botnet and preventing it in real time.
  - » Prisma Cloud Compute has distinct sensors for file system, network, and process activity. Each sensor is implemented individually, with its own set of rules and alerting.
  - » Prisma Cloud Compute includes a wide range of compliance checks that can prevent or alert in case workloads such as containers are configured in a way that may increase risk of excessive resource usage. These checks include:
    - Applying memory limits to containers
    - Setting container CPU priority appropriately
    - Containers that share the host's process namespace
    - Checking container health at runtime
- **Cloud Code Security**
  - » Prisma Cloud Code Security identifies and blocks Kubernetes manifests without resource request levels or limits. It notifies developers in their DevOps tools about the issue as they code or attempt to commit changes that violate policies.

CNAS-10: Ineffective Logging & Monitoring

Insufficient logging and monitoring of cloud native applications combined with ineffective integrations with incident response tools lead to gaps in your security operations. Attackers exploit these gaps by continuously attacking the system, and once they infiltrate the system, they tend to move laterally to extract or destroy data. Leaving infrastructure unmonitored leads to delays in detection of breaches for your cloud native applications.

Examples: No container or host process activity monitoring, no network communications monitoring among microservices, no resource consumption monitoring to ensure availability of critical resources, and lack of monitoring on orchestration configuration propagation and stale configs.

Logging, Monitoring & Visibility with Prisma Cloud

- **Cloud Workload Protection**
  - » Prisma Cloud Compute's Incident Explorer elevates raw audit data to actionable security intelligence, enabling a more rapid and effective response to incidents. Rather than having to manually sift through reams of audit data, Incident Explorer automatically correlates individual events generated by the firewall and runtime sensors to identify unfolding attacks.
  - » Prisma Cloud lets customers surface critical policy breaches by sending alerts to any number of channels. Alerts ensure that significant events are put in front of the right audience at the right time. These channels include AWS Security Hub, Cortex® XSOAR, email alerts, Google Cloud Pub/Sub, Google Cloud Security Command Center, JIRA, etc.
- **Cloud Security Posture Management**
  - » Prisma Cloud helps customers visualize their entire cloud infrastructure and provides insights into security and compliance risks. Prisma Cloud helps to connect the dots between configuration, user activity, and network traffic data so that customers have the context necessary to define appropriate policies and create alert rules. To conduct such investigations, Prisma Cloud provides customers with a proprietary query language called RQL that is similar to SQL.
- **Cloud Network Security**
  - » Prisma Cloud Identity-Based Microsegmentation delivers continuous network communications logging and monitoring among microservices.

Summary

As cloud native application development is quickly becoming the de facto method for building and delivering modern applications, organizations are encouraged to evolve their application security programs and adopt modern cloud native application security solutions that provide end-to-end security and defense in depth.

Prisma Cloud is at the bleeding edge of cloud native security and provides customers with the most elaborate security capabilities necessary for protecting their entire cloud native application stack.

To experience all the great functionality and more of Prisma Cloud, request a hands-on demo.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com