Market Guide for Cloud Workload Protection Platforms

Published 12 July 2021 - ID G00725997 - 22 min read

By Analyst(s): Neil MacDonald, Tom Croll

Initiatives: Infrastructure Security

Workload protection must span virtual machines, containers and serverless workloads in public and private clouds. Security and risk management leaders should use this Market Guide to understand the need for protection that spans development and runtime and includes cloud security posture management.

Overview

Key Findings

- Most enterprises are purposefully using more than one public cloud infrastructure as a service (IaaS) platform, but still have on-premises workloads to protect.
- With cloud-native applications, workload security must start proactively during development.
- 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.
- Emerging approaches, such as the use of agentless CWPPs, appeal to buyers because of their ease of deployment.
- Enterprises using endpoint protection platform (EPP) offerings designed to protect end-user devices for server workload protection are putting their data and applications at risk.

Recommendations

Security and risk management leaders responsible for infrastructure security should:

- Implement a CWPP offering that protects workloads regardless of location, size, runtime duration or application architecture.
- Secure workloads earlier by extending workload scanning and compliance efforts into development (DevSecOps), especially for container-based and serverless function platform as a service (PaaS)-based development and deployment.
- Consolidate CWPP and CSPM strategies over the next 12 to 24 months to reduce costs and complexity and identify risks better.
- Design for CWPP scenarios where runtime agents cannot be used or no longer make sense. Require CWPP and CSPM vendors to support agentless deployment options.

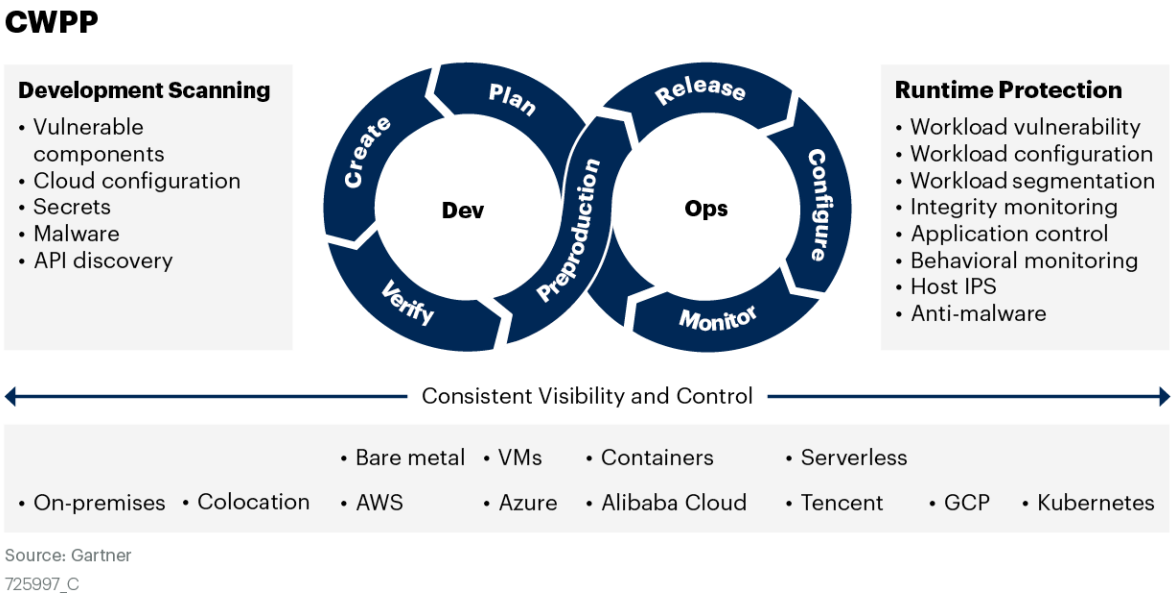
Market Definition

CWPPs are workload-centric security products that protect server workloads in hybrid, multicloud data center environments (see Note 1). CWPPs provide consistent visibility and control for physical machines, virtual machines (VMs), containers and serverless workloads, regardless of location. CWPP offerings protect workloads using a combination of system integrity protection, application control, behavioral monitoring, intrusion prevention and optional anti-malware protection at runtime. CWPP offerings should also include scanning for workload risk proactively in the development pipeline.

Market Description

CWPPs protect server workloads from attack, regardless of the location or granularity of the workload. They provide security and risk management leaders with consistent visibility into, and control of, all server workloads. CWPP offerings should start by scanning for known vulnerabilities and risks in development. At runtime, they should protect workloads from attack, typically using a combination of system integrity protection, application control, behavioral monitoring, host-based intrusion prevention and optional anti-malware protection (see Figure 1).

Figure 1: Cloud Workload Protection Platform Capabilities



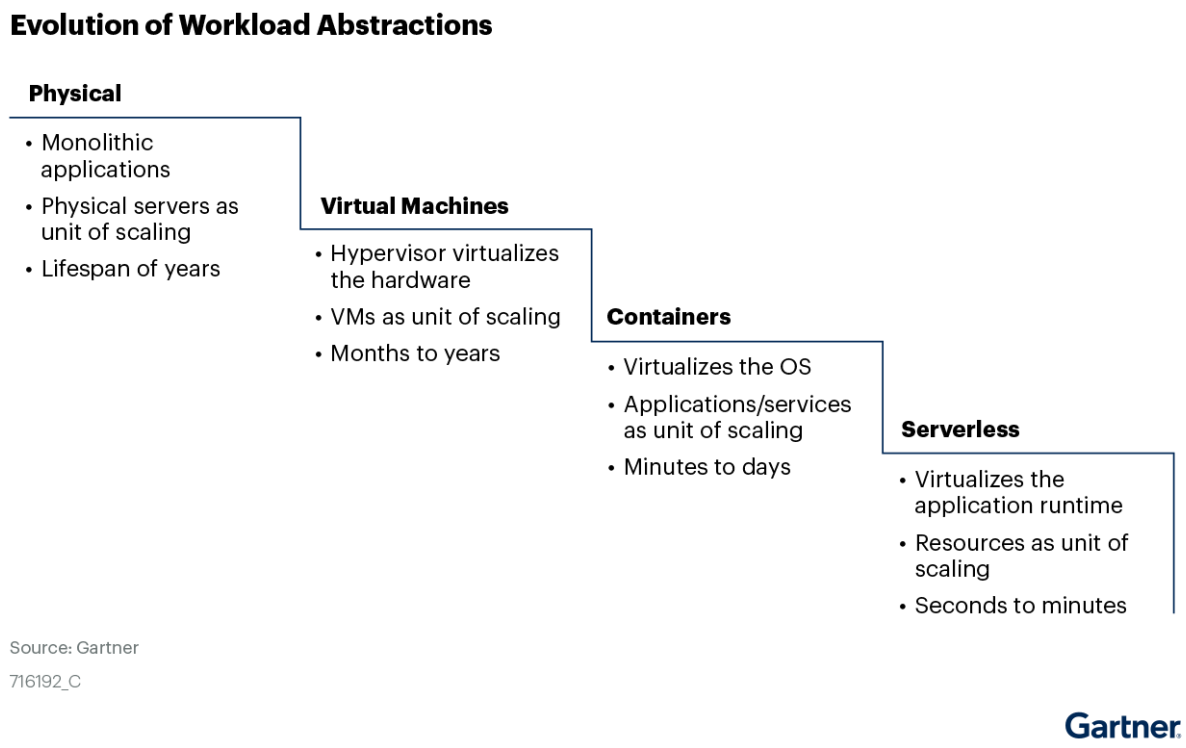
Source: Gartner
725997_C

Gartner

CWPP requirements continue to evolve and further separate from EPP. Modern digital business applications and services are composed of multiple workloads (units of back-end compute work) running on-premises and also in IaaS. In a recent Gartner survey, 76% of enterprises indicated they are using multiple IaaS providers. [1] Furthermore, in the same survey, the top challenge identified by respondents when using multiple public IaaS providers was increased security risk. [2] The reality is that most enterprises will have workloads distributed across a combination of on-premises, colocation and multiple public cloud IaaS platforms. We refer to this combination as a hybrid, multicloud architecture. CWPPs must protect this architecture.

At the same time, the granularity of workloads, their life span and the ways they are created are changing. Linux containers are widely adopted and there is increasing adoption of serverless function PaaS (also referred to as function PaaS [fPaaS]). [3] A CWPP strategy should be adopted to provide consistent visibility and control of workloads, regardless of their granularity and level of abstraction (see Figure 2).

Figure 2: Evolution of Workload Abstractions



Reading Figure 2 from left to right, we see how workloads have become more granular over time — with shorter life spans at runtime — as development organizations have adopted DevOps-style development patterns. DevOps is designed for multiple small iterations, often several times per week and, in some cases, several times per day. The best way to secure these rapidly changing and short-lived workloads is to start their protection proactively in the development phase (see 12 Things to Get Right for Successful DevSecOps), so that when a workload is instantiated in production, it is created compliant. Further, cloud-native applications are often composed of a combination of VMs, containers and serverless PaaS working together to deliver the application service — all of which need protection.

Occasionally, we still find enterprises using end-user-focused EPP offerings designed for desktops, laptops and tablets on server workloads. These are ill-suited to the requirements of dynamic hybrid, multicloud workload protection. The risk profile and threat exposure of a server workload is markedly different from that of an end-user-facing system. Enterprises that use an EPP offering designed for end-user-supporting devices are putting enterprise data and applications at risk. In contrast, CWPP offerings focus on the protection needs of server workloads in a modern hybrid (on-premises and cloud-based), multicloud (that is, using multiple public cloud IaaS providers) data center. Indeed, several of the larger CWPP vendors, such as Broadcom (Symantec), Crowdstrike, McAfee, Trend Micro and VMware (Carbon Black), offer distinct and separate offerings for EPP and CWPP to address the unique requirements of each of these markets. Some smaller vendors address only the CWPP market.

Market Direction

CWPPs provide enterprises with a way to protect hybrid, multicloud workloads and provide consistent visibility into, and control of, all server workloads, regardless of the location or granularity of the workload. We have formally sized this market at an estimated U.S. $1.699 billion at YE21, with a growth rate of 18.1% in 2021 (see Forecast Analysis: Cloud Workload Protection Platforms, Worldwide). The market is increasingly fragmented as the three largest vendors — Trend Micro, Broadcom and McAfee — come under pressure from newer point solution providers and the entry of other, established providers.

There are multiple trends behind the increased adoption of CWPP offerings by enterprises:

- Workloads are being moved from on-premises to public cloud IaaS, and the overall number of IaaS workloads (including containers and serverless functions) is growing rapidly.
- In IaaS, workload-centric, host-based CWPP network controls are providing an easier and more scalable architectural option for enforcing security policy than traditional in-line network-based security controls.
- The need for pervasive Secure Sockets Layer/Transport Layer Security (SSL/TLS) decryption and inspection is being met more easily at the host workload where a session is terminated than by decrypting traffic in line using “man in the middle” approaches. This is especially true when inspecting traffic that moves laterally from service to service in microservices-based architectures.

- The shift to cloud-native application development using container-based application architectures, microservices-based applications and adoption of serverless PaaS requires new CWPP capabilities both for development and at runtime. Cloud-native applications require specific solutions designed to address the protection requirements of cloud-based systems.
- Improvements to the ease of CWPP adoption. Console as a service is a requirement for most enterprises shifting CWPP administration to the cloud and administering policies across multiple clouds. Emerging approaches for visibility without the use of agents also reduce the friction of adoption. In addition, for some enterprises, the emergence of managed CWPP offerings (such as those of Armor and ClearDATA) is further reducing the need to develop in-house skills.

Other key CWPP market trends include:

- Segmentation orchestration using the built-in capabilities of the underlying cloud platform. Many enterprises prefer using the built-in segmentation capabilities of the underlying cloud fabric (for example, Azure network security groups). This has reduced the need for CWPP vendors to provide a host-based firewall. Others program the built-in firewalls of Windows and Linux. Some host-based vendors focus entirely on identity-based segmentation where integration with the native capabilities of the underlying cloud platform's segmentation capability is a common requirement.
- Requests from enterprises for workload threat detection and response capabilities. Organizations that adopt Gartner's continuous and adaptive risk and trust assessment (CARTA) strategic framework and a zero trust security architecture acknowledge that CWPP strategies cannot rely solely on preventive controls. Thus, server workload behavioral monitoring (endpoint detection and response [EDR] for servers) is becoming a critical requirement of CWPPs. Vendors such as CrowdStrike, SentinelOne and VMware (Carbon Black) (well-known for end-user EDR) are now actively targeting the workload detection/response use case. Indeed, some CWPP vendors are focusing only on the threat detection/response (sometimes referred to as workload detection and response [WDR]) use case.

- The increasingly short life spans of workloads. With cloud-native development using containers and serverless computing, processes and threads that compromise an application come and go quickly. There is no time for traditional loading of signature files or anti-malware scanning. Behavioral monitoring solutions that rely on observation of a running workload may need dozens of instantiations before a reliable model can be created. Workloads need to be created compliant from the moment they are instantiated. This creates a critical need for development scanning and modeling/simulation in the continuous integration/continuous delivery (CI/CD) pipeline and reduces the need for invasive runtime security.

- The shift to an immutable infrastructure mindset. This is an operational model in which no configuration changes, patches or software updates are allowed on production systems. Patches and updates are applied to the base ("golden") images and layers, and then the production workloads are built afresh from these images and replaced, rather than serviced. With immutable infrastructure, CWPP protection strategies will shift to a zero trust mindset and focus on application control and container lockdown (default deny/zero trust) at runtime, with a stronger emphasis on scanning for vulnerabilities before deployment. An extension of this idea is memory immutability to ensure that only known-good and approved code resides in memory during the lifetime of a workload.

- The shift to alternative control deployment options in container environments. There is no guarantee that an enterprise will be able to place agents in the Linux host OS in a container-based deployment. This is increasingly the case with locked-down minimal kernels and with some managed container services. The answer is to provide an architectural option to run the CWPP offering as a privileged container (or as a sidecar in Kubernetes pods and service mesh architectures). Some CWPP startups focus only on the protection requirements of containers.

- The rapid adoption of Kubernetes. Kubernetes has emerged as the de facto standard for Linux container orchestration. Some startup CWPP vendors focus only on securing Kubernetes environments. Support for Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) managed Kubernetes services is a common requirement, along with support for IBM Red Hat OpenShift.

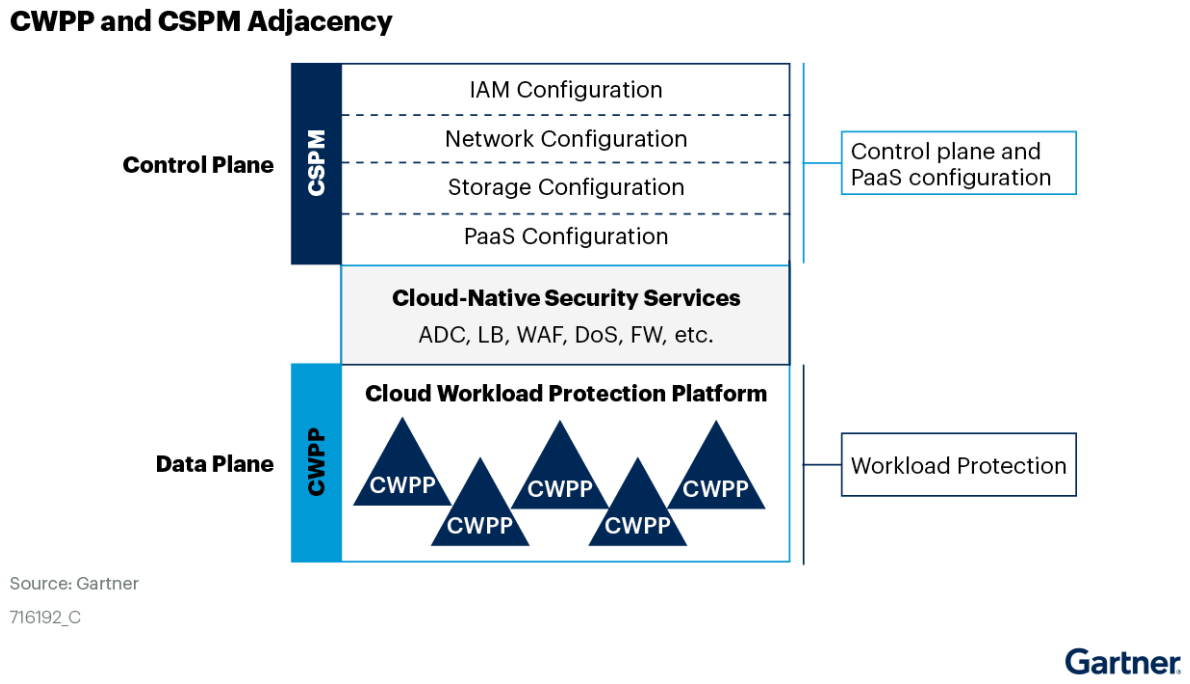
- In conjunction with Kubernetes, alternatives for service mesh constructs are emerging (see Emerging Technology Analysis: Service Mesh). These offerings provide service resiliency, automate service discovery, and abstract the complexity of setting up encrypted connectivity and key rotation away from the hands of the developer and into a policy-defined overlay. CWPP offerings need to integrate with these emerging offerings or subsume their capabilities into a broader set of capabilities.

- The shift to CWPP code layering, wrappering or insertion for protecting serverless functions. In serverless PaaS environments, agents and privileged containers/sidecars will not work. New approaches are needed, which are starting to overlap with other approaches in the application runtime protection market (see Hype Cycle for Application Security, 2020).

- Running without runtime protection instrumentation. With containers and serverless architectures, if workloads are scanned in development, foundational requirements (such as network segmentation) are met, and the infrastructure is treated as immutable, why burden containers/serverless functions with any runtime protection? Assuming prescanning, the core runtime protection needs — such as segmentation, network monitoring and behavioral monitoring — may be delivered outside the workload.

- The convergence of CWPP and CSPM, and the emergence of the cloud-native application protection platform (CNAPP). As security scanning for CWPP shifts left into development (scanning for OS, library and executable vulnerabilities, dependencies, hard-coded secrets and malware), it is also advantageous to scan the cloud configuration for excessive risk. We refer to this scanning for risky cloud configurations and compliance as cloud security posture management (see Innovation Insight for Cloud Security Posture Management). [4] CSPM should extend to environments that use Kubernetes, which itself is a cloud-native platform. We refer to this as Kubernetes security posture management (KSPM). CSPM/KSPM is a natural adjacency for CWPP providers and vice versa (see Figure 3 and Notes 2 and 3).

Figure 3: CWPP and CSPM Adjacency



There is synergy in combining CWPP and CSPM capabilities, shifting left and scanning for vulnerabilities, including in configurations. In a recent Gartner survey, respondents identified vulnerability severity score and the external accessibility of applications as the two most important metrics for measuring the risk of a vulnerability in application code or software components. [5]

Multiple vendors are converging CWPP, CSPM and workload-scanning capabilities, and shifting left into development. The combination will create a new category of CNAPP, first identified as a top emerging trend in 2020 (Top Security and Risk Management Trends), that scans workloads and configurations in development and protects workloads and configurations at runtime.

Market Analysis

Figure 4 shows the major elements of a workload protection strategy for a modern, hybrid multicloud data center architecture.

Figure 4: Risk-Based Hierarchy of Cloud Workload Protection Controls

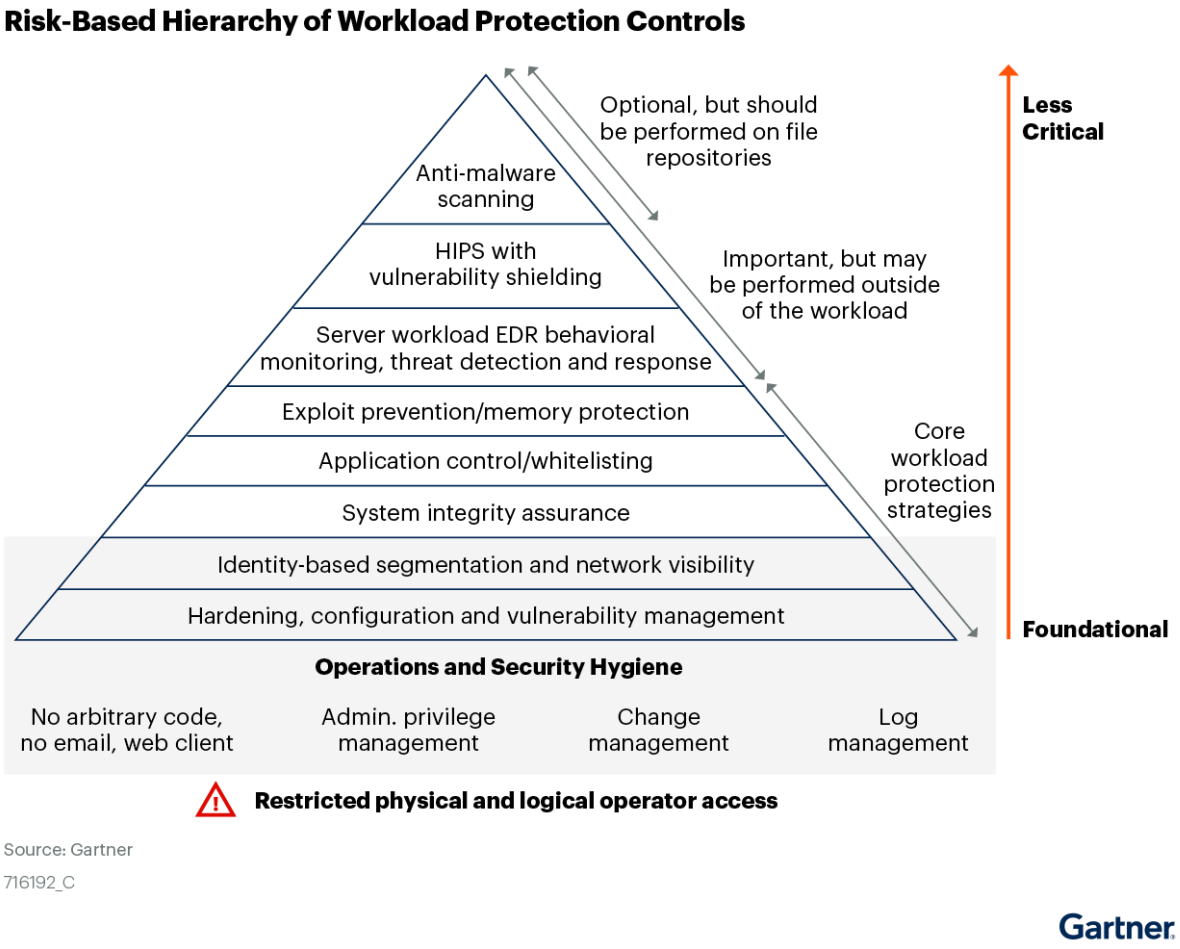


Figure 4 shows a hierarchical triangle with a rectangular foundation. The security of server workloads is rooted in the solid operations hygiene and configuration best practices shown in the shaded base. Any workload protection strategy must start there and ensure that:

- It is difficult for anyone (attacker or administrator) to access the workloads physically and logically.
- The workload image has only the code it needs. Browsers and email usage should be banned from server workload images.
- Changes to the server workloads are possible only using a managed, disciplined process with auditability, and administrative access is tightly controlled with mandatory strong authentication (typically using a privileged access management [PAM] product; see Magic Quadrant for Privileged Access Management).

- The OS and application logs are collected and monitored as part of an overall enterprise log management/security information and event management (SIEM) or extended detection and response (XDR) effort.
- The workload is hardened, minimized and patched, thus reducing the surface area for attack.
- The workload is segmented according to identity-based policies — in many cases using built-in segmentation capabilities, such as tagging of the underlying programmable cloud infrastructure on which the cloud workload is deployed. There is a separate but adjacent market for identity-based segmentation offerings (see Three Styles of Identity-Based Segmentation). One of the three styles of identity-based segmentation uses an agent-based approach. These offerings are adjacent, but beyond the scope of this Market Guide.

Above this foundation is the hierarchical layering of controls recommended for server workload protection — a combination of preventive and detection/response controls. Collectively, these provide comprehensive workload protection.

However, not every layer will be needed for every server workload. Which layers are required will depend on the usage profile of the workload, the workload's exposure and the enterprise's tolerance for risk. Notably, anti-malware scanning is one of these least important controls for server workloads. Although this scanning is essential for file-sharing repositories and object storage, it can be performed outside the workload (for example, using a cloud access security broker [CASB]; see Magic Quadrant for Cloud Access Security Brokers).

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings. A vendor is listed in the category that best aligns with its offering's core capabilities. If a vendor appears more than once, a separate offering is called out. See also Note 1.

Table 1: Examples of Cloud Workload Protection Platform Vendors and Their Offerings

(Enlarged table in Appendix)

Vendor Name [Offering name]
Aqua Security [Cloud Native Security Platform]
Alibaba Cloud [Cloud Security Center]
Armo [Armo Kubernetes Fabric]
Atomicorp [Atomic Protector]
Beijing Qianxin Technology (China only) [Unified Server Security Manager]
Bitdefender [GravityZone Platform]
Broadcom (acquired Symantec) [Data Center Security, Cloud Workload Protection]
Capsule8 [Capsule8]
Caveonix [Cloud Workload Protection Platform]
Cimcor [CimTrak]
Cisco [(acquired Portshift) and Secure Workload]
CrowdStrike [Falcon Platform]
Fidelis (acquired CloudPassage) [Halo]
Huawei [Host Security Service]
IBM [Red Hat Advanced Cluster Security for Kubernetes (acquired StackRox)]
Intezer [Intezer Analyze, Intezer Protect]
Kaspersky (see Note 4) [Hybrid Cloud Security]
Lacework [Lacework]
McAfee [Cloud Workload Security, Application Control, Change Control]
Microsoft [Azure Defender]
Morphisec [Morphisec]
NeuVector [Full Lifecycle Container Security]
Orca Security [Orca]
Palo Alto Networks [Prisma Cloud]
Polyverse [Polymorphing for Linux]
Qingteng (China only) [Qingteng Wanxiang·Workload Adaptive Security Platforms]
Qualys [Container Security and Cloud Platform]
Rezilion [Rezilion]
Safedog (China only) [Cloud Armor, Cloud Eye, Cloud Gap]
SentinelOne [Cloud Workload Protection, Container Protection]
Sophos [Intercept X for Server]
Sysdig [Sysdig Secure]
Tencent [Cloud Workload Protection]
Threat Stack [Threat Stack]
Tigera [Calico Enterprise]
Trend Micro [Deep Security, Cloud One Application Security (serverless), Cloud One Container Security, Cloud One Workload Protection]
Tripwire [Tripwire Enterprise]
Virsec [Virsec]
VMware (Carbon Black) [App Control, Workload Protection, Container Protection]
Wiz [Wiz]

Source: Gartner

Market Introduction

The market for CWPPs has emerged over the past 10 years as the protection needs of modern hybrid cloud workloads have diverged from the protection needs of end-user endpoints. CWPP capabilities are different and, where common controls are used, they are prioritized differently from those of EPPs (see Endpoint and Server Security: Common Goals, Divergent Solutions). The market for endpoint protection has split into two distinct markets — one focused on end-user-focused device protection (EPP; see Magic Quadrant for Endpoint Protection Platforms) and the other on CWPP (discussed in this Market Guide).

Market Recommendations

The need for CWPP offerings continues to grow as enterprise requirements evolve. We recommend using the following criteria when evaluating CWPP offerings:

- Coverage of the hierarchy of controls in Figure 4 that are important to the enterprise.
- Support for Windows, Linux and Linux containers (with explicit support for Kubernetes), and support for serverless function scanning and runtime protection.
- Licensing portability across on-premises and public cloud deployments.
- Traditional per-workload/per-year licensing, with licensing options for usage-based consumption based on image size (for example, per minute).
- Console as a service provided from the cloud for ease of deployment.
- Software available and integrated in the cloud provider's application store for ease of consumption.
- Integrated CSPM/KSPM capabilities (typically charged for separately).
- Optional anti-malware scanning capabilities, including the option to scan cloud object stores.

We recommend the following best practices when evaluating CWPP offerings:

- Develop a specific strategy for the protection of cloud workloads that meets the unique requirements of server workload protection.
- Do not expect an offering designed to protect end-user endpoints to provide adequate protection for server workloads.
- If you still use Windows Server 2008 or other OSs that are no longer supported by their providers, require CWPP vendors to continue to support those OSs, and identify what, if any, compensating controls they provide if the system is unpatched.
- Require CWPP offerings to protect physical machines, VMs, containers and serverless workloads — all managed from a single console, regardless of location. Hybrid, multicloud architecture represents the future of most enterprise data centers.
- Require CWPP offerings to expose all their functionality via APIs to facilitate automation.

- Make container protection capabilities a requirement in your CWPP evaluation. If you are using Kubernetes and considering a managed Kubernetes service, make explicit support of this environment a requirement as well.
- Ask CWPP vendors about their roadmaps and architectures for serverless function scanning and protection.
- If your existing CWPP vendor lacks mature support for containers or serverless functions, consider purchasing another vendor's CWPP offering that does provide this support.
- Extend workload scanning (especially for containers and serverless functions) proactively into the CI/CD pipeline. CWPP offerings that focus on runtime protection only are missing the critical shift in terms of how applications and the workloads that host them are developed.
- Require CWPP vendors to provide CSPM/KSPM capabilities.
- Require CWPP vendors to support alternative deployment options, including privileged containers, Kubernetes DaemonSets, sidecars and emerging options for disk image analysis (typically via snapshotting).
- Prepare for a future in which CWPP runtime agents may not be needed. Containers and serverless functions should be scanned for vulnerabilities and configuration predeployment. However, when deployed within immutable infrastructure and monitored from the outside for unusual behaviors, they may not warrant supplemental runtime protection from within the workload itself.

Evidence

[1] Gartner's 2020 Cloud End-User Buying Behavior Survey was conducted to understand how technology leaders approach buying, renewing and using cloud technology.

It was conducted online from July through August 2020, with 850 respondents from midsize and larger organizations (those with over $100 million in annual revenue) in the U.S., Canada, Germany, Australia and India.

Industries represented included energy, financial services, government, healthcare, insurance, manufacturing, retail, and utilities.

All the respondents' organizations were required to have cloud technology currently deployed.

Respondents were involved, either as decision makers or decision advisors, in new purchases, contract renewals, or contract reviews for one of the following types of cloud technology in the previous three years: public cloud infrastructure (IaaS), public cloud platforms (PaaS), public cloud software (SaaS), private cloud infrastructure, hybrid cloud infrastructure, multicloud infrastructure.

Respondents were required to work in IT-focused roles, except for a small subset of procurement respondents.

The survey included the following question: Which of the following statements best describes your organization's approach to working with public cloud infrastructure (IaaS) providers? In response, 76% of the respondents indicated that they use multiple cloud providers (n = 724 respondents currently using public cloud, hybrid cloud or multicloud infrastructure [IaaS], excluding "don't know/not sure")

[2] Gartner's 2020 Cloud End-User Buying Behavior Survey also asked: What are the top three challenges related to working with multiple public cloud infrastructure (IaaS) providers? The most frequently selected challenge was increased security risk (46% of respondents chose this). Close behind came increased complexity in operating and administering multiple clouds (45%). (n = 545 respondents currently using multiple public cloud IaaS providers, excluding "don't know/not sure")

[3] 2020 Cloud Native Computing Foundation Survey: Ninety-two percent of respondents said they use containers in production, up from 84% of respondents in 2019 and 73% in 2018. Thirty percent of respondents used serverless technologies in production environments.

[4] Standard configuration baselines are available from organizations such as the Center for Internet Security. This group has established baselines for AWS (Securing Amazon Web Services), Azure (Securing Microsoft Azure) and environments such as Docker (CIS Docker Benchmarks). Other organizations, such as the U.S. Defense Information Systems Agency, have established guidelines as well.

[5] Gartner's Enabling Cloud-Native DevSecOps Survey was conducted online from 12 May to 21 May 2021 to identify the emerging governing structures, security owners, technologies used and current challenges in the DevSecOps pipeline to secure cloud-native applications.

In total, 85 IT and business leaders involved in DevSecOps initiatives participated in the survey. Eighty-two were from Gartner's IT and Business Leaders Research Circle — a Gartner-managed panel. Three were from an external sample.

Participants from North America (44%), EMEA (35%), Asia/Pacific (8%) and Latin America (13%) responded to the survey.

The survey was developed collaboratively by a team of Gartner analysts. It was reviewed, tested, and administered by Gartner's Research Data and Analytics team.

Note: the results of this study are representative of the respondent base and not necessarily of the market as a whole.

"Vulnerability severity score" (62%) and "whether the application is externally accessible" (60%) were the two metrics identified as most important (n = 82, excluding "not sure").

Note 1
Representative Vendor Selection

At the time of this Market Guide's publication, each representative vendor listed had a shipping offering specifically designed for workload-centric protection.

Note 2 Examples of CWPP Vendors That Are Building or Acquiring CSPM Capabilities

Aqua Security (acquired CloudSploit); Armo; Caveonix; CloudAware; Fidelus (CloudPassage); FireEye (acquired Cloudvisory); CrowdStrike; Lacework; McAfee (via its MVISION ePO offering); Palo Alto Networks (acquired RedLock, Evident.io and Bridgecrew); Sophos; Symantec; Sysdig; Threat Stack; Trend Micro (acquired Cloud Conformity); VMware (acquired CloudCoreo)

Note 3 Examples of CSPM Vendors That Are Building or Acquiring CWPP Capabilities

Check Point CloudGuard; Orca Security (visibility into workload vulnerabilities, configuration and malware); Radware (protection extended into Kubernetes); Rapid7 (acquired Alcide); Wiz (visibility into workload vulnerabilities, configuration and malware)

Note 4 Kaspersky

In September 2017, the U.S. government ordered all federal agencies to remove Kaspersky's software from their systems. Several media reports, citing unnamed intelligence sources, made additional claims. Gartner is unaware of any evidence brought forward in this matter. Kaspersky launched its Global Transparency Initiative (GTI) and established data centers in Switzerland to relocate customer data processing functions as well as launched transparency centers in Switzerland and Spain to allow external review of its internal processes and source code of its products. The company has undergone a SOC 2 Type 1 audit by a Big 4 firm and obtained ISO/IEC 27001:2013 certification, and increased bug bounty awards up to $100,000 for security researchers. Kaspersky is continuing to migrate North America and Europe customers and plans to open additional transparency centers in Kuala Lumpur, Malaysia, and São Paulo, Brazil. Gartner clients who work directly with U.S. federal agencies should consider this information in their vendor selection and continue to monitor this situation for updates.

Document Revision History

Market Guide for Cloud Workload Protection Platforms - 14 April 2020

Market Guide for Cloud Workload Protection Platforms - 8 April 2019

Market Guide for Cloud Workload Protection Platforms - 26 March 2018

Market Guide for Cloud Workload Protection Platforms - 22 March 2017

Market Guide for Cloud Workload Protection Platforms - 3 March 2016

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

How to Make Cloud More Secure Than Your Own Data Center

12 Things to Get Right for Successful DevSecOps

How to Protect Your Clouds With CSPM, CWPP, CNAPP and CASB

Endpoint and Server Security: Common Goals, Divergent Solutions

Emerging Technologies: Functionality Spectrum for Cloud Workload Protection Platforms

Integrating Security Into the DevSecOps Toolchain

Gartner Peer Insights 'Lessons Learned': Implementing Cloud Workload Protection Platforms

Table 1: Examples of Cloud Workload Protection Platform Vendors and Their Offerings

Vendor Name [Offering name]
Aqua Security [Cloud Native Security Platform]
Alibaba Cloud [Cloud Security Center]
Armo [Armo Kubernetes Fabric]
Atomicorp [Atomic Protector]
Beijing Qianxin Technology (China only) [Unified Server Security Manager]
Bitdefender [GravityZone Platform]
Broadcom (acquired Symantec) [Data Center Security, Cloud Workload Protection]
Capsule8 [Capsule8]
Caveonix [Cloud Workload Protection Platform]
Cimcor [CimTrak]
Cisco [(acquired Portshift) and Secure Workload]
CrowdStrike [Falcon Platform]
Fidelis (acquired CloudPassage) [Halo]
Huawei [Host Security Service]
IBM [Red Hat Advanced Cluster Security for Kubernetes (acquired StackRox)]

Intezer [Intezer Analyze, Intezer Protect]
Kaspersky (see Note 4) [Hybrid Cloud Security]
Lacework [Lacework]
McAfee [Cloud Workload Security, Application Control, Change Control]
Microsoft [Azure Defender]
Morphisec [Morphisec]
NeuVector [Full Lifecycle Container Security]
Orca Security [Orca]
Palo Alto Networks [Prisma Cloud]
Polyverse [Polymorphing for Linux]
Qingteng (China only) [Qingteng Wanxiang·Workload Adaptive Security Platforms]
Qualys [Container Security and Cloud Platform]
Rezilion [Rezilion]
Safedog (China only) [Cloud Armor, Cloud Eye, Cloud Gap]
SentinelOne [Cloud Workload Protection, Container Protection]
Sophos [Intercept X for Server]
Sysdig [Sysdig Secure]
Tencent [Cloud Workload Protection]

Threat Stack [Threat Stack]
Tigera [Calico Enterprise]
Trend Micro [Deep Security, Cloud One Application Security (serverless), Cloud One Container Security, Cloud One Workload Protection]
Tripwire [Tripwire Enterprise]
Virsec [Virsec]
VMware (Carbon Black) [App Control, Workload Protection, Container Protection]
Wiz [Wiz]

Source: Gartner