Forecast Analysis: Cloud Workload Protection Platforms, Worldwide

Published 1 December 2021 - ID G00755223 - 8 min read

By Analyst(s): Mark Wah, Shailendra Upadhyay, Rahul Yadav

Initiatives: Technology Market Essentials

The cloud workload protection platform market is expected to grow from an estimated $2 billion in 2020 to $6.65 billion by 2025 due to accelerated cloud adoption and pull-forward demand due to COVID-19.

Overview

Forecast Assumptions

- Through 2022, cloud workload protection platform (CWPP) will observe higher growth rates between 28% and 40% that is in line with IaaS and PaaS growth rates before slowing gradually.

- By 2025, at least 70% of CWPP spend will be on CWPP vendors with broad CWPP capabilities compared to specialized capabilities such as memory protection and operating systems protection only, up from approximately 50% in 2020.

- By 2025, more than 50% of traditional security revenue protecting on-premises workloads, such as server protection, endpoint protection, and identity-based segmentation, will shift to CWPP as vendors position platform capabilities to address diverse workloads.
Market Impacts

- The CWPP market spending is projected to experience accelerated growth in the short term, growing to $3.5 billion in 2022.

- As more enterprises are adopting diverse cloud workloads, CWPP products with broad coverage will be preferred, and it is imperative for technology and service providers (TSPs) to meet this need.

- Cloud migration will require new approaches to address workload security, and many security vendors are repositioning their portfolio to address the need toward cloud security platforms such as CWPP.

Notable Changes

This document provides updated estimates of the revenue size and the associated five-year compound annual growth rate (CAGR) for a defined market segment. It also accounts for macroeconomic trends as the result of COVID-19. For more details about the methodology used to create our forecast for cloud workload protection platforms, see Market Definitions and Methodology: Software.

Forecast Data Summary

Figure 1 shows the CWPP market revenue forecast for 2020 through 2025 and the associated five-year CAGR.
Figure 1. Forecast Cloud Workload Protection Platforms, Worldwide, 2020-2025

**Forecast Analysis Cloud Workload Protection Platforms**

- **Five-Year Market Growth = $4.65 Billion (CAGR 27.2%)**
- **Worldwide Market Revenue, 2025 = $6.65 Billion**

Source: Gartner (December 2021)
ID: 756223

**Forecast Model Summary**

Figure 2 shows a simplified market model for the worldwide CWPP market revenue forecast.
Influencing Factors and Assumptions

Organizations continue to adopt public cloud, private cloud, containers and serverless computing at higher rates as the result of COVID-19 and digital transformation as described in The 2021 CIO Agenda: Seize This Opportunity for Digital Business Acceleration. Organizations are also modernizing cloud workloads with cloud-native services capabilities that introduce diverse workloads that require different workload protection capabilities. Some are incorporating DevSecOps practice that includes integrations cloud security products such as CWPP. Technology and service providers (TSPs) must meet this demand by offering broad CWPP capabilities that align with all forms of cloud workloads.

General Influencing Factors

CWPP solutions are influenced by multiple general adoption factors, including:

- CWPP Growth Will Correlate IaaS and PaaS Growth Rates
- Diverse Cloud Workload Drives Demand for CWPP With Broad-Based Capabilities
- Traditional Security Revenue Shifting to Cloud Security, Including CWPP

With these associated assumptions:

- Through 2022, cloud workload protection platform will observe higher growth rates between 20% and 40% that is in line with IaaS and PaaS growth rates before slowing gradually.
- By 2025, at least 70% of CWPP spend will be on CWPP vendors with broad CWPP capabilities compared to specialized capabilities such as memory protection and operating systems protection only, up from 50% in 2020.
- By 2025, more than 50% of traditional security revenue protecting on-premises workloads, such as server protection, endpoint protection, and identity-based segmentation, will shift to CWPP as vendors position platform capabilities to address diverse workloads.
Influencing Factor: CWPP Growth Will Correlate IaaS and PaaS Growth Rates

Gartner’s forecast for public cloud infrastructure as a service (IaaS) and platform as a service (PaaS) services continues to grow at a five-year CAGR of 31.9% and 25.6%, respectively, through 2025 (see Forecast Analysis: Public Cloud Services, Worldwide, 3Q21 Update). End-user spending on CWPP is correlated to the adoption of IaaS and PaaS services, but slightly lags initial adoption. For example, CWPP may not be adopted in test and development environments, but will be part of the staging and production environment.

Forecast Assumption: Through 2022, cloud workload protection platform will observe higher growth rates between 28% and 40% that is in line with IaaS and PaaS growth rates before slowing gradually.

Updated — Cloud adoption and digital transformation continue to grow, having been accelerated by COVID-19. From the security perspective, Emerging Technologies: Adoption Growth Insights for Cloud Workload Protection Platforms highlights the need to meet new security requirements in the cloud through CWPP as workloads move to the cloud leveraging IaaS and PaaS. This is apparent in key growth areas such as highly regulated industries and larger enterprises with legacy on-premises workloads that are being migrated to the cloud — both public and private cloud.

- COVID-19 and digital transformation acceleration, including cloud-native workload adoption from containers to serverless functions.
- CWPP capabilities and features aligning with user needs from simple IaaS workloads to cloud-native workloads.
- Adoption of hybrid, multicloud infrastructure. Seventy-six percent of a Gartner survey respondents are leveraging multicloud.¹
- CWPP and cloud security posture management (CSPM) convergence and the emergence of cloud-native application protection platform (CNAPP).
- Adjacent services needed, for example, support, implementation, managed security services and emerging vendor-delivered service wrapper as described in Emerging Technologies and Trends Impact Radar: Security.
- Regulatory demands in highly regulated industries (for example, for General Data Protection Regulation [GDPR], PCI, and Health Insurance Portability and Accountability Act [HIPAA])
The broader cloud security space is active with acquisitions and venture capital investments as described in *Emerging Technologies: Venture Capital Growth Insights for Cloud Security*. CWPP which is part of the convergence toward cloud-native application protection platforms (CNAPP) has strong venture capital investment interests with $603 million in 2020 and more than $2 billion in 2021. This contributes to market awareness and increased sales capacity by CWPP and CNAPP vendors. See *Innovation Insight for Cloud-Native Application Protection Platforms* and *How to Protect Your Clouds With CSPM, CWPP, CNAPP and CASB* for additional details.

High growth within CWPP will continue through 2022, but will taper off to be closer to IaaS and PaaS growth rates in the 20% to 25% range through 2025, as shown in Figure 1. Part of the initial high growth is attributed to the pull-forward demand due to digital transformation trends and some revenue shifts from traditional security capabilities protecting on-premises workloads to CWPP.

---

**Influencing Factor: Diverse Cloud Workload Drives Demand for CWPP With Broad-Based Capabilities**

Organizations are adopting more cloud-native services at a higher rate, and PaaS that aligns with cloud-native consumption is growing at a CAGR of 25.6% as described in *Forecast Analysis: Public Cloud Services, Worldwide, 3Q21 Update*.

**Forecast Assumption: By 2025, at least 70% of CWPP spend will be on CWPP vendors with broad CWPP capabilities compared to specialized capabilities such as memory protection and operating systems protection only, up from 50% in 2020.**

New — Cloud-native services such as containers are growing slightly higher where the container management market is expected to grow at a CAGR of 34% as described in *Market Guide for Container Management* that covers both public and private cloud. *Market Guide for Cloud Workload Protection Platforms* indicates that many CWPP vendors have expanded their offering to address diverse workloads from hybrid environments with on-premises workloads to serverless PaaS. Many vendors have also added adjacent capabilities like cloud security posture management (CSPM).

CWPP vendors with broad CWPP capabilities that address diverse cloud workloads have larger market share compared to vendors specializing in specific capabilities. Based on the vendor survey and estimates, the market share for vendors with broad CWPP capabilities is approximately 50% in 2020 compared to vendors specializing in memory protection and operating systems protection that capture less than 20% of the estimated market share.
As end-user organizations operate in a hybrid and multicloud environment, many will prefer to work with fewer vendors to address the security needs for CWPP compared to multiple best-of-breed vendors. This is a general trend observed and described in Security Vendor Consolidation Trends — Should You Pursue a Consolidation Strategy? This also applies to CWPP as the expected capabilities will expand.

**Influencing Factor: Traditional Security Revenue Shifting to Cloud Security, Including CWPP**

In the initial cloud migration phase, end user organizations attempted to use traditional server and endpoint security products to address IaaS cloud workload security. These organizations will soon realize that traditional endpoint security solutions are not well-suited for cloud-specific scenarios where workloads require automated scaling, consistency across dynamic cloud changes, and unified reporting and alerting.

The adoption of cloud-native application development using container, Kubernetes, and serverless PaaS require CWPP capabilities to adapt to these modern workloads. Many CWPP TSPs have responded by building new capabilities and acquiring startups focusing in these areas. Some TSPs have repositioned traditional on-premises security products to be part of CWPP. This is not surprising given that innovation, new products and services are being built and delivered from the cloud.

**Forecast Analysis: By 2025, more than 50% of traditional security revenue protecting on-premises workloads, such as server protection, endpoint protection, and identity-based segmentation, will shift to CWPP as vendors position platform capabilities to address diverse workloads.**

New — Gartner believes that, by 2025, more than 50% of traditional security products protecting on-premises workloads such as server protection, endpoint protection, and identity-based segmentation, will shift to CWPP as vendors position platform capabilities to address hybrid and multicloud workloads. Many TSPs have transitioned their focus from traditional security products to cloud security platforms, such as CWPP, in response to digital transformation and the shift in market needs.

This change is also observed in the vendor survey outcomes for CWPP. Several endpoint protection platforms (EPP) and identity-based segmentation TSPs have shifted their revenue toward CWPP. This shift has also contributed to higher growth observed for 2020 and estimated to continue through 2022.
Evidence

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

The research was conducted online from July through August 2020 among 850 respondents from midsize and larger ($100+ million in revenue) organizations in the U.S., Canada, the U.K., Germany, Australia and India. Industries surveyed include energy, financial services, government, healthcare, insurance, manufacturing, retail and utilities. All organizations were required to currently have cloud deployed.

Respondents are involved, either as a decision maker or decision advisor, in new purchases, contract renewals or contract reviews for one of the following cloud types in the past three years: public cloud infrastructure (IaaS), public cloud platform (PaaS), public cloud software (SaaS), private cloud infrastructure, hybrid cloud infrastructure or multicloud infrastructure. Respondents were also required to work in IT-focused roles, with a small subset of procurement respondents.

The study was developed collaboratively by Gartner analysts and the Primary Research Team.

Disclaimer: Results of this study do not represent global findings or the market as a whole, but reflect sentiment of the respondents and companies surveyed.

Document Revision History

Forecast Analysis: Cloud Workload Protection Platforms, Worldwide - 2 July 2019

Recommended by the Authors

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

Forecast Analysis: Public Cloud Services, Worldwide, 3Q21 Update
The 2021 CIO Agenda: Seize This Opportunity for Digital Business Acceleration
Emerging Technologies and Trends Impact Radar: Security
Emerging Technologies: Venture Capital Growth Insights for Cloud Security
Emerging Technologies: Adoption Growth Insights for Cloud Workload Protection Platforms
Market Guide for Cloud Workload Protection Platforms