What Is a Cloud Workload Protection Platform (CWPP)?

Cloud Workload Protection Platform (CWPP) as defined by Gartner is a “workload-centric security solution that targets the unique protection requirements” of workloads in modern enterprise environments.

Workloads in modern environments have evolved to include physical servers, virtual machines (VMs), containers, and serverless workloads.

The cloud workload protection platform (CWPP) market is increasingly overlapping with the cloud security posture management (CSPM) market and shifting left into development to address the full life cycle of cloud-native application protection requirements.

Gartner recommendations:

Implement a CWPP offering that protects workloads regardless of location, size, runtime duration or application architecture.

1. Support for Windows, Linux, and Linux containers (with explicit support for Kubernetes), and support for serverless function scanning and runtime protection
2. Licensing portability across on-premises and public cloud deployments.
3. Traditional per-workload/per-year licensing, with licensing options for usage-based consumption based on image size (for example, per minute).
4. Console as a service provided from the cloud for ease of deployment.
5. Software available and integrated in the cloud provider’s application store for ease of consumption
6. Integrated CSPM/KSPM capabilities
7. Anti-malware scanning capabilities, including the option to scan cloud object stores.
8. Coverage of the hierarchy of controls that are important to the enterprise
9. These controls include restricted operator access, change, and log management. Operations and security hygiene is also present—such as vulnerability management, network visibility, system integrity, application control, exploit prevention, server/workload EDR, host-based IPS, and vulnerability shielding.

Why CWPP is important

The transformation from legacy to cloud-native applications isn't automatic. Organisations can't "copy and paste" to the cloud an application that is currently on-premise. Here are four reasons why Cloud Workload Protection Platform (CWPP) is important:

1. Most companies have legacy applications and infrastructure that prevent a complete movement of functionality to the cloud.

2. Most organisations are deliberately using multiple cloud vendors, depending on their specific needs. As a result, most enterprises—by circumstance or design—are working in a hybrid, multi-cloud environment. This makes it difficult for security professionals to know, see, and manage where applications and data are in a fragmented environment.

3. Today, application developers grab code from a variety of places like GitHub, leverage workloads to create an application and publish it directly to their target audience of consumers. This approach is called Development Operations (DevOps) and is a cycle of "continuous innovation and continuous development" (CI/CD) where they can quickly respond to customers and improve that response and experience for their customers and partners in weeks or days.

4. The tradeoff of process for speed and the constant improvement of applications means that security is no longer a strict gate for application production. Security professionals can't apply controls at application run time as they used to be able to do.
5. The risk to data and applications due to the changing nature of workloads, lack of visibility and control, and the rise of the "always on" DevOps environment makes CWPP an important security solution in the modern enterprise.

What are the key benefits of CWPP?

1. Combining vulnerability data with real-time traffic visibility
2. Understanding how applications work and where you are most vulnerable
3. Use visibility to create and enforce micro-segmentation policies.
4. End-to-End managed security for container environments covering security policies
5. Vulnerability scanning capabilities throughout the container lifecycle

6. Container workloads monitoring and protection and compliance reporting
7. Protection for server devices across platforms and operating systems
8. 2 tiers levels address compliance projects e.g require host firewall
9. Cost: Lower upfront costs, reduced cost of hardware, lower maintenance & operational overhead
10. Flexibility: Scale up and scale down application capacity, according to demand
11. Improved Customer Service: Respond better and faster to customer requests, driving more business
12. Ease of Use: Stand up, use from anywhere and collect analytics from applications
13. Security: Shared responsibility and evolution of cloud security